DISA AT Mock Test Papers

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

© The Institute of Chartered Accountants of India

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic mechanical, photocopying, recording, or otherwise, without prior permission, in writing, from the publisher.

DISCLAIMER

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every effort have been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit CIT portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Edition	:	October, 2015
Committee/Department	:	Committee on Information Technology
Email	:	cit@icai.in
Website	:	www.icai.org http://cit.icai.org
Price	:	₹
ISBN No	:	978-81-8441-
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra - 282 003.

Contents

Mock Assessment Test Paper 1

1. In switching over to an Electronic Fund Transfer (EFT) environment, which of the following risks DOES NOT occur?

   A. Increased access violations

   B. Increased cost per transaction

   C. Inadequate backup and recovery procedures

   D. Duplicate transaction processing

   The correct answer is: B. Increased cost per transaction

   Explanation: Automation Leads to decrease in cost and increase in performance. Choices A, C and D are not applicable in the given context.

2. Which of the following is NOT TRUE about a database management system application environment?

   A. Multiple users use data concurrently

   B. Data are shared by passing files between programs or systems

   C. The physical structure of the data is independent of user needs

   D. Each request for data made by an application program must be analyzed by DBMS.

   The correct answer is B. Data are shared by passing files between programs or systems

   Explanation: In DBMS data exchange is facilitated through SQL hence Option B is not true Files are not used for data exchange. Option A, C and D are features of DBMS.

3. Which one of the following network architectures is designed to provide data services using physical networks that are more reliable and offer greater bandwidth?

   A. Transmission control protocol/Internet Protocol (TCP/IP)

   B. File transfer protocol

   C. Permanent Virtual Circuit (PVC) Integrated services digital network (ISDN)

   The correct answer is: D. Integrated services digital network (ISDN)

   Explanation: Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Option A, B and C are not applicable.

4. Which of the following decisions most likely cannot be made on the basis of performance monitoring statistics that are calculated:

   A. whether new hardware/system software resources are needed

   B. whether unauthorized use is being made of hardware/system software resources

   C. whether the system being monitored has provided users with a strategic advantage over their competitors.

   D. whether there is any abnormal work load during a particular shift which may be because of private use of resources by some staff

   The correct answer is: C. whether the system being monitored has provided users with a strategic advantage over their competitors.

   Explanation: Only Option C is a kind of decision that is subjective in nature and in not based on statistics as Option A, B and D are.

5. Control over data preparation is important because:

   A. it is often a major cost area taking about 50% of the data processing budget

   B. unauthorized changes to data and program can take place

   C. the work is boring so high turnover always occurs

   D. it can be a major bottleneck in the work flow in a data processing installation

   The correct answer is: D. it can be a major bottleneck in the work flow in a data processing installation.

   Explanation: Data Preparation is very critical for various operations that needs data so it may result in bottlenecks and affects performance. Option A may also be a reason but not the most important. Option B is not applicable as we are considering data only not programs. Option C is not applicable in the given context.

6. During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

   A. test data to validate data input

   B. test data to determine system sort capabilities

   C. generalized audit software to search for address field duplications

   D. generalized audit software to search for account field duplications

   The correct answer is: C. generalized audit software to search for address field duplications.

   Explanation: Since the name is not the same (due to name variations), one method to

detect duplications would be to compare other common fields, such as addresses. Subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

7. The IS department of an organization wants to ensure that the computer files used in the information processing facility are adequately backed up to allow for proper recovery. This is a(n):

   A. control procedure

   B. control objective

   C. corrective control

   D. operational control

   The correct answer is: B. control objective.

   Explanation: IS control objectives specify the minimum set of controls to ensure efficiency and effectiveness in the operations and functions within an organization. Control procedures are developed to provide reasonable assurance that specific objectives will be achieved. A corrective control is a category of controls that aims to minimize the threat and/or remedy problems that were not prevented or were not initially detected. Operational controls address the day-to-day operational functions and activities, and aid in ensuring that the operations are meeting the desired business objectives.

8. During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

   A. create the procedures document

   B. terminate the audit

   C. conduct compliance testing

   D. identify and evaluate existing practices.

   The correct answer is: D. identify and evaluate existing practices.

   Explanation: One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, and doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

9. When implementing continuous monitoring systems, an IS auditor's first step is to identify:

   A. reasonable target thresholds

   B. high-risk areas within the organization

   C. the location and format of output files

   D. applications that provide the highest potential payback

   The correct answer is: B. high-risk areas within the organization.

   Explanation: The first and most critical step in the process is to identify high-risk areas within the organization. Business department managers and senior executives are in the best positions to offer insight into these areas. Once potential areas of implementation have been identified, an assessment of potential impact should be completed to identify applications that provide the highest potential payback to the organization. At this point, tests and reasonable target thresholds should be determined prior to programming. During systems development, the location and format of the output files generated by the monitoring programs should be defined.

10. In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools is MOST suitable for performing that task?

    A. CASE tools

    B. Embedded data collection tools

    C. Heuristic scanning tools

    D. Trend/variance detection tools

    The correct answer is: D. Trend/variance detection tools.

    Explanation: Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for pre-numbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

11. Computer viruses could be detected by which one of the following actions?

    A. Maintain backups of program and data.

    B. Monitor usage of the device.

    C. Use write-protect tabs on disks.

    D. Examine the creation date and file size.

    The correct answer is: D. Examine the creation date and file size

Explanation: Viruses can be detected by examining file content and other attributes of file hence option D is applicable. Option A, B and C are not applicable.

12. Before disposing off the PC used for storing confidential data the most important precautionary measure to be taken is

    A. mid-level formatting of hard disk

    B. deleting all the files in the hard disk

    C. deleting all the data on the hard disk

    D. demagnetizing the hard disk.

    The correct answer is: B. vulnerabilities and threats are identified.

    Explanation: Demagnetizing is reduction or elimination of the magnetic moment in an object; that is, the reverse of magnetization. This results in complete erase of hard disk content. Option A, B and C are not as effective as Demagnetizing.

13. The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

    A. Test data

    B. Generalized audit software

    C. Integrated test facility

    D. Embedded audit module

    The correct answer is: B. Generalized audit software.

    Explanation: Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and re-computations. The IS auditor, using generalized audit software, could design appropriate tests to recompute the payroll and, thereby, determine if there were overpayments and to whom they were made. Test data would test for the existence of controls that might prevent overpayments, but it would not detect specific, previous miscalculations. Neither an integrated test facility nor an embedded audit module would detect errors for a previous period.

14. Which of the following would be the BEST population to take a sample from when testing program changes?

    A. Test library listings

    B. Source program listings

    C. Program change requests

    D. Production library listings

The correct answer is: D. Production library listings

Explanation: The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be time intensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

15. Which of the following normally would be the MOST reliable evidence for an auditor?

    A. A confirmation letter received from a third party verifying an account balance

    B. Assurance from line management that an application is working as designed

    C. Trend data obtained from World Wide Web (Internet) sources

    D. Ratio analysis developed by the IS auditor from reports supplied by line management

    The correct answer is: A. A confirmation letter received from a third party verifying an account balance

    Explanation: Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

16. During a review of the controls over the process of defining IT service levels, an IS auditor would MOST likely interview the:

    A. systems programmer

    B. legal staff

    C. business unit manager

    D. application programmer

    The correct answer is: C. business unit manager.

    Explanation: Understanding the business requirements is key in defining the service levels. While each of the other entities listed may provide some definition, the best choice here is the business unit manager because of this person's knowledge of the requirements of the organization.

17. In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, an IS auditor should:

    A. identify and assess the risk assessment process used by management

    B. identify information assets and the underlying systems

C. disclose the threats and impacts to management

D. identify and evaluate the existing controls.

The correct answer is: D. identify and evaluate the existing controls.

Explanation: It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

18. A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. A can identify high-risk areas that might need a detailed review later

B. allows IS auditors to independently assess risk

C. can be used as a replacement for traditional audits

D. allows management to relinquish responsibility for control.

The correct answer is: A can identify high-risk areas that might need a detailed review later.

Explanation: CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Answer B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Answer C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Answer D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

19. Senior management has requested that an IS auditor assist the departmental management in the implementation of necessary controls. The IS auditor should:

A. refuse the assignment since it is not the role of the IS auditor

B. inform management of his/her inability to conduct future audits

C. perform the assignment and future audits with due professional care

D. obtain the approval of user management to perform the implementation and follow-up.

The correct answer is: B. inform management of his/her inability to conduct future audits.

Explanation: In this situation the IS auditor should inform management of the impairment of independence in conducting further audits in the auditee area. An IS auditor can perform non-audit assignments where the IS auditor's expertise can be of use to management;

however, by performing the non-audit assignment, the IS auditor cannot conduct the future audits of the auditee as his/her independence may be compromised. However, the independence of the IS auditor will not be impaired when suggesting/recommending controls to the auditee after he audit.

20. Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

    A. Multiple cycles of backup files remain available.

    B. Access controls establish accountability for e-mail activity

    C. Data classification regulates what information should be communicated via e-mail.

    D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

    The correct answer is: A. Multiple cycles of backup files remain available.

    Explanation: Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

21. Which of the following is a benefit of a risk-based approach to audit planning? Audit:

    A. scheduling may be performed months in advance

    B. budgets are more likely to be met by the IS audit staff

    C. staff will be exposed to a variety of technologies

    D. resources are allocated to the areas of highest concern

    The correct answer is: D. resources are allocated to the areas of highest concern.

    Explanation: The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year

22. Internet was established NOT for:

    A. minimizing the high risk protocol conversion functions that the gateways perform

    B. controlling all the networks connected in a better way

C. improving the overall reliability of the networks

D. restricting access to sensitive messages by restricting them to specific parts of the network

The correct answer is: A. minimizing the high risk protocol conversion functions that the gateways perform.

Explanation: The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. Internet was not established for minimizing the high risk protocol conversion functions that the gateways perform. Option B, C and D are reasons for establishment of internet .

23. An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the network.

B. Users can install software on their desktops

C. Network monitoring is very limited

D. Many user ids have identical passwords.

The correct answer is: D. Many user ids have identical passwords.

Explanation: Exploitation of a known user id and password requires minimum technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user ids have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high (for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

24. While planning an audit, an assessment of risk should be made to provide:

A. reasonable assurance that the audit will cover material items.

B. definite assurance that material items will be covered during the audit work

C. reasonable assurance that all items will be covered by the audit

D. sufficient assurance that all items will be covered during the audit work

The correct answer is: A. reasonable assurance that the audit will cover material items.

Explanation: The ISACA IS Auditing Guideline G15 on planning the IS audit states, "An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems." Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

25. To identify the value of inventory that has been kept for more than eight weeks, an IS auditor would MOST likely use:

    A. test data

    B. statistical sampling

    C. an integrated test facility

    D. generalized audit software

    The correct answer is: D. generalized audit software.

    Explanation: Generalized audit software will facilitate reviewing the entire inventory file to look for those items that meet the selection criteria. Generalized audit software provides direct access to data and provides for features of computation, stratification, etc. Test data are used to verify programs, but will not confirm anything about the transactions in question. The use of statistical sampling methods is not intended to select specific conditions, but is intended to select samples from a file on a random basis. In this case, the IS auditor would want to check all of the items that meet the criteria and not just a sample of them. An integrated test facility allows the IS auditor to test transactions through the production system.

26. An integrated test facility is considered a useful audit tool because it:

    A. is a cost-efficient approach to auditing application controls

    B. enables the financial and IS auditors to integrate their audit tests

    C. compares processing output with independently calculated data

    D. provides the IS auditor with a tool to analyze a large range of information

    The correct answer is: C. compares processing output with independently calculated data.

    Explanation: An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves

setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

27. The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

    A. Inherent

    B. Detection

    C. Control

    D. Business

    The correct answer is: B. Detection

    Explanation: Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks usually are not affected by the IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by the IS auditor.

28. Data flow diagrams are used by IS auditors to:

    A. order data hierarchically

    B. highlight high-level data definitions

    C. graphically summarize data paths and storage

    D. portray step-by-step details of data generation.

    The correct answer is: C. graphically summarize data paths and storage.

    Explanation: Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

29. Reviewing management's long-term strategic plans helps the IS auditor:

    A. gain an understanding of an organization's goals and objectives

    B. test the enterprise's internal controls.

    C. assess the organization's reliance on information systems

    D. determine the number of audit resources needed

    The correct answer is: A. gain an understanding of an organization's goals and objectives.

    Explanation: Strategic planning sets corporate or departmental objectives into motion. Strategic planning is time- and project-oriented, but must also address and help determine

priorities to meet business needs. Reviewing long-term strategic plans would not achieve the objectives expressed by the other choices.

30. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware:

    A. of the point at which controls are exercised as data flow through the system

    B. that only preventive and detective controls are relevant

    C. that corrective controls can only be regarded as compensating

    D. that classification allows an IS auditor to determine which controls are missing.

    The correct answer is: A. of the point at which controls are exercised as data flow through the system.

    Explanation: An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

31. The risk of an IS auditor using an inadequate test procedure and concluding that material errors do not exist when, in fact, they do is an example of:

    A. inherent risk

    B. control risk

    C. detection risk

    D. audit risk.

    The correct answer is: C. detection risk.

    Explanation: This is an example of detection risk.

32. The PRIMARY purpose of an audit charter is to:

    A. document the audit process used by the enterprise

    B. formally document the audit department's plan of action

    C. document a code of professional conduct for the auditor

    D. describe the authority and responsibilities of the audit department

    The correct answer is: D. describe the authority and responsibilities of the audit department.

    Explanation: The audit charter typically sets out the role and responsibility of the internal audit department. It should state management's objectives for and delegation of authority to

the audit department. It is rarely changed and does not contain the audit plan or audit process, which is usually part of annual audit planning, nor does it describe a code of professional conduct, since such conduct is set by the profession and not by management.

33. An IS auditor has evaluated the controls for the integrity of the data in a financial application. Which of the following findings would be the MOST significant?

A. The application owner was unaware of several changes applied to the application by the IT department.

B. The application data are backed up only once a week.

C. The application development documentation is incomplete.

D. Information processing facilities are not protected by appropriate fire detection systems.

The correct answer is: A. The application owner was unaware of several changes applied to the application by the IT department.

Explanation: Choice A is the most significant finding as it directly affects the integrity of the application's data and is evidence of an inadequate change control process and incorrect access rights to the processing environment. Although backing up the application data only once a week is a finding, it does not affect the integrity of the data in the system. Incomplete application development documentation does not affect integrity of the data. The lack of appropriate fire detection systems does not affect the integrity of the data but may affect the storage of the data.

34. Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability

B. the magnitude of the impact should a threat source successfully exploit the vulnerability

C. the likelihood of a given threat source exploiting a given vulnerability

D. the collective judgment of the risk assessment team.

The correct answer is: A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

Explanation: Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

35. Which one of the following could an IS auditor use to validate the effectiveness of edit and validation routines?

    A. Domain integrity test

    B. Relational integrity test

    C. Referential integrity test

    D. Parity checks

    The correct answer is: A. Domain integrity test

    Explanation: Domain integrity testing is aimed at verifying that the data conform to definitions, i.e., the data items are all in the correct domains. The major objective of this exercise is to verify that the edit and validation routines are working satisfactorily. Relational integrity tests are performed at the record level and usually involve calculating and verifying various calculated fields, such as control totals. Referential integrity tests involve ensuring that all references to a primary key from another file actually exist in their original file. A parity check is a bit added to each character prior to transmission. The parity bit is a function of the bits making up the character. The recipient performs the same function on the received character and compares the result to the transmitted parity bit. If it is different, an error is assumed.

36. An IS auditor reviews an organizational chart PRIMARILY for:

    A. an understanding of workflows.

    B. investigating various communication channels.

    C. understanding the responsibilities and authority of individuals.

    D. investigating the network connected to different employees.

    The correct answer is: C. understanding the responsibilities and authority of individuals.

    Explanation: An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

37. An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

    A. the controls already in place.

    B. the effectiveness of the controls in place.

    C. the mechanism for monitoring the risks related to the assets.

    D. the threats/vulnerabilities affecting the assets.

The correct answer is: D. the threats/vulnerabilities affecting the assets.

Explanation: One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase. A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

38. Which of the following is an objective of a control self-assessment (CSA) program?

A. Concentration on areas of high risk

B. Replacement of audit responsibilities

C. Completion of control questionnaires

D. Collaborative facilitative workshops

The correct answer is: A. Concentration on areas of high risk

Explanation: The objectives of CSA programs include education for line management in control responsibility and monitoring and concentration by all on areas of high risk. The objectives of CSA programs include the enhancement of audit responsibilities, not replacement of audit responsibilities. Choices C and D are tools of CSA, not objectives.

39. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.

B. Determine the risks/threats to the data center site.

C. Review business continuity procedures.

D. Test for evidence of physical access at suspect locations.

The correct answer is: B. Determine the risks/threats to the data center site.

Explanation: During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

40. The traditional role of an IS auditor in a control self-assessment (CSA) should be that of:

A. facilitator.

B. manager.

C. partner.

D. stakeholder.

The correct answer is: A. facilitator.

Explanation: When CSA programs are established, IS auditors become internal control professionals and assessment facilitators. IS auditors are the facilitators and the client (management and staff) is the participant in the CSA process. During a CSA workshop, instead of the IS auditor performing detailed audit procedures, they should lead and guide the clients in assessing their environment. Choices B, C and D should not be roles of the IS auditor. These roles are more appropriate for the client.

41. The use of statistical sampling procedures helps minimize:

A. sampling risk.

B. detection risk.

C. inherent risk.

D. control risk.

The correct answer is: B. detection risk.

Explanation: Detection risk is the risk that the IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when in fact they do. Using statistical sampling, an IS auditor can quantify how closely the sample should represent the population and quantify the probability of error. Sampling risk is the risk that incorrect assumptions will be made about the characteristics of a population from which a sample is selected. Assuming there are no related compensating controls, inherent risk is the risk that an error exists, which could be material or significant when combined with other errors found during the audit. Statistical sampling will not minimize this. Control risk is the risk that a material error exists, which will not be prevented or detected on a timely basis by the system of internal controls. This cannot be minimized using statistical sampling.

42. An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

A. Design further tests of the calculations that are in error.

B. Identify variables that may have caused the test results to be inaccurate.

C. Examine some of the test cases to confirm the results.

D. Document the results and prepare a report of findings, conclusions and recommendations.

The correct answer is: C. Examine some of the test cases to confirm the results.

Explanation: The IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

43. An IS auditor is assigned to perform a post implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.

B. designed an embedded audit module exclusively for auditing the application system.

C. participated as a member of the application system project team, but did not have operational responsibilities.

D. provided consulting advice concerning application system best practices.

The correct answer is: A. implemented a specific control during the development of the application system.

Explanation: Independence may be impaired if the IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair the IS auditor's independence. Choice D is incorrect because the IS auditor's independence is not impaired by providing advice on known best practices.

44. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs.

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

The correct answer is: C. preparing simulated transactions for processing and comparing the results to predetermined results.

Explanation: Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

45. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

    A. Integrated test facility (ITF)

    B. Continuous and intermittent simulation (CIS)

    C. Audit hooks

    D. Snapshots

    The correct answer is: D. Snapshots

    Explanation: A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

46. The PRIMARY advantage of a continuous audit approach is that it:

    A. does not require an IS auditor to collect evidence on system reliability while processing is taking place.

    B. requires the IS auditor to review and follow up immediately on all information collected.

    C. can improve system security when used in time-sharing environments that process a large number of transactions.

    D. does not depend on the complexity of an organization's computer systems.

    The correct answer is: C. can improve system security when used in time-sharing environments that process a large number of transactions.

    Explanation: The use of continuous auditing techniques can improve system security when used in time-sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

47. Which of the following sampling methods is MOST useful when testing for compliance?

    A. Attribute sampling

    B. Variable sampling

    C. Stratified mean per unit

    D. Difference estimation

The correct answer is: A. Attribute sampling

Explanation: Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

48. An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable sampling.

B. substantive testing.

C. compliance testing.

D. stop-or-go sampling.

The correct answer is: C. compliance testing.

Explanation: Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

49. The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

A. information assets are overprotected.

B. a basic level of protection is applied regardless of asset value.

C. appropriate levels of protection are applied to information assets.

D. an equal proportion of resources are devoted to protecting all information assets.

The correct answer is: C. appropriate levels of protection are applied to information assets.

Explanation: Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or under protected. The risk assessment approach will ensure an appropriate level of protection is

applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

50. In a risk-based audit approach, an IS auditor should FIRST complete a(n):

A. inherent risk assessment.

B. control risk assessment.

C. test of control assessment.

D. substantive test assessment.

The correct answer is: A. inherent risk assessment.

Explanation: The first step in a risk-based audit approach is to gather information about the business and industry to evaluate the inherent risks. After completing the assessment of the inherent risks, the next step is to complete an assessment of the internal control structure. The controls are then tested and, on the basis of the test results, substantive tests are carried out and assessed.

51. The development of an IS security policy is ultimately the responsibility of the:

A. IS department.

B. security committee.

C. security administrator.

D. board of directors.

The correct answer is: D. board of directors.

Explanation: Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

52. To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

A. O/S and hardware refresh frequencies

B. Gain-sharing performance bonuses

C. Penalties for noncompliance

D. Charges tied to variable cost metrics

The correct answer is: B. Gain-sharing performance bonuses

Explanation: Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

53. Involvement of senior management is MOST important in the development of:

A. strategic plans.

B. IS policies.

C. IS procedures.

D. standards and guidelines.

The correct answer is: A. strategic plans.

Explanation: Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

54. An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program changes.

B. reviews network load requirements in terms of current and future transaction volumes.

C. assesses the impact of the network load on terminal response times and network data transfer rates.

D. recommends network balancing procedures and improvements.

The correct answer is: A. monitors systems performance and tracks problems resulting from program changes.

Explanation: The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

55. The output of the risk management process is an input for making:

A. business plans.

B. audit charters.

C. security policy decisions.

D. software design decisions.

The correct answer is: C. security policy decisions.

Explanation: The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

56. The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction policy.

B. security policy.

C. archive policy.

D. audit policy.

The correct answer is: C. archive policy.

Explanation: With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

57. An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirements.

B. if proposed system functionality is adequate.

C. the stability of existing software.

D. the complexity of installed technology.

The correct answer is: A. whether IT processes support business requirements.

Explanation: The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

58. An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environment.

B. the business plan.

C. the present IT budget.

D. current technology trends.

The correct answer is: B. the business plan.

Explanation: The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, the IS auditor would first need to familiarize him/herself with the business plan.

59. As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirements.

B. baseline security following best practices.

C. institutionalized and commoditized solutions.

D. an understanding of risk exposure.

The correct answer is: A. security requirements driven by enterprise requirements.

Explanation: Information security governance, when properly implemented, should provide four basic outcomes. They are strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

60. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

A. compute the amortization of the related assets.

B. calculate a return on investment (ROI).

C. apply a qualitative approach.

D. spend the time needed to define exactly the loss amount.

The correct answer is: C. apply a qualitative approach.

Explanation: The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor (e.g., one is a very low impact to the business and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to

estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

61. The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial results.

B. customer satisfaction.

C. internal process efficiency.

D. innovation capacity.

The correct answer is: A. financial results.

Explanation: Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

62. Establishing the level of acceptable risk is the responsibility of:

A. quality assurance management.

B. senior business management.

C. the chief information officer.

D. the chief security officer.

The correct answer is: B. senior business management.

Explanation: Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

63. Which of the following is the MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

The correct answer is: A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Explanation: Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules are also required along with the user's education on the importance of security.

64. To ensure an organization is complying with privacy requirements, the IS auditor should FIRST review:

A. the IT infrastructure.

B. the organization's policies, standards and procedures.

C. legal and regulatory requirements.

D. the adherence to organizational policies, standards and procedures.

The correct answer is: C. legal and regulatory requirements.

Explanation: To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, the IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

65. Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls

B. Boundary controls

C. Access controls

D. Compensating controls

The correct answer is: D. Compensating controls

Explanation: Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same

control objective or exposure Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

66. Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider

B. Participating in systems design with the provider

C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

The correct answer is: D. Monitoring the outsourcing provider's performance

Explanation: In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

67. Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.

B. define key performance indicators.

C. provide business value to IT projects.

D. control IT expenses.

The correct answer is: B. define key performance indicators.

Explanation: A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

68. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.

B. a lack of a methodology for systems development.

C. the technology not aligning with the organization's objectives.

D. an absence of control over technology contracts.

The correct answer is: C. the technology not aligning with the organization's objectives.

Explanation: A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

69. Which of the following would BEST provide assurance of the integrity of new staff?

A. Background screening

B. References

C. Bonding

D. Qualifications listed on a resumé

The correct answer is: A. Background screening

Explanation: A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a résumé may not be accurate.

70. Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.

B. Specific user accountability cannot be established.

C. Unauthorized users may have access to originate, modify or delete data.

D. Audit recommendations may not be implemented.

The correct answer is: C. Unauthorized users may have access to originate, modify or delete data.

Explanation: Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

71. Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business plan.

B. audit plan.

C. security plan.

D. investment plan.

The correct answer is: A. business plan.

Explanation: To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, and the security plan should be at a corporate level.

72. Which of the following is a function of an IS steering committee?

A. Monitoring vendor-controlled change control and testing

B. Ensuring a separation of duties within the information's processing environment

C. Approving and monitoring major projects, the status of IS plans and budgets

D. Liaising between the IS department and the end users

The correct answer is: C. Approving and monitoring major projects, the status of IS plans and budgets

Explanation: The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

73. A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

A. the length of service since this will help ensure technical competence.

B. age as training in audit techniques may be impractical.

C. IS knowledge since this will bring enhanced credibility to the audit function.

D. ability, as an IS auditor, to be independent of existing IS relationships.

The correct answer is: D. ability, as an IS auditor, to be independent of existing IS relationships.

Explanation: Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that

the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

74. Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response

B. Correction

C. Detection

D. Monitoring

The correct answer is: A. Response

Explanation: A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

75. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services

B. Participating in systems design with the provider

C. Managing compliance with the contract for the outsourced services

D. Negotiating contractual agreement with the provider

The correct answer is: C. Managing compliance with the contract for the outsourced services

Explanation: Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

76. When reviewing IS strategies, the IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

A. has all the personnel and equipment it needs.

B. plans are consistent with management strategy.

C. uses its equipment and personnel efficiently and effectively.

D. has sufficient excess capacity to respond to changing directions.

The correct answer is: B. plans are consistent with management strategy.

Explanation: Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

77. Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors.

B. Gather performance data.

C. Establish performance baselines.

D. Optimize performance.

The correct answer is: D. Optimize performance.

Explanation: An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability, and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

78. Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications

B. Identification of network applications to be externally accessed

C. Identification of vulnerabilities associated with network applications to be externally accessed

D. Creation of an applications traffic matrix showing protection methods

The correct answer is: B. Identification of network applications to be externally accessed

Explanation: Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for and possible methods of controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

79. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivity.

B. reduce the opportunity for an employee to commit an improper or illegal act.

C. provide proper cross-training for another employee.

D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

The correct answer is: B. reduce the opportunity for an employee to commit an improper or illegal act.

Explanation: Required vacations/holidays of a week or more duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions. This reduces the opportunity to commit improper or illegal acts, and during this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

80. In reviewing the IS short-range (tactical) plan, the IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.

B. there is a clear definition of the IS mission and vision.

C. there is a strategic information technology planning methodology in place.

D. the plan correlates business objectives to IS goals and objectives.

The correct answer is: A. there is an integration of IS and business staffs within projects.

Explanation: The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

81. An organization acquiring other businesses continues using its legacy EDI systems and uses three separate value-added network (VAN) providers. No written VAN agreements exist. The IS auditor should recommend that management:

A. obtains independent assurance of the third-party service providers.

B. sets up a process for monitoring the service delivery of the third party.

C. ensures that formal contracts are in place.

D. considers agreements with third-party service providers in the development of continuity plans.

The correct answer is: C. ensures that formal contracts are in place.

Explanation: Written agreements would assist management in ensuring compliance with external requirements. While management should obtain independent assurance of compliance, this cannot be achieved until there is a contract in place. One aspect of managing third-party services is to provide monitoring; however, this cannot be achieved until there is a contract. Ensuring that VAN agreements are available for review may assist in the development of continuity plans, if they are deemed critical IT resources. However, this cannot be achieved until a contract is in place.

82. Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package.

B. Perform an evaluation of information technology needs.

C. Implement a new project planning system within the next 12 months.

D. Become the supplier of choice for the product offered.

The correct answer is: D. Become the supplier of choice for the product offered.

Explanation: Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

83. Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT projects.

B. using the firm's past actual loss experience to determine current exposure.

C. reviewing published loss statistics from comparable organizations.

D. reviewing IT control weaknesses identified in audit reports.

The correct answer is: A. evaluating threats associated with existing IT assets and IT projects.

Explanation: To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Hence, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited and there may not be a sufficient assessment of strategic IT risks.

84. An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. Which would be the next task?

A. Report the risks to the CIO and CEO immediately.

B. Examine e-business application in development.

C. Identify threats and likelihood of occurrence.

D. Check the budget available for risk management.

The correct answer is: C. Identify threats and likelihood of occurrence.

Explanation: The IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

85. Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are managed.

B. A knowledge base on customers, products, markets and processes is in place.

C. A structure is provided that facilitates the creation and sharing of business information.

D. Top management mediate between the imperatives of business and technology

The correct answer is: D. Top management mediate between the imperatives of business and technology

Explanation: Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being

managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

86. Which of the following would be a compensating control to mitigate risks resulting from an inadequate segregation of duties?

A. Sequence check

B. Check digit

C. Source documentation retention

D. Batch control reconciliations

The correct answer is: D. Batch control reconciliations

Explanation: Batch control reconciliations are an example of compensating controls. Other examples of compensating controls are transaction logs, reasonableness tests, independent reviews and audit trails, such as console logs, library logs and job accounting date. Sequence checks and check digits are data validation edits, and source documentation retention is an example of a data file control.

87. The lack of adequate security controls represents a(n):

A. threat.

B. asset.

C. impact.

D. vulnerability

The correct answer is: D. vulnerability.

Explanation: The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers, resulting in loss of sensitive information, which could lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the “Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.” The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

88. IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedures.

B. best IT security control practices relevant to a specific entity.

C. techniques for securing information.

D. security policy.

The correct answer is: A. desired result or purpose of implementing specific control procedures.

Explanation: An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

89. To support an organization's goals, the IS department should have:

A. a low-cost philosophy.

B. long- and short-range plans.

C. leading-edge technology.

D. planned to acquire new hardware and software.

The correct answer is: B. long- and short-range plans.

Explanation: To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

90. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information

B. information security is not critical to all functions.

C. IS audit should provide security training to the employees.

D. the audit finding will cause management to provide continuous training to staff.

The correct answer is: A. this lack of knowledge may lead to unintentional disclosure of sensitive information

Explanation: All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

91. The general ledger setup function in an enterprise resource planning (ERP) system allows for setting accounting periods. Access to this function has been permitted to users in finance, the warehouse and order entry. The MOST likely reason for such broad access is the:

    A. need to change accounting periods on a regular basis.

    B. requirement to post entries for a closed accounting period.

    C. lack of policies and procedures for the proper segregation of duties.

    D. need to create/modify the chart of accounts and its allocations.

    The correct answer is: C. lack of policies and procedures for the proper segregation of duties.

    Explanation: Setting of accounting periods is one of the critical activities of the finance function. Granting access to this function to warehouse and order entry personnel could be a result of a lack of proper policies and procedures for the adequate segregation of duties. Accounting periods should not be changed at regular intervals, but established permanently. The requirement to post entries for a closed accounting period is a risk. If necessary, this should be done by someone in the finance or accounting area. The need to create/modify the chart of accounts and its allocations is the responsibility of the finance department and is not a function that should be performed by warehouse or order entry personnel.

92. A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

    A. recovery.

    B. retention.

    C. rebuilding.

    D. reuse.

    The correct answer is: B. retention.

    Explanation: Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic "paper" makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

93. A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organization.

B. that they are implemented as a part of risk assessment.

C. compliance with all policies.

D. that they are reviewed periodically.

The correct answer is: A. that they are consistent across the organization.

Explanation: Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

94. The following is an advantage of using link encryption:

A. it protects messages against traffic analysis

B. Even if an intermediate node in the network is broken into, the traffic passing through that node does not get exposed

C. If an encryption key is compromised the exposure is restricted to a single user to who the key applies

D. It is easy to assign the cost of using link encryption to the users of the link.

The correct answer is: A. it protects messages against traffic analysis

Explanation: Link Encryption results in protection against traffic analysis. Options B, C and D are not applicable.

95. A probable advantage to an organization that has outsourced its data processing services is that:

A. needed IS expertise can be obtained from the outside.

B. greater control can be exercised over processing.

C. processing priorities can be established and enforced internally.

D. greater user involvement is required to communicate user needs.

The correct answer is: A. needed IS expertise can be obtained from the outside.

Explanation: Outsourcing is a contractual arrangement whereby the organization relinquishes control over part or all of the information processing to an external party. This is frequently done to acquire additional resources or expertise that is not obtainable from inside the organization.

96. When an organization is outsourcing their information security function, which of the following should be kept in the organization?

    A. Accountability for the corporate security policy

    B. Defining the corporate security policy

    C. Implementing the corporate security policy

    D. Defining security procedures and guidelines

    The correct answer is: A. Accountability for the corporate security policy

    Explanation: Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

97. When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

    A. Restricting physical access to computing equipment

    B. Reviewing transaction and application logs

    C. Performing background checks prior to hiring IT staff

    D. Locking user sessions after a specified period of inactivity

    The correct answer is: B. Reviewing transaction and application logs

    Explanation: Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue with a lack of segregation of duties is more the misuse (deliberately or inadvertently) of access privileges that have officially been granted.

98. Which of the following reduces the potential impact of social engineering attacks?

    A. Compliance with regulatory requirements

    B. Promoting ethical understanding

    C. Security awareness programs

    D. Effective performance incentives

    The correct answer is: C. Security awareness programs

Explanation: Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

99. An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.

B. inadequate succession planning.

C. one person knowing all parts of a system.

D. a disruption of operations.

The correct answer is: C. one person knowing all parts of a system.

Explanation: Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

100. When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question with regards to the legal jurisdiction.

B. Having a provider abroad will cause excessive costs in future audits.

C. The auditing process will be difficult because of the distances.

D. There could be different auditing norms.

The correct answer is: A. There could be a question with regards to the legal jurisdiction.

Explanation: In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

101. Which of the following is critical to the selection and acquisition of the correct operating system software?

A. Competitive bids

B. User department approval

C. Hardware configuration analysis

D. Purchasing department approval

The correct answer is: C. Hardware configuration analysis

Explanation: The purchase of operating system software is dependent on the fact that the software is compatible with the existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

102. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

A. Encrypting the hash of the payment instruction with the public key of the financial institution

B. Affixing a time stamp to the instruction and using it to check for duplicate payments

C. Encrypting the hash of the payment instruction with the private key of the instructor

D. Affixing a time stamp to the hash of the instruction before having it digitally signed by the instructor

The correct answer is: B. Affixing a time stamp to the instruction and using it to check for duplicate payments

Explanation: Affixing a time stamp to the instruction and using it to check for duplicate payments makes the instruction unique. The financial institution can check that the instruction was not intercepted and replayed, and thus, it could prevent crediting the account three times. Encrypting the hash of the payment instruction with the public key of the financial institution does not protect replay, it only protects confidentiality and integrity of the instruction. Encrypting the hash of the payment instruction with the private key of the instructor ensures integrity of the instruction and non-repudiation of the issued instruction. The process of creating a message digest requires applying a cryptographic hashing algorithm to the entire message. The receiver, upon decrypting the message digest, will recompute the hash using the same hashing algorithm and compare the result with what was sent. Hence, affixing a time stamp into the hash of the instruction before being digitally signed by the instructor would violate the integrity requirements of a digital signature.

103. Assumptions while planning an IS project involve a high degree of risk because they are:

A. based on known constraints.

B. based on objective past data.

C. a result of a lack of information.

D. often made by unqualified people.

The correct answer is: C. a result of a lack of information.

Explanation: Assumptions are made when adequate information is not available. When an IS project manager makes an assumption, there is a high degree of risk because the lack of proper information can cause unexpected loss to an IS project. Assumptions are not based on "known" constraints. When constraints are known in advance, a project manager can plan according to those constraints rather than assuming the constraints will not affect the project. Having objective data about past IS projects will not lead to making assumptions, but rather helps the IS project manager in planning the project. Hence, if objective past data are available and the project manager makes use of them, the risk to the project is less. Regardless of whether they are made by qualified people or unqualified people, assumptions are risky.

104. An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.

B. prototyping.

C. software reuse.

D. reengineering.

The correct answer is: D. reengineering.

Explanation: Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

105. When implementing an acquired system in a client-server environment, which of the following tests would confirm that the modifications in the Windows registry do not adversely impact the desktop environment?

A. Sociability testing

B. Parallel testing

C. White box testing

D. Validation testing

The correct answer is: A. Sociability testing

Explanation: When implementing an acquired system in an client-server environment, sociability testing would confirm that the system can operate in the target environment without adversely impacting other systems. Parallel testing is the process of feeding test data to the old and new systems and comparing the results. White box testing is based on a close examination of procedural details, and validation testing tests the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

106. Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.

B. transaction journal.

C. automated suspense file listing.

D. user error report.

The correct answer is: B. transaction journal.

Explanation: The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, and the user error report would only list input that resulted in an edit error.

107. The IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could the IS auditor use to estimate the size of the development effort?

A. Program evaluation review technique (PERT)

B. Counting source lines of code (SLOC)

C. Function point analysis

D. White box testing

The correct answer is: C. Function point analysis

Explanation: Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is

useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

108. The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.

B. central processing site during the running of the application system.

C. remote processing site after transmission of the data to the central processing site.

D. remote processing site prior to transmission of the data to the central processing site.

The correct answer is: D. remote processing site prior to transmission of the data to the central processing site.

Explanation: It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

109. Which of the following is the FIRST thing an IS auditor should do after the discovery of a Trojan horse program in a computer system?

A. Investigate the author.

B. Remove any underlying threats.

C. Establish compensating controls.

D. Have the offending code removed.

The correct answer is: D. Have the offending code removed.

Explanation: The IS auditor's first duty is to prevent the Trojan horse from causing further damage. After removing the offending code, follow up actions would include investigation and recommendations (choices B and C).

110. The GREATEST benefit in implementing an expert system is the:

A. capturing of the knowledge and experience of individuals in an organization.

B. sharing of knowledge in a central repository.

C. enhancement of personnel productivity and performance.

D. reduction of employee turnover in key departments.

The correct answer is: A. capturing of the knowledge and experience of individuals in an organization.

Explanation: The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

111. An IS auditor reviewing a proposed application software acquisition should ensure that the:

A. operating system (OS) being used is compatible with the existing hardware platform.

B. planned OS updates have been scheduled to minimize negative impacts on company needs.

C. OS has the latest versions and updates.

D. products are compatible with the current or planned OS.

The correct answer is: D. products are compatible with the current or planned OS.

Explanation: Choices A, B and C are incorrect because none of them is related to the area being audited. In reviewing the proposed application the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not, it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

112. Which of the following is MOST likely to occur when a system development project is in the middle of the programming/coding phase?

A. Unit tests

B. Stress tests

C. Regression tests

D. Acceptance tests

The correct answer is: A. Unit tests

Explanation: During the programming phase, the development team should have mechanisms in place to ensure that coding is being developed to standard and is working correctly. Unit tests are key elements of that process in that they ensure that individual

programs are working correctly. They would normally be supported by code reviews. Stress tests, regression tests and acceptance tests would normally occur later in the development and testing phases. As part of the process of assessing compliance with quality processes, IS auditors should verify that such reviews are undertaken.

113. An organization planning to purchase a software package asks the IS auditor for a risk assessment. Which of the following is the MAJOR risk?

A. Unavailability of the source code

B. Lack of a vendor-quality certification

C. Absence of vendor/client references

D. Little vendor experience with the package

The correct answer is: A. Unavailability of the source code

Explanation: If the vendor goes out of business, not having the source code available would make it impossible to update the (software) package. Lack of a vendor-quality certification, absence of vendor/client references and little vendor experience with the package are important issues but not critical.

114. An IS auditor assigned to audit a reorganized process should FIRST review which of the following?

A. A map of existing controls

B. Eliminated controls

C. Process charts

D. Compensating controls

The correct answer is: C. Process charts

Explanation: To ensure adequate control over the business process, the auditor should first review the flow charts showing the before and after processes. The process charts aid in analyzing the changes in the processes. The other choices—analyzing eliminated controls, ensuring that compensating controls are in place and analyzing the existing controls—are incorrect as each, performed individually, would not be as effective and all-encompassing as reviewing the process charts.

115. The PRIMARY benefit of integrating total quality management (TQM) into a software development project is:

A. comprehensive documentation.

B. on-time delivery.

C. cost control.

D. end-user satisfaction.

The correct answer is: D. end-user satisfaction.

Explanation: Quality is ultimately a measure of end-user satisfaction. If the end user is not satisfied, then the product was not properly developed. Comprehensive documentation, on-time delivery and costs are all secondary to end-user satisfaction.

116. When reviewing the quality of an IS department's development process, the IS auditor finds that he/she does not use any formal, documented methodology and standards. The IS auditor's MOST appropriate action would be to:

A. complete the audit and report the finding.

B. investigate and recommend appropriate formal standards.

C. document the informal standards and test for compliance.

D. withdraw and recommend a further audit when standards are implemented.

The correct answer is: C. document the informal standards and test for compliance.

Explanation: The IS auditor's first concern would be to ensure that projects are consistently managed. Where it is claimed that an internal standard exists, it is important to ensure that it is operated correctly, even when this means documenting the claimed standards first. Merely reporting the issue as a weakness and closing the audit without findings would not help the organization in any way and investigating formal methodologies may be unnecessary if the existing, informal standards prove to be adequate and effective.

117. During unit testing, the test strategy applied is:

A. black box.

B. white box.

C. bottom-up.

D. top-down.

The correct answer is: B. white box.

Explanation: White box testing examines the internal structure of a module. A programmer should perform this test for each module prior to integrating the module with others. Black box testing focuses on the functional requirements and does not consider the control structure of the module. Choices C and D are not correct because these tests require that several modules have already been assembled and tested.

118. A decision support system (DSS):

A. is aimed at solving highly structured problems.

B. combines the use of models with nontraditional data access and retrieval functions.

C. emphasizes flexibility in the decision-making approach of users.

D. supports only structured decision-making tasks.

The correct answer is: C. emphasizes flexibility in the decision-making approach of users.

Explanation: DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semistructured decision-making tasks.

119. Which of the following phases represents the optimum point for software baselining to occur?

A. Testing

B. Design

C. Requirement

D. Development

The correct answer is: B. Design

Explanation: Software baselining is the cut-off point in the design and development of an application, beyond which change should not occur without undergoing formal procedures for approval and should be supported by a cost-benefit business impact analysis. The optimum point for software baselining to occur is the design phase.

120. A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, the IS auditor should recommend the inclusion of:

A. validation controls.

B. internal credibility checks.

C. clerical control procedures.

D. automated systems balancing.

The correct answer is: D. automated systems balancing.

Explanation: Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

121. When auditing the conversion of an accounting system an IS auditor should verify the existence of a:

A. control total check.

B. validation check.

C. completeness check.

D. limit check.

The correct answer is: A. control total check.

Explanation: Tallying a control total of all accounts before and after conversion will assure the IS auditor that all amount data has been taken into the new system. Later one-to-one checking by users will assure that all the data has been converted. The other choices are incorrect. Validation checks, completeness checks and limit checks would be applied at the point at which the data are originally entered into the accounting system.

122. A debugging tool, which reports on the sequence of steps executed by a program, is called a(n):

A. output analyzer.

B. memory dump.

C. compiler.

D. logic path monitor.

The correct answer is: D. logic path monitor.

Explanation: Logic path monitors report on the sequence of steps executed by a program. This provides the programmer with clues to logic errors, if any, in the program. An output analyzer checks the results of a program for accuracy by comparing the expected results with the actual results. A memory dump provides a picture of the content of a computer's internal memory at any point in time, often when the program is aborted, thus providing information on inconsistencies in data or parameter values. Though compilers have some potential to provide feedback to a programmer, they are not generally considered a debugging tool.

123. Which of the following facilitates program maintenance?

A. More cohesive and loosely coupled programs

B. Less cohesive and loosely coupled programs

C. More cohesive and strongly coupled programs

D. Less cohesive and strongly coupled programs

The correct answer is: A. More cohesive and loosely coupled programs

Explanation: Cohesion refers to the performance of a single, dedicated function by each program. Coupling refers to the independence of the comparable units. Loosely coupled units, when the program code is changed, will reduce the probability of affecting other program units. More cohesive and loosely coupled units are best for maintenance.

124. Which of the following ensures completeness and accuracy of accumulated data?

A. Processing control procedures

B. Data file control procedures

C. Output controls

D. Application controls

The correct answer is: A. Processing control procedures

Explanation: Processing controls ensure the completeness and accuracy of accumulated data, for example, editing and run-to-run totals. Data file control procedures ensure that only authorized processing occurs to stored data, for example, transaction logs. Output controls ensure that data delivered to users will be presented, formatted and delivered in a consistent and secure manner, for example, using report distribution. "Application controls" is a general term comprising all kinds of controls used in an application.

125. The MAJOR concern for an IS auditor reviewing a CASE environment should be that the use of CASE does not automatically:

A. result in a correct capture of requirements.

B. ensure that desirable application controls have been implemented.

C. produce ergonomic and user-friendly interfaces.

D. generate efficient code.

The correct answer is: A. result in a correct capture of requirements.

Explanation: The principal concern should be to ensure an alignment of the application with business needs and user requirements. While the CASE being used may provide tools to cover this crucial initial phase, a cooperative user-analyst interaction is always needed. Choice B should be the next concern. If the system meets business needs and user requirements, it should also incorporate all desirable controls. Controls have to be specified since CASE can only automatically incorporate certain, rather low-level, controls (such as type of input data, e.g., date, expected). CASE will not (choice C) automatically generate ergonomic and user-friendly interfaces, but it should provide tools for easy (and automatically documented) tuning. CASE applications (choice D) generally come short of optimizing the use of hardware and software resources, precisely because they are designed to optimize other elements, such as developers' effort or documentation.

126. The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the server.

B. the server does not run the program and the output is not sent over the network.

C. they improve the performance of the web server and network.

D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

The correct answer is: C. they improve the performance of the web server and network.

Explanation: An applet is a JAVA program that is sent over the network from the web server, through a web browser, to the client machine. Then the code is run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network, over which the server and client are connected, drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

127. Ideally, stress testing should be carried out in a:

A. test environment using test data.

B. production environment using live workloads.

C. test environment using live workloads.

D. production environment using test data.

The correct answer is: C. test environment using live workloads.

Explanation: Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

128. Good quality software is BEST achieved:

A. through thorough testing.

B. by finding and quickly correcting programming errors.

C. by determining the amount of testing using the available time and budget.

D. by applying well-defined processes and structured reviews throughout the project.

The correct answer is: D. by applying well-defined processes and structured reviews throughout the project.

Explanation: Testing can point to quality deficiencies, However, it cannot by itself fix them. Corrective action at this point in the project is expensive. While it is necessary to detect and correct program errors, the bigger return comes from detecting defects as they occur in upstream phases, such as requirements and design. Choice C is representative of the most common mistake when applying quality management to a software project. It is seen as overhead, instead early removal of defects has a substantial payback. Rework is actually the largest cost driver on most software projects. Choice D represents the core of achieving quality, that is, following a well-defined, consistent process and effectively reviewing key deliverables.

129. A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be the IS auditor's main concern about the new process?

A. Are key controls in place to protect assets and information resources?

B. Does it address the corporate customer requirements?

C. Does the system meet the performance goals (time and resources)?

D. Have owners been identified who will be responsible for the process?

The correct answer is: A. Are key controls in place to protect assets and information resources?

Explanation: The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the BPR process should achieve, but they are not the auditor's primary concern.

130. A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house-developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.

B. A quality plan is not part of the contracted deliverables.

C. Not all business functions will be available on initial implementation.

D. Prototyping is being used to confirm that the system meets business requirements.

The correct answer is: B. A quality plan is not part of the contracted deliverables.

Explanation: A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed

development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

131. The use of a GANTT chart can:

A. aid in scheduling project tasks.

B. determine project checkpoints.

C. ensure documentation standards.

D. direct the post implementation review.

The correct answer is: A. aid in scheduling project tasks.

Explanation: A GANTT chart is used in project control. It may aid in the identification of needed checkpoints, but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post implementation review.

132. Using test data as part of a comprehensive test of program controls in a continuous online manner is called a(n):

A. test data/deck.

B. base-case system evaluation.

C. integrated test facility (ITF).

D. parallel simulation.

The correct answer is: B. base-case system evaluation.

Explanation: A base-case system evaluation uses test data sets developed as part of comprehensive testing programs. It is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

133. Testing the connection of two or more system components that pass information from one area to another is:

A. pilot testing.

B. parallel testing

C. interface testing.

D. regression testing.

The correct answer is: C. interface testing.

Explanation: Interface testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. Pilot testing is a preliminary test that focuses on specific and predetermined aspects of a system and is not meant to replace other methods. Parallel testing is the process of feeding test data into two systems—the modified system and an alternative system—and comparing the results. Regression testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing is the same as the data used in the original test.

134. Regression testing is the process of testing a program to determine if:

A. the new code contains errors.

B. discrepancies exist between functional specifications and performance.

C. new requirements have been met.

D. changes have introduced any errors in the unchanged code.

The correct answer is: D. changes have introduced any errors in the unchanged code.

Explanation: Regression testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing is used to determine if a new code contains errors or does not meet requirements.

135. Which of the following groups/individuals should assume overall direction and responsibility for costs and timetables of system development projects?

A. User management

B. Project steering committee

C. Senior management

D. Systems development management

The correct answer is: B. Project steering committee

Explanation: The project steering committee is ultimately responsible for all costs and timetables. User management assumes ownership of the project and the resulting system. Senior management commits to the project and approves the resources necessary to complete the project. System development management provides technical support for the hardware and software environments by developing, installing and operating the requested system.

136. The difference between white box testing and black box testing is that white box testing:

A. involves the IS auditor.

B. is performed by an independent programmer team.

C. examines a program's internal logical structure.

D. uses the bottom-up approach.

The correct answer is: C. examines a program's internal logical structure.

Explanation: Black box testing observes a system's external behavior, while white box testing is a detailed exam of a logical path, checking the possible conditions. The IS auditor need not be involved in either testing method. The bottom-up approach can be used in both tests. White box testing requires knowledge of the internals of the program or the module to be implemented/tested. Black box testing requires that the functionality of the program be known. The independent programmer team would not be aware of the application of a program in which they have not been involved; hence, the independent programmer team cannot provide any assistance in either of these testing approaches.

137. An IS auditor reviewing a project, where quality is a major concern, should use the project management triangle to explain that a(n):

A. increase in quality can be achieved, even if resource allocation is decreased.

B. increase in quality is only achieved, if resource allocation is increased.

C. decrease in delivery time can be achieved, even if resource allocation is decreased.

D. decrease in delivery time can only be achieved, if quality is decreased.

The correct answer is: A. increase in quality can be achieved, even if resource allocation is decreased.

Explanation: The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

138. Which of the following integrity tests examines the accuracy, completeness, consistency and authorization of data?

A. Data

B. Relational

C. Domain

D. Referential

The correct answer is: A. Data

Explanation: Data integrity testing examines the accuracy, completeness, consistency and authorization of data. Relational integrity testing detects modification to sensitive data by the use of control totals. Domain integrity testing verifies that data conforms to specifications. Referential integrity testing ensures that data exists in its parent or original file before it exists in the child or another file.

139. Which of the following is MOST effective in controlling application maintenance?

A. Informing users of the status of changes

B. Establishing priorities on program changes

C. Obtaining user approval of program changes

D. Requiring documented user specifications for changes

The correct answer is: C. Obtaining user approval of program changes

Explanation: User approvals of program changes will ensure that changes are correct as specified by the user and that they are authorized. Therefore, erroneous or unauthorized changes are less likely to occur, minimizing system downtime and errors.

140. Which of the following groups should assume ownership of a systems development project and the resulting system?

A. User management

B. Senior management

C. Project steering committee

D. Systems development management

The correct answer is: A. User management

Explanation: User management assumes ownership of the project and resulting system. They should review and approve deliverables as they are defined and accomplished. Senior management approves the project and the resources needed to complete it. The project steering committee provides overall direction and is responsible for monitoring costs and timetables. Systems development management provides technical support.

141. To make an electronic funds transfer (EFT), one employee enters the amount field and another employee reenters the same data again, before the money is transferred. The control adopted by the organization in this case is:

A. sequence check.

B. key verification.

C. check digit.

D. completeness check.

The correct answer is: B. key verification.

Explanation: Key verification is a process in which keying-in is repeated by a separate individual using a machine that compares the original entry to the repeated entry. Sequence check refers to the continuity in serial numbers within the number range on documents. A check digit is a numeric value that has been calculated mathematically and added to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. Completeness checks ensure that all the characters required for a field have been input.

142. An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

A. continuous improvement.

B. quantitative quality goals.

C. a documented process.

D. a process tailored to specific projects.

The correct answer is: A. continuous improvement.

Explanation: An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

143. The use of fourth-generation languages (4GLs) should be weighed carefully against using traditional languages, because 4GLs:

A. can lack the lower-level detail commands necessary to perform data intensive operations.

B. cannot be implemented on both the mainframe processors and microcomputers.

C. generally contain complex language subsets that must be used by skilled users.

D. cannot access database records and produce complex online outputs.

The correct answer is: A. can lack the lower-level detail commands necessary to perform data intensive operations.

Explanation: All of the answers are advantages of using 4GLs except that they can lack the lower-level detail commands necessary to perform data intensive operations. These operations are usually required when developing major applications.

144. During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

A. increased maintenance.

B. improper documentation of testing.

C. inadequate functional testing.

D. delays in problem resolution.

The correct answer is: C. inadequate functional testing.

Explanation: The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B and D are not as important.

145. An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. a backup server be available to run ETCS operations with up-to-date data.

B. a backup server be loaded with all the relevant software and data.

C. the systems staff of the organization be trained to handle any event.

D. source code of the ETCS application be placed in escrow.

The correct answer is: D. source code of the ETCS application be placed in escrow.

Explanation: Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business. Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

146. Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Black box test

B. Desk checking

C. Structured walk-through

D. Design and code

The correct answer is: A. Black box test

Explanation: A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as

a single unit/entity consisting of numerous modules, and second with the user data that flows across software modules. In some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and somebody closely examines it by applying his/her mind, without actually activating the software. Hence, these cannot be referred to as dynamic analysis tools.

147. The impact of EDI on internal controls will be:

A. that fewer opportunities for review and authorization will exist.

B. an inherent authentication.

C. a proper distribution of EDI transactions while in the possession of third parties.

D. that IPF management will have increased responsibilities over data center controls.

The correct answer is: A. that fewer opportunities for review and authorization will exist.

Explanation: EDI promotes a more efficient paperless environment, but at the same time, less human intervention makes it more difficult for reviewing and authorizing. Choice B is incorrect; since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and does not include any distinguishing human element or signature. Choice C is incorrect because this is a security risk associated with EDI. Choice D is incorrect because there are relatively few, if any, additional data center controls associated with the implementation of EDI applications. Instead, more control will need to be exercised by the user's application system to replace manual controls, such as site reviews of documents. More emphasis will need to be placed on control over data transmission (network management controls).

148. Which of the following tasks occurs during the research stage of the benchmarking process?

A. Critical processes are identified.

B. Benchmarking partners are visited.

C. Findings are translated into core principles.

D. Benchmarking partners are identified.

The correct answer is: D. Benchmarking partners are identified.

Explanation: During the research stage, the team collects data and identifies the benchmarking partners. In the planning stage, the team identifies the critical processes to be benchmarked. Visiting the benchmarking partners is performed in the observation stage. Translating the findings into core principles is performed during the adaptation stage.

149. Which of the following would be a risk specifically associated with the agile development process?

A. Lack of documentation

B. Lack of testing

C. Poor requirements definition

D. Poor project management practices

The correct answer is: A. Lack of documentation

Explanation: Agile development relies on knowledge held by people within the organization, as opposed to external knowledge. The main issue is the necessity for providing compensating controls to ensure that changes and enhancements to the system can be made later on, even if the key personnel who know the implemented business logic leave the company. Lack of testing might be an issue but without formal documentation it is difficult for an auditor to gather objective evidence. Rapid response to changing requirements is one strength of the agile development processes. Replanning the project at the end of each iteration, including reprioritizing requirements, identifying any new requirements and determining in which release delivered functionality is to be implemented, is a main aspect of the agile process. Applied project management practices are slightly different than those required for traditional methods of software development. The project manager's role. This role shifts from one primarily concerned with planning the project, allocating tasks and monitoring progress, to that of a facilitator and advocate. Responsibility for planning and control shifts to the team members.

150. An IS auditor evaluating data integrity in a transaction-driven system environment should review atomicity to determine whether:

A. the database survives failures (hardware or software).

B. each transaction is separated from other transactions.

C. integrity conditions are maintained.

D. a transaction is completed or a database is updated.

The correct answer is: D. a transaction is completed or a database is updated.

Explanation: This concept is included in the atomicity, completeness, isolation and durability (ACID) principle. Durability means that the database survives failures (hardware or software). Isolation means that each transaction is separated from other transactions. Consistency means that integrity conditions are maintained.

151. The MOST effective method of preventing unauthorized use of data files is:

A. automated file entry.

B. tape librarian.

C. access control software.

D. locked library.

The correct answer is: C. access control software.

Explanation: Access control software is an active control designed to prevent unauthorized access to data.

152. Which of the following should be verified by an IS auditor reviewing a Business Continuity Plan?

A. Approval of the plan by Board of Directors.

B. Plan is tested once in a year.

C. Plan is reviewed and updated regularly.

D. Plan is circulated to all the Head of Departments

The correct answer is: C. Plan is reviewed and updated regularly.

Explanation: Business Continuity Plan should be reviewed regularly. Options A, B and D are not that relavant.

153. Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

A. Registration authority

B. Certificate authority (CA)

C. Certification relocation list

D. Certification practice statement

The correct answer is: B. Certificate authority (CA)

Explanation: The certificate authority maintains a directory of digital certificates for the reference of those receiving them. It manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

154. Passwords should be:

A. assigned by the security administrator for first time logon.

B. changed every 30 days at the discretion of the user.

C. reused often to ensure the user does not forget the password.

D. displayed on the screen so that the user can ensure that it has been entered properly.

The correct answer is: A. assigned by the security administrator for first time logon.

Explanation: Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again; old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

155. An IS auditor reviewing an organisation's Business Continuity Plan discovered that the plan provides for an alternate site which can accommodate about 50% of the processing requirements of the organisation. Which of the following steps should the IS Auditor take?

A. Ensure that the alternate site could process all the critical applications.

B. Recommend that the processing capacity of the alternate site should be increased.

C. Identify applications that could be processed at the alternate site and develop manual procedures for other applications.

D. Under normal circumstances only about 25% of the processing is critical to an organization. Hence, there is no need to take any action.

The correct answer is: A. Ensure that the alternate site could process all the critical applications.

Explanation: In given context important is to take care of critical applications hence Option A is correct. Option B, C and D are not that relevant.

156. The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

A. make unauthorized changes to the database directly, without an audit trail.

B. make use of a system query language (SQL) to access information.

C. remotely access the database.

D. update data without authentication.

The correct answer is: A. make unauthorized changes to the database directly, without an audit trail.

Explanation: Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information. In a networked environment, accessing the database remotely does not make a difference. What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user id.

157. Which of the following antispam filtering techniques would BEST prevent a valid, variable-length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

A. Heuristic (rule-based)

B. Signature-based

C. Pattern matching

D. Bayesian (statistical)

The correct answer is: D. Bayesian (statistical)

Explanation: Bayesian filtering applies statistical modeling to messages, by performing a frequency analysis on each word within the message and then evaluating the message as whole. Hence, it can "ignore" a suspicious keyword, if the entire message is within normal bounds. Heuristic filtering is less effective, since new "exception" rules may need to be defined when a valid message is labeled as spam. Signature-based filtering is useless against variable-length messages, because the calculated MD5 hash changes all the time. Finally, pattern matching is actually a degraded rule-based technique, where the rules operate at the word level, using wildcards, and not at higher levels.

158. An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?

A. Kerberos

B. Vitality detection

C. Multimodal biometrics

D. Before-image/after-image logging

The correct answer is: A. Kerberos

Explanation: Kerberos is a network authentication protocol for client-server applications that can be used to restrict access to the database to authorized users. Choices B and C are not correct because vitality detection and multimodal biometrics are controls against spoofing and mimicry attacks. Before-image/after-image logging of database transactions is a detective control, as opposed to Kerberos, which is a preventative control.

159. Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

A. Analyzer

B. Administration console

C. User interface

D. Sensor

The correct answer is: D. Sensor

Explanation: Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

160. The risk of gaining unauthorized access through social engineering can BEST be addressed by:

A. security awareness programs.

B. asymmetric encryption.

C. intrusion detection systems.

D. a demilitarized zone.

The correct answer is: A. security awareness programs.

Explanation: The human factor is the weakest link in the information security chain. Social engineering is the human side of breaking into an enterprise's network. It relies on interpersonal relations and deception. Organizations with technical security countermeasures, such as an authentication process, encryption, intrusion detection systems or firewalls, may still be vulnerable if an employee gives away confidential information. The best means of defense for social engineering is an ongoing security awareness program wherein all employees are educated about the dangers of social engineering.

161. While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

A. A scan of all floppy disks before use

B. A virus monitor on the network file server

C. Scheduled daily scans of all network drives

D. A virus monitor on the user's personal computer

The correct answer is: C. Scheduled daily scans of all network drives

Explanation: Scheduled daily scans of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

162. The creation of an electronic signature:

A. encrypts the message.

B. verifies from where the message came.

C. cannot be compromised when using a private key.

D. cannot be used with e-mail systems.

The correct answer is: B. verifies from where the message came.

Explanation: The creation of an electronic signature does not in itself encrypt the message or secure it from compromise. It only verifies the message's origination.

163. The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

A. Relocate the shutoff switch.

B. Install protective covers.

C. Escort visitors.

D. Log environmental failures.

The correct answer is: B. Install protective covers.

Explanation: A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation. Relocating the shutoff switch would defeat the purpose of having it readily accessible. Escorting the personnel who move the equipment may not have prevented this incident, and logging of environmental failures would provide management with a report of incidents, but reporting alone would not prevent a reoccurrence.

164. Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy

B. Access control lists

C. Password management

D. System configuration files

The correct answer is: A. Information systems security policy

Explanation: The information systems security policy developed and approved by the top management in an organization is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are tools for implementing the access controls.

165. Which of the following provides nonrepudiation services for e-commerce transactions?

A. Public key infrastructure (PKI)

B. Data Encryption Standard (DES)

C. Message authentication code (MAC)

D. Personal identification number (PIN)

The correct answer is: A. Public key infrastructure (PKI)

Explanation: PKI is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it, it is capable of verification, it is under the sole control of the person using it, and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address non-repudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission. It has nothing to do with non-repudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

166. The BEST overall quantitative measure of the performance of biometric control devices is:

A. false-rejection rate.

B. false-acceptance rate.

C. equal-error rate.

D. estimated-error rate.

The correct answer is: C. equal-error rate.

Explanation: A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EER is the measure of the more effective biometrics control device. Low false-rejection rates or low

false-acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is non-existing and hence irrelevant.

167. Active radio frequency ID (RFID) tags are subject to which of the following exposures?

A. Session hijacking

B. Eavesdropping

C. Malicious code

D. Phishing

The correct answer is: B. Eavesdropping

Explanation: Like wireless devices, active RFID tags are subject to eavesdropping. They are by nature not subject to session hijacking, malicious code or phishing.

168. Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic

B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic

C. Having no physical signs on the outside of a computer center building

D. Using two firewalls in parallel to check different types of incoming traffic

The correct answer is: B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic

Explanation: Defense in-depth means using different security mechanisms that back up each other. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

169. Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access

B. Excessive CPU cycle usage

C. Lockout of terminal polling

D. Multiplexor control dysfunction

The correct answer is: A. Unauthorized data access

Explanation: Line grabbing will enable eavesdropping, thus allowing unauthorized data access. It will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

170. When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

A. Read access to data

B. Delete access to transaction data files

C. Logged read/execute access to programs

D. Update access to job control language/script files

The correct answer is: B. Delete access to transaction data files

Explanation: Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to control job execution.

171. A certificate authority (CA) can delegate the processes of:

A. revocation and suspension of a subscriber's certificate.

B. generation and distribution of the CA public key.

C. establishing a link between the requesting entity and its public key.

D. issuing and distributing subscriber certificates.

The correct answer is: C. establishing a link between the requesting entity and its public key.

Explanation: Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform. Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

172. Use of asymmetric encryption in an Internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

A. customer over the authenticity of the hosting organization.

B. hosting organization over the authenticity of the customer.

C. customer over the confidentiality of messages from the hosting organization.

D. hosting organization over the confidentiality of messages passed to the customer.

The correct answer is: A. customer over the authenticity of the hosting organization.

Explanation: Any false site will not be able to encrypt using the private key of the real site, so the customer would not be able to decrypt the message using the public key. Many customers have access to the same public key so the host cannot use this mechanism to ensure the authenticity of the customer. The customer cannot be assured of the confidentiality of messages from the host as many people have access to the public key and can decrypt the messages from the host. The host cannot be assured of the confidentiality of messages sent out, as many people have access to the public key and can decrypt it.

173. Which of the following is a feature of an intrusion detection system (IDS)?

A. Gathering evidence on attack attempts

B. Identifying weaknesses in the policy definition

C. Blocking access to particular sites on the Internet

D. Preventing certain users from accessing specific servers

The correct answer is: A. Gathering evidence on attack attempts

Explanation: An IDS can gather evidence on intrusive activity such as an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, and choice B requires a manual review and, therefore, is outside the functionality of an IDS.

174. Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

A. The buyer is assured that neither the merchant nor any other party can misuse his/her credit card data.

B. All personal SET certificates are stored securely in the buyer's computer.

C. The buyer is liable for any transaction involving his/her personal SET certificates.

D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

The correct answer is: C. The buyer is liable for any transaction involving his/her personal SET certificates.

Explanation: The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of his/her personal SET certificates for ecommerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card

number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter his/her credit card data, he/she will have to handle the wallet software.

175. An Internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.

B. cause modification to the contents of certain transactions.

C. be used to gain access to systems containing proprietary information.

D. result in major problems with billing systems and transaction processing agreements.

The correct answer is: C. be used to gain access to systems containing proprietary information.

Explanation: Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

176. Which of the following is the MOST important action in recovering from a cyberattack?

A. Creation of an incident response team

B. Use of cyberforensic investigators

C. Execution of a business continuity plan

D. Filing an insurance claim

The correct answer is: C. Execution of a business continuity plan

Explanation: The most important key step in recovering from cyberattacks is the execution of a business continuity plan to quickly and cost-effectively recover critical systems, processes and data. The incident response team should exist prior to a cyberattack. When a cyberattack is suspected, cyberforensics investigators should be used to set up alarms, catch intruders within the network, and track and trace them over the Internet. After taking the above steps, an organization may have a residual risk that needs to be insured and claimed for traditional and electronic exposures.

177. An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers—one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

A. The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.

B. Both fire suppression systems present a risk of suffocation when used in a closed room.

C. The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).

D. The documentation binders should be removed from the equipment room to reduce potential risks.

The correct answer is: B. Both fire suppression systems present a risk of suffocation when used in a closed room.

Explanation: Protecting people's life should always be of highest priority in fire suppression activities. CO2 and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards. In many countries installing or refilling halon fire suppression systems is not allowed. Although CO2 and halon are effective and appropriate for fires involving synthetic combustibles and electrical equipment, they are nearly totally ineffective on solid combustibles (wood and paper). Although not of highest priority, removal of the documentation would probably reduce some of the risks.

178. With the help of the security officer, granting access to data is the responsibility of:

A. data owners.

B. programmers.

C. system analysts.

D. librarians.

The correct answer is: A. data owners.

Explanation: Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

179. Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

A. Virtual private network

B. Dedicated line

C. Leased line

D. Integrated services digital network

The correct answer is: A. Virtual private network

Explanation: The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the Internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small to medium-sized organizations.

180. Which of the following results in a denial-of-service attack?

A. Brute-force attack

B. Ping of death

C. Leapfrog attack

D. Negative acknowledgement (NAK) attack

The correct answer is: B. Ping of death

Explanation: The use of Ping with a packet size higher than 65 KB and no fragmentation flag on will cause a denial of service. A brute-force attack is typically a text attack that exhausts all possible key combinations. A leapfrog attack, the act of telneting through one or more hosts to preclude a trace, makes use of user id and password information obtained illicitly from one host to compromise another host. A negative acknowledgement attack is a penetration technique that Capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

181. Which of the following is an advantage of elliptic curve encryption over RSA encryption?

A. Computation speed

B. Ability to support digital signatures

C. Simpler key distribution

D. Greater strength for a given key length

The correct answer is: A. Computation speed

Explanation: The main advantage of elliptic curve encryption over RSA encryption is its computation speed. This method was developed by Diffie and Martin E. Hellman, who were the first to conceive of the concept of public key encryption. Both encyption methods support digital signatures, are used for public key encryption and distribution, and are of similar strength.

182. In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

A. connectionless integrity.

B. data origin authentication.

C. antireplay service.

D. confidentiality.

The correct answer is: D. confidentiality.

Explanation: Both protocols support choices A, B and C, but only the ESP protocol provides confidentiality via encryption.

183. The security level of a private key system depends on the number of:

A. encryption key bits.

B. messages sent.

C. keys.

D. channels used.

The correct answer is: A. encryption key bits.

Explanation: The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

184. Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based

B. Signature-based

C. Neural network

D. Host-based

The correct answer is: A. Statistical-based

Explanation: A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may include, at times, unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like

a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of an IDS. Either of the three IDSs above may be host- or network-based.

185. Which of the following can consume valuable network bandwidth?

A. Trojan horses

B. Trapdoors

C. Worms

D. Vaccines

The correct answer is: C. Worms

Explanation: Worms are destructive programs that may destroy data or utilize tremendous computer and communication resources. Trojan horses can capture and transmit private information to the attacker's computer. Trapdoors are exits out of an authorized program. Vaccines are programs designed to detect computer viruses.

186. An accuracy measure for a biometric system is:

A. system response time.

B. registration time.

C. input file size.

D. false-acceptance rate.

The correct answer is: D. false-acceptance rate.

Explanation: For a biometric solution three main accuracy measures are used: false-rejection rate (FRR), cross-error rate (CER) and false-acceptance rate (FAR). FRR is a measure of how often valid individuals are rejected. FAR is a measure of how often invalid individuals are accepted. CER is a measure of when the false-rejection rate equals the false-acceptance rate. Choices A and B are performance measures.

187. Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

A. Overwriting the tapes

B. Initializing the tape labels

C. Degaussing the tapes

D. Erasing the tapes

The correct answer is: C. Degaussing the tapes

Explanation: The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the

tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

188. What is a risk associated with attempting to control physical access to sensitive areas, such as computer rooms, using card keys or locks?

A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.

B. The contingency plan for the organization cannot effectively test controlled access practices.

C. Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.

D. Removing access for those who are no longer authorized is complex.

The correct answer is: A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.

Explanation: The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated. Regarding choice D, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

189. Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the Internet?

A. Customers are widely dispersed geographically, but the certificate authorities are not.

B Customers can make their transactions from any computer or mobile device.

C The certificate authority has several data processing sub centers to administer certificates.

D. The organization is the owner of the certificate authority.

The correct answer is: D. The organization is the owner of the certificate authority.

Explanation: If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, he/she could allege that because of the shared interests an unlawful agreement exists between the parties generating the certificates. If a customer wanted to repudiate a transaction, he/she could argue that there exists a bribery between the parties to generate the certificates, as there exist shared interests. The other options are not weaknesses.

190. An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures

B. Hashing

C. Parsing

D. Steganography

The correct answer is: D. Steganography

Explanation: Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and it is widely applied in the design of programming languages or in data entry editing.

191. Which of the following cryptography options would increase overhead/cost?

A. The encryption is symmetric rather than asymmetric.

B. A long asymmetric encryption key is used.

C. The hash is encrypted rather than the message.

D. A secret key is used.

The correct answer is: B. A long asymmetric encryption key is used.

Explanation: Computer processing time is increased for longer asymmetric encryption keys, and the increase may be disproportionate. For example, one benchmark showed that doubling the length of an RSA key from 512 bits to 1,024 bits caused the decrypt time to increase nearly six-fold. An asymmetric algorithm requires more processing time than symmetric algorithms. A hash is shorter than the original message; hence, a smaller overhead is required if the hash is encrypted rather than the message. Use of a secret key, as a symmetric encryption key, is generally small and used for the purpose of encrypting user data.

192. To determine who has been given permission to use a particular system resource, the IS auditor should review?

A. Activity lists

B. Access control lists

C. Logon ID lists

D. Password lists

The correct answer is: B. Access control lists

Explanation: Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

193. When using public key encryption to secure data being transmitted across a network:

A. both the key used to encrypt and decrypt the data are public.

B. the key used to encrypt is private, but the key used to decrypt the data is public.

C. the key used to encrypt is public, but the key used to decrypt the data is private.

D. both the key used to encrypt and decrypt the data are private.

The correct answer is: C. the key used to encrypt is public, but the key used to decrypt the data is private.

Explanation: Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

194. When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

A. Number of nonthreatening events identified as threatening

B. Attacks not being identified by the system

C. Reports/logs being produced by an automated tool

D. Legitimate traffic being blocked by the system

The correct answer is: B. Attacks not being identified by the system

Explanation: Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem, and an IDS does not block any traffic.

195. Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

A. The organization does not have control over encryption.

B. Messages are subjected to wire tapping.

C. Data might not reach the intended recipient.

D. The communication may not be secure.

The correct answer is: A. The organization does not have control over encryption.

Explanation: The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the datum while it is being transmitted over the Internet. The encryption is done in the background, without any interaction from the user, consequently there is no password to remember either. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data. All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

196. The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.

B. the security administrator has read-only rights to the audit file.

C. date and time stamps are recorded when an action occurs.

D. users can amend audit trail records when correcting system errors.

The correct answer is: D. users can amend audit trail records when correcting system errors.

Explanation: An audit trail is not effective if the details in it can be amended.

197. A malicious code that changes itself with each file it infects is called a:

A. logic bomb.

B. stealth virus.

C. Trojan horse.

D. polymorphic virus.

The correct answer is: D. polymorphic virus.

Explanation: A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify. A logic bomb is code that is hidden in a program or system which will cause something to happen when the user performs a certain action or when certain conditions are met. A logic bomb, which can be downloaded along with a corrupted shareware or freeware program, may destroy data, violate system security or erase the hard drive. A stealth virus is

a virus that hides itself by intercepting disk access requests. When an antivirus program tries to read files or boot sectors to find the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector. A Trojan horse is a virus program that appears to be useful and harmless but which has harmful side effects such as destroying data or breaking the security of the system on which it is run.

198. An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. The IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

A. The new access points with stronger security are affordable.

B. The old access points are poorer in terms of performance.

C. The organization's security would be as strong as its weakest points.

D. The new access points are easier to manage.

The correct answer is: C. The organization's security would be as strong as its weakest points.

Explanation: The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

199. Who is principally responsible for periodically reviewing users' access to systems?

A. Computer operators

B. Security administrators

C. Data owners

D. IS auditors

The correct answer is: C. Data owners

Explanation: The data owners, who are responsible for the use and reporting of information under their control, should provide written authorization for users to gain access to that information. The data owner should periodically review and evaluate authorized (granted) access to ensure these authorizations are still valid.

200. In the ISO/OSI model, which of the following protocols is the FIRST to establish security for the user application?

A. Session layer

B. Transport layer

C. Network layer

D. Presentation layer

The correct answer is: A. Session layer

Explanation: The session layer provides functions that allow two applications to communicate across the network. The functions include security, recognition of names, logons and so on. The session layer is the first layer where security is established for user applications. The transportation layer provides transparent transfer of data between end points. The network layer controls the packet routing and switching within the network, as well as to any other network. The presentation layer provides common communication services, such as encryption, text compression and reformatting.

Mock Assessment Test Paper 2

1. In .....type of communication the router forwards the received packet through only one of its interfaces.

   A. Announcement

   B. multicasting

   C. broadcasting

   D. point to point / Unicast

   A. Announcement is not the precise term that we normally use in networks.

   B. Multicasting is the term used to describe communication where a piece of information is sent from one or more points to a set of other points.

   C. Broadcasting is the term used to describe communication where a piece of information is sent from one point to all other points.

   D. Unicast is the term used to describe communication where a piece of information is sent from one point to another point.

2. Which of the following is not a networking device

   A. Gateways

   B. Linux

   C. Routers

   D. Bridges

   A. Gateway is a network device

   B. Linux is an Operating System and not a network device.

   C. Router is a network device

   D. Beidge is a network device

3. What is the size of MAC address

   A. 16 bits

   B. 48 bits

   C. 64 bits

   D. 32 bits

   A. This is not the correct size of MAC address.

B. MAC addresses are 6-byte (48-bits) in length, and are written in MM:MM:MM:SS:SS:SS format

C. This is not the correct size of MAC address.

D. This is not the correct size of MAC address.

4. Which of the following can be a software:

A. Routers

B. Switches

C. Bridges

D. Firewalls

A. Router is a network device and is a hardware

B. Switch is a network device and is a hardware

C. Bridge is a network device and is a hardware

D. Firewall can be a hardware or software or combination of the two.

5. What is the use of PING command?

A. To test the reachability of a device on a network

B. To test hard disk fault

C. To test a bug in an application

D. To test printer quality

A. Ping command is used to test the reachability of a device on a network

B. Ping command is not used to test had disk fault.

C. Ping command is not used to test a bug in the application

D. Ping command is not used to test the printer quality.

6. Each IP packet must contain

A. Only Source address

B. Only Destination address

C. Source and Destination address

D. Source or Destination address

A. Each IP packet must contain Source and Destination Address; hence this is not a correct answer.

B. Each IP packet must contain Source and Destination Address; hence this is not a correct answer.

C. Each IP packet must contain Source and Destination Address

D. Each IP packet must contain Source and Destination Address; hence this is not a correct answer.

7. Which of the following is correct regarding Class B Address of IP address

A. Network bit – 14, Host bit – 16

B. Network bit – 16, Host bit – 14

C. Network bit – 18, Host bit – 16

D. Network bit – 12, Host bit – 14

*A. In Class B IP Addresses, First two network bits behave like higher significant bits hence, total usable bits from first two network octats would be(8 *2 = 16) -2 = 14. And from Host bits both the octats are available fully. Hence, 8* 2= 16. Hence this is the correct answer.*

B. This is not the correct for Class B IP Addresses

C. This is not the correct for Class B IP Addresses

D. This is not the correct for Class B IP Addresses

8. MAC Address is considered by ____ Layer for Node to Node Data Transmission in the form of Frames.

A. Transport Layer

B. Data Link Layer

C. Application Layer

D. Physical Layer

A. MAC Address is considered by Data Link Layer for Node to Node Data Transmission in the form of frames. At transport layer, 'packets' are the units of transportation.

B. MAC Address is considered by Data Link Layer for Node to Node Data Transmission in the form of frames.

C. MAC Address is considered by Data Link Layer for Node to Node Data Transmission in the form of frames. Application layer performs endpoint sending and receiving of data.

D. MAC Address is considered by Data Link Layer for Node to Node Data Transmission in the form of frames. Physical layer performs actual transmission in the form of bits.

9. How many layers does TCP/IP model has?

   A. 7

   B. 4

   C. 5

   D. 6

   A. OSI Model has 7 layers.

   B. TCP/IP has five layers. Hence this is not the correct answer.

   C. TCP/IP has five layers. – Application, Transport, Network, Data Link, Physical

   D. TCP/IP has five layers. Hence this is not the correct answer.

10. IPv4 Address is:

   A. 32 bits

   B. 64 bits

   C. 128 bits

   D. 8 bits

   *A. IPv4 is made up of four bytes. Hence 4*8 = 32 bits.*

   B. IPv4 is made up of four bytes. Hence 4*8 = 32 bits. Hence, this is not a correct answer.

   C. IPv4 is made up of four bytes. Hence 4*8 = 32 bits. Hence, this is not a correct answer.

   D. IPv4 is made up of four bytes. Hence 4*8 = 32 bits. Hence, this is not a correct answer.

11. Which of the following is NOT a cloud service model:

   A. Infrastructure as a Service

   B. Software as a Service

   C. Platform as a Service

   D. Protocol as a Service

   A. Infrastructure as a Service is one of the cloud service model.

   B. Software as a Service is one of the cloud service model.

C. Platform as a Service is one of the cloud service model.

D. Protocol as a Service is not a cloud service model.

12. Which of the following is NOT a class of IP Address:

A. A

B. B

C. G

D. C

A. There are IP Address classes ranging from A to E. Hence, A is the valid IP Address class.

B. There are IP Address classes ranging from A to E. Hence, B is the valid IP Address class.

C. There are IP Address classes ranging from A to E. Hence, G is not a valid IP Address class.

D. There are IP Address classes ranging from A to E. Hence, C is the valid IP Address class.

13. Which of the following is related to 'Discovery of hidden patterns in the large data to find some valuable information' :

A. Data Mining

B. Data Warehousing

C. Data Mart

D. Database

A. Data Mining refers to 'Discovery of hidden patterns in the large data to find some valuable information'.

B. Data Warehousing refers to central repositories of integrated data from one or more disparate sources.

C. Data Mart is a subset of thedata warehouse that is usually oriented to a specific business line or team.

D. A database is a collection of information that is organized so that it can easily be accessed, managed, and updated.

14. Which of the following is NOT a measure of Green IT Initiative:

A. Unused servers should be consolidated

B. Endeavour to decrease carbon footprint

C. Preferring Air Travel over Road Travel to reduce the carbon level

D. Making use of e-mails rather than printing documents.

A. Consolidation of unused server reduces the energy consumption and optimizes the utilization of resources. Hence it is a measure of Green IT Initiative.

B. Endeavour to decrease carbon footprint is a measure of Green IT Initiative.

C. Preferring Air Travel over Road Travel to reduce the carbon level is not a Green IT Initiative.

D. Making use of e-mails rather than printing documents saves environment hence a measure of Green IT Initiative.

15. Which of the following is NOT a Web 2.0 security concern:

A. Third Party content

B. Community based

C. Openness

D. Technology

A. Third Party content is a big Web 2.0 security concern.

B. Community based web is a Web 2.0 security concern.

C. Openness which affects the privacy and confidentiality aspect is a web 2.0 concern.

D. Technology is an enabler of Web 2.0 and not a security concern.

16. Which of the following is a concern of BYOD:

A. Security Administration issues

B. Cost of the device

C. Network Bandwidth

D. Skill set of the employee

A. Security Administration issues are one of the major concerns of BYOD

B. Cost of the device is not a concern of BYOD

C. Network Bandwidth is not a concern of BYOD

D. Skill set of the employee, now a days is not a concern of BYOD

17. Which of the following specific tag language is used for exchanging business reporting information?

A. XML

B. XBRL

C. Web 2.0

D. Business Exchange Language

A. XML (eXtensible Markup Language) is a tag language but is not specifically used for business reporting information.

B. XBRL (eXtensible Business Reporting Language) is a specific tag language used for exchanging business reporting information.

C. Web 2.0 is not a tag language.

D. Business Exchange Language is not a term used to indicate any specific tag language.

18. Which of the following cloud service model indicates use of the service provider's application/software on cloud infrastructure?

A. Software as a Service

B. Platform as a Service

C. Infrastructure as a Service

D. Cloud as a Service

A. In Software as a Service, one uses service provider's application/software on cloud infrastructure.

B. In Platform as a Service, one uses service provider's basic computing infrastructure along with OS and Database Support. However, application software has to be managed by the user.

C. In Infrastructure as a Service, cloud service provider provides with basic computing infrastructure only.

D. Cloud as a Service is not a cloud service model.

19. 'Google' is the example of _____ Cloud.

A. Community Cloud

B. Private Cloud

C. Public Cloud

D. Personal Cloud

A. Google encompasses many aspects beyond just a Community Cloud

B. Google provides its services world-wide and hence not a Private Cloud.

C. Google is the example of Public Cloud.

D. Google provides its services world-wide and hence not a Private Cloud.

20. Which of the following is NOT the Risk involved in Outsourcing Services:

A. Privacy & Confidentiality

B. Complying with SLAs (Service Level Agreements)

C. Attrition of staff of Outsourcing company

D. Different platforms (Operating Systems) being used by the outsourcing service provider and the client.

A. Privacy & Confidentiality is the major risk with outsourcing services.

B. Complying with SLAs (Service Level Agreements) is a risk with outsourcing services.

C. Attrition of staff of outsourcing company can be a risk to its client.

D. Use of different platforms, normally, doesn't affect the deliverable agreed with the outsourcing company and hence, not a risk involved in outsourcing services.

21. Which of the following is not an Operating System?

A. Windows

B. Linux

C. Router

D. Android

A. Windows is an operating system

B. Linux is an operating system

C. Router is one of the network components and not an operating system

D. Android is an operating system

22. Which of the following does connect CPU and other components on mother-board:

A. Fiber Optic Cable

B. BUS

C. Twisted Pair Cable

D. Registers

A. Fiber Optic Cable is a communication media that works outside the CPU and doesn't connect CPU and other components on mother-board

B. BUS connects CPU and other components on mother board

C. Twisted Pair Cable is a communication media that works outside the CPU and doesn't connect CPU and other components on mother-board

D. Registers are the memory locations owned by the CPU and doesn't connect CPU and other components on mother-board

23. Which of the following is NOT directly related to functioning of CPU :

A. Arithmetic and Logical unit

B. Control unit

C. Network Interface card

D. Registers

A. Arithmetic and logical unit is one of the parts of CPU hence directly related to the functioning of CPU.

B. Control Unit is one of the parts of CPU hence directly related to the functioning of CPU.

C. Network Interface Card is not directly related to the functioning of CPU. It is used to connect system to the network.

D. Registers are one of the parts of CPU hence directly related to the functioning of CPU.

24. Which of the following memory doesn't exist physically but is created as per the need basis by sharing the secondary memory?

A. Random Access Memory

B. Non-volatile Memory

C. Virtual Memory

D. Cache Memory

A. Random Access Memory exists physically and is not shared from secondary memory.

B. Non-volatile memory refers to the secondary memory and it exists physically.

C. Virtual Memory doesn't exist physically but created as per the need basis by sharing the secondary memory to support the RAM.

D. Cache Memory exists physically and is used to store frequently used data.

25. Which of the following options is NOT an Internal (primary) memory:

    A. Random Access Memory

    B. Read Only Memory

    C. Cache Memory

    D. Virtual Memory

    A. Random Access Memory is a part of internal (primary) memory

    B. Read Only Memory is a part of internal (primary) memory

    C. Cache Memory is a part of internal (primary) memory

    D. Virtual Memory is not a part of internal (primary) memory, however it's virtually created to support internal memory

26. Which of the following is correct hierarchy of below data units / terms

    1. Character
    2. Record
    3. Field
    4. Database
    5. File

    A. 2-3-4-1-5

    B. 4-5-2-3-1

    C. 4-2-5-3-1

    D. 4-3-1-2-5

    A. Database contains Files, File contains records, Record contains fields, Field contains characters. Hence, this is not a correct option.

    B. Database contains Files, File contains records, Record contains fields, Field contains characters. Hence, this is a correct option.

    C. Database contains Files, File contains records, Record contains fields, Field contains characters. Hence, this is not a correct option.

    D. Database contains Files, File contains records, Record contains fields, Field contains characters. Hence, this is not a correct option.

27. Which of the following database model explains the relationship among entities in the form of tables and relationships among the tables:

    A. Network Model

B. Hierarchy Model

C. Table Model

D. Relational Model

A. Network Model doesn't explain relationship in the form of tables

B. Hierarchy Model doesn't explain relationship in the form of tables

C. There is no database model called table model.

D. Relational model explains the relationship among entities in the form of tables and relationships among the tables

28. If a magnet with strong magnetic field comes in physical contact with below data storage devices; data on which of the following devices may get scrambled?

A. Hard Drive (Hard Disk)

B. Audio CD

C. Video CD

D. DVD

A. Hard Drive (Hard Disk) is a magnetic device hence if a magnet with strong magnetic field comes in physical contact; its data may get scrambled.

B. Audio CD is an optical device hence not affected by a magnet

C. Video CD is an optical device hence not affected by a magnet

D. DVD is an optical device hence not affected by a magnet

29. The Primary job of the operating system is

A. Manage Commands

B. Manage Users

C. Manage Programs

D. Manage Resources

A. Managing command is not the primary job of operating system

B. Managing Users is not the primary job of operating system

C. Managing Programs us not the primary job of operating system

D. Managing Resources is the primary job of operating system

30. Virtual Memory is

A. Extremely Large Main memory

B. Extremely Large Secondary memory

C. An illusion of extremely large main memory

D. An illusion of extremely large secondary memory

A. Virtual Memory is not extremely large main memory

B. Virtual Memory is also not an extremely large secondary memory

C. Virtual Memory is an illusion of extremely large main memory

D. Virtual Memory is not an illusion o extremely large secondary memory

31. Which of the following does NOT belong to any type of database languages grouped under Structured Query Language (SQL):

A. Data Definition Language

B. Data Modification Language

C. Data Control Language

D. Data Manipulation Language

A. Data Definition Language (DDL) belongs to a type of database languages grouped under Structured Query Language (SQL)

B. Data Modification Language doesn't belong to a type of database languages grouped under Structured Query Language (SQL)

C. Data Control Language (DCL) belongs to a type of database languages grouped under Structured Query Language (SQL)

D. Data Manipulation Language (DML) belongs to a type of database languages grouped under Structured Query Language (SQL)

32. What should be the FIRST step while OS upgrading?

A. Delete old Operating System

B. Backup old Operating System

C. Backup Critical Data

D. Format Hard Disks

A. While upgrading OS, firstly critical data should be backed up hence this is not a correct option

B. While upgrading OS, firstly critical data should be backed up hence this is not a correct option

C. While upgrading OS, firstly critical data should be backed up hence this is a correct option

D. While upgrading OS, firstly critical data should be backed up hence this is not a correct option

33. Which of the following is correct option arranging memories from highest speed to the lowest

1. Primary Memory
2. Cache Memory
3. Secondary Memory
4. Registers

A. 4- 3- 2- 1

B. 2- 3- 4- 1

C. 4- 2- 1- 3

D. 4- 1- 2- 3

A. The Register is the memory having highest speed followed by primary memory, then cache memory and at last secondary memory hence this is not the correct option

B. The Register is the memory having highest speed followed by primary memory, then cache memory and at last secondary memory hence this is not the correct option

C. The Register is the memory having highest speed followed by primary memory, then cache memory and at last secondary memory hence this is not the correct option

D. The Register is the memory having highest speed followed by primary memory, then cache memory and at last secondary memory hence this is the correct option

34. For which of the following applications would rapid recovery be MOST crucial?

A. Corporate planning

B. Regulatory reporting

C. Departmental Reporting

D. Banking Website

A. Recovery of corporate planning is important but not as crucial as banking website

B. Recovery of regulatory reporting is important but not as crucial as banking website

C. Recovery of departmental reporting is important but not as crucial as banking website

D. Rapid recovery of Banking Website is the MOST crucial

35. Response Time in Hardware Asset Management refers to:

A. Length of time between submission of transaction and first character of output.

B. Length of time for submission of the job and receipt of completed output.

C. Length of time between the requisitions to buy the asset is raised and the asset is received.

D. Length of time required to repair the hardware.

A. Response time in hardware asset management refers to Length of time between submission of transaction and first character of output.

B. Length of time for submission of the job and receipt of completed output is called throughput time.

C. Length of time between the requisitions to buy the asset is raised and the asset is received is not referred to by response time

D. Length of time required to repair the hardware is not referred to by response time

36. Following is an Example of System Software:

A. Tally ERP 9

B. Microsoft Word

C. Easytax – Tax Return Preparation Software

D. Android

A. Tally ERP 9 is an example of application software

B. Microsoft Word is an example of application software

C. Easytax – Tax Return Preparation Software is an example of application software

D. Android is an example of system software

37. Which of the following is an example of End Point Device:

A. Switch

B. Router

C. Smart Phone

D. Gateway

A. Switch is an example of intermediate network device. It's not an end point device

B. Router is an example of intermediate network device. It's not an end point device

C. Smart Phone is an example of end point device

D. Gateway is an example of intermediate network device. It's not an end point device

38. Organizing fields and tables in a database so as to minimize redundancy and maximize efficiency is specifically called:

A. Simplification of Database

B. Normalization of Database

C. Updation of Database

D. Maintenance of Database

A. 'Simplification' is not the proper term that is used to indicate 'Organizing fields and tables in a database so as to minimize redundancy and maximize efficiency'

B. Normalization refers to organizing fields and tables in a database so as to minimize redundancy and maximize efficiency

C. 'Updation' is not the proper term that is used to indicate 'Organizing fields and tables in a database so as to minimize redundancy and maximize efficiency'

D. 'Maintenance' is not the proper term that is used to indicate 'Organizing fields and tables in a database so as to minimize redundancy and maximize efficiency'

39. Which of the following is NOT the function of Database Administrator:

A. Designing the schema of Database

B. Tuning the database for changing use needs.

C. Maintaining availability and ensuring integrity of databases

D. Deciding about the policy matter related to data

A. Designing the schema of Database is a function of Database Administrator

B. Tuning the database for changing use needs is a function of Database Administrator

C. Maintaining availability and ensuring integrity of databases is a function of database administrator

D. Deciding about the policy matter related to data is a function of Data Administrator and not of Database administrator

40. Which of the following memory is called a bridge between CPU and Main Memory:

A. Registers

B. Cache Memory

C. Virtual Memory

D. Secondary Memory

A. Registers are the part of CPU and is not a bridge between CPU and Main Memory

B. Cache Memory is called a bridge between CPU and Main Memory

C. Virtual Memory is not a bridge between CPU and Main Memory

D. Secondary Memory is not a bridge between CPU and Main Memory

41. While performing cyber forensic investigation, the IS auditor is MOST concerned with

A. Analysis of Audit Evidence

B. Confidentiality of Audit Evidence

C. Preservation of Audit Evidence

D. Evaluation of Audit Evidence

A. Analysis of Evidence is important but not as crucial as preservation of audit evidence.

B. Confidentiality of Evidenceis important but not as crucial as preservation of audit evidence.

C. Preservation of Audit Evidence is the most important and crucial part of cyber forensic investigation hence the biggest concern for an IS Auditor

D. Evaluation of Evidenceis important but not as crucial as preservation of audit evidence.

42. An IS auditor auditing a co-operative bank observed that a clerk was performing the function of a Manager (Branch Operations). He should:

A. Conclude that the Internal Controls are inadequate

B. Conclude that the segregation of duty is not performed

C. Suspend the Audit

D. *Expand the scope to perform substantive testing to see the implication of clerk's actions*

A. Direct conclusion, without verifying further evidences is not proper.

B. Direct conclusion, without verifying further evidences is not proper.

C. Suspension of the Audit is without any base and reason.

D. Expansion of scope in search of more corroborative and compelling evidences to see the implication of clerk's is the correct course of action.

43. During an exit interview, one of the audit committee member doesn't agree with the impact of a finding concluded by the IS auditor. An IS auditor should:

A. Ask the audit committee member to accept the full responsibility of impact in writing

B. Agree with the audit committee member as he is the part of senior management

C. *Explain the significance of finding and risk of not correcting the same*

D. Suspend the assignment and walkout

A. Acceptance of full responsibility by the audit committee member will not preclude the auditor from his responsibilities. This is not a proper course of action.

B. Agreement with committee member because he is part of senior management is not justified on the part of auditor and is not a proper course of action.

C. Explaining the significance of finding and risk of not correcting the same is proper course of action.

D. Suspension of audit and walking out due to non agreement of a finding with senior management is not the prudent practice on the part of auditor.

44. Which of the following is the BEST segregation of duty to ensure that unauthorized data entry or data modification cannot take place:

A. *Separate computer operator from DBA (Database Administrator)*

B. Separate application programmer from DBA

C. Separate Test programmers from application programmers

D. Separate quality assurance personnel from DBA

A. Data Entry and Data Modification is normally undertaken by the computer operator and it happens in the database which is handled by the DBA. Hence, this option indicates the BEST segregation of duty.

B. Separating the application programmer from DBA doesn't ensure unauthorized data entry and data modification.

C. Separating Test programmers from application programmers doesn't ensure unauthorized data entry and data modification.

D. Separating QA personnel from DBA doesn't ensure unauthorized data entry and data modification.

45. Two personnel simultaneously accessing and refilling cash in the ATM machine of a bank is the BEST example of:

A. Dual Access

B. *Dual Control*

C. Supervisory Control

D. Maker Checker Control

A. In Dual Access, two persons simultaneously open the ATM Machine but responsibility of cash deposit is on one of the persons only.

B. Two personnel simultaneously accessing and refilling cash in the ATM machine of a bank is the BEST example of Dual Control.

C. Supervisory Control doesn't suit the given scenario hence not the correct answer.

D. Maker Checker Controldoesn't suit the given scenario hence not the correct answer.

46. _____ is a set of methodologies that transform raw data into meaningful and useful information for business purpose.

A. Data analysis

B. CAAT Tools

C. Artificial Intelligence

D. *Business Intelligence*

A. Data Analysis is not the precise term that is used for the given question.

B. CAAT Tools are the tools to perform many functions over and above transforming raw data into meaningful and useful information for business purpose.

C. Artificial Intelligence is not related to the matter given in the question.

D. Business Intelligence is a set of methodologies that transform raw data into meaningful and useful information for business purpose.

47. Which of the following is the BEST example of Compliance Testing?

A. *Verification of user access controls*

B. Vouching of transaction with supporting evidences

C. Re-performance of interest calculation on a sample of bank FD accounts

D. Verification of accuracy of purchase of transaction for a given period

A. Verification of user access control is the BEST example of Compliance Testing.

B. Vouching of transaction with supporting evidences is the example of Substantive Testing.

C. Re-performanceof interest calculation on a sample of bank FD accounts is the example of Substantive Testing.

D. Verification of accuracy of purchase of transaction for a given periodis the example of Substantive Testing.

48. _____ is an end-to-end evaluation of a control to see that if operated as designed, it can effectively mitigate the risk to an acceptable level.

A. Audit Trail

B. *Structured Walkthrough*

C. Analytical Review procedures

D. Observation

A. Audit Trail covers the trace of the transaction right from beginning to the end.

B. Structured Walkthrough is an end-to-end evaluation of a control to see that if operated as designed, it can effectively mitigate the risk to an acceptable level.

C. Analytical Review Procedures are part of Substantive procedures and doesn't precisely indicate the given scenario.

D. Observation doesn't indicate precisely, the given scenario.

49. While carrying out an IS audit, the auditor was informed that the system he is auditing is attacked by an intruder. Which of the following is the BIGGEST concern of the auditor?

A. *Rebooting of the system*

B. Disconnecting the system from internet

C. Senior management was not informed about the attack immediately after the event

D. Backup routine was not run for past seven days

A. Rebooting, if done without confirming the preservation of the required evidence can have a serious impact on investigation hence the BIGGEST concern for IS Auditor.

B. Disconnecting the system from internet is not the concern of the auditor.

C. Not informing senior management about the attack, immediately after the event is not the BIGGEST concern for the auditor.

D. Non running of backup routine is a concern but not as big as rebooting of the system.

50. An IS Auditor observed that the client has outsourced its Accounting process to an outsourcing firm. Which of the following is the BIGGEST concern for the IS auditor?

A. *'Right to audit' is not reserved in the agreement*

B. Client and the outsourcing firm are operated on different platforms and OS

C. There is a minor discrepancy in drafting the SLA (Service Level Agreement)

D. The outsourcing firm is in a different country

A. 'Right to audit' is very important aspect of control when it comes to outsourcing of any process of an organization. Hence, if it is not reserved in agreement, is a BIGGEST concern for the IS auditor.

B. Client and the outsourcing firm operated on different platforms and OS is not the concern for IS auditor.

C. There is a minor discrepancy in drafting the SLA (Service Level Agreement) is not a BIGGEST concern for IS auditor.

D. Outsourcing firm in a different company is not a BIGGEST concern for IS auditor.

51. Before issuing the final IS audit report, the IS auditor should discuss the finding (draft report) with management staff so as:

A. To get approval for issuance of final IS audit report

B. To see that nothing is left auditing from the decided scope

C. *To gain agreement on the finding*

D. To decide the format of the final IS audit report

A. IS auditor is not required to take approval on the findings.

B. To see that nothing is left from the decided scope is the responsibility of the auditor himself.

C. IS auditor should discuss the finding (draft report) with management staff to gain agreement on the finding thereby avoiding any misunderstanding and confusion.

D. Format of the final IS audit report should be such that the decided scope and achievement of objective of the audit can be conveyed in the best manner. For that there is no need to discuss draft report with management.

52. Which of the following is NOT undertaken during an exit interview?

A. *Decision regarding material findings to be included in Audit Report*

B. Ensuring that the facts presented in the report are correct

C. Ensuring that the recommendations are realistic and cost effective.

D. Recommending implementation dates for agreed on recommendations

A. Decision regarding material findings to be included in Audit Report depends on the professional judgment of IS Auditor. It is not to be undertaken in exit interview.

B. Ensuring that the facts presented in the report are correct is undertaken in exit interview.

C. Ensuring that the recommendations are realistic and cost effective is undertaken in exit interview.

D. Recommending implementation dates for agreed on recommendations is undertaken in exit interview.

53. Which of the following sampling type is used when the auditor wants to prevent excessive sampling by stopping the audit test at earliest possible moment?

A. Discovery sampling

B. Attribute sampling

C. *Stop-or-go sampling*

D. Judgemental sampling

A. Discovery sampling is a method of sampling to assess whether the percentage error is not in excess of a specified percentage of the population.

B. Attribute Sampling allows the auditor to estimate the proportion of population items containing a specified characteristic.

C. Stop-or-go sampling is used when the auditor wants to prevent excessive sampling by stopping the audit test at earliest possible moment.

D. Judgmental sampling is a type of nonrandom sampling that is selected based on the opinion/intuition of an expert.

54. In Control Self Assessment (CSA), the role of the IS auditor is:

A. To conduct the audit on his own

B. To conduct the assessment of his own work

C. To setup evaluation criteria for assessment of controls

D. *To facilitate the management in carrying out assessment of controls.*

A. In Control Self Assessment (CSA), various controls are evaluated by the employees of client organization only.

B. In Control Self Assessment (CSA), role of the auditor is that of the facilitator. There is no question of evaluation of his own work.

C. In Control Self Assessment (CSA), evaluation criteria is also set by the responsible persons of client organization.

D. In Control Self Assessment (CSA), the IS auditor facilitates the management in carrying out assessment of controls.

55. Which of the following does a lack of adequate internal control represent?

A. A vulnerability

B. *A threat*

C. An impact

D. An asset

A. Vulnerability refers to the weakness contained by the system which can be exploited by the threat to create risk.

B. Threat represents a lack of adequate internal control.

C. Impact is the out-come if the risk gets exploited.

D. Asset is not represented by a lack of adequate internal control.

56. What is the MAJOR benefit of preferring control self assessment(CSA) over traditional audit?

A. It requires less audit resources

B. It doesn't require formal audit report

C. *It detects risk sooner*

D. Auditing standards are not required to be followed

A. Audit Resources required for performing a particular evaluation process is the same no matter it is conducted by IS Auditor (Traditional Audit) or by personnel of the organization (CSA).

B. Non requirement of Formal Audit Report is not the benefit of preferring CSA over traditional audit.

C. Control Self Assessment takes place at the regular interval by the personnel who belong to the organization only. Hence, it detects risk sooner.

D. Non compliance of Auditing Standardsis not the benefit of preferring CSA over traditional audit.

57. An IS auditor wants to verify the number of instances where system changes were not appropriately approved. Which of the following sampling method should an IS auditor use to draw the conclusion?

A. Judgemental sampling

B. Stop-or-go sampling

C. Variable sampling

D. *Attribute sampling*

A. Judgmental sampling is a type of nonrandom sampling that is selected based on the opinion/intuition of an expert.

B. Stop-or-go sampling is used when the auditor wants to prevent excessive sampling by stopping the audit test at earliest possible moment.

C. Variable sampling is used in case of Substantive audit procedures.

D. To see whether all the systems changes were approved or not is the compliance test. For compliance test attribute sampling is used. Attribute Sampling allows the auditor to estimate the proportion of population items containing a specified characteristic.

58. While auditing the firewall system, it was noticed by the IS auditor that it was installed by his associate firm. What should an IS auditor do FIRST?

A. *Disclose the fact to the client*

B. Suspend the audit

C. Take steps to restore the level of independence

D. Put a note in audit report

A. Disclosing the fact to the client is the FIRST step the IS auditor should take when he notices that the firewall, he was auditing, is installed by his associate firm.

B. There is no need to suspend the audit in this issue.

C. No restoration is feasible once the firewall is already installed. However, the management should be informed about the fact.

D. Putting a note in audit report will not be an effective action.

59. A client is proposing to implement a newer version of mail management system. Which of the following tasks IS auditor can perform without affecting his independence?

A. Recommend the vendor who can provide the BEST mail management system

B. Supporting the client in designing of various controls for the new system

C. *Review the penetration test results to opine on the effectiveness of the controls*

D. Offering his own customized mail management system

A. Recommending the vendor who can provide the BEST mail management system will compromising his independence.

B. Supporting the client in designing of various controls for the new system will compromise his independence.

C. Review of penetration test results to opine on the effectiveness of the controls can be performed without affecting the effectiveness of the control.

D. Offering his own customized mail management system will definitely compromise his independence.

60. An IS auditor is testing the user access matrix of the large financial company for which he has selected a sample from current employee list provided by the client. Which of the following evidence is MOST reliable to support such testing?

A. *A list of user accounts with access rights which is generated from the system*

B. HR level documents signed by the respective departmental heads

C. An excel sheet provided by the system administrator

D. Observation of the users while they are accessing the system in the presence of system administrator

61. Which of the following type of risk is directly attributable to the actions and decisions of IS Auditor?

A. *Detection Risk*

B. Inherent Risk

C. Control Risk

D. Administrative Risk

A. Detection Risk is directly attributable to the actions and decisions of IS Auditor

B. Inherent Risk refers to the auditor's assessment of the likelihood that there are material misstatements due to error or fraud in segment before considering the effectiveness of internal control

C. Control Risk refers to the risk that a misstatement could occur but may not be detected and corrected or prevented by entity's internal controlmechanism

D. Administrative Risk is not the risk directly attributable to the actions or decisions of IS Auditor

62. In planning the IS Audit, the MOST important thing is to decide:

A. *Significant Risk Areas*

B. Remuneration for the audit

C. Qualification of audit staff

D. Time available for audit

A. In planning the IS Audit, the MOST important thing is to decide Significant Risk Areas

B. Remuneration for the audit is not as important as deciding significant risk areas

C. Qualification of audit staff is not as important as deciding significant risk areas

D. Time available for audit is not as important as deciding significant risk areas

63. Which of the following statement is correct for IS Auditor with reference to the Materiality:

A. Lower the level of materiality, lower is the audit risk that an IS auditor is willing to take.

B. Higher the level of materiality, higher is the audit risk that an IS auditor is willing to take.

C. *Higher the level of materiality, lower is the audit risk that an IS auditor is willing to take.*

D. None of the Above

A. Level of materiality and level of audit risk is inversely related hence this option is not correct

B. Level of materiality and level of audit risk is inversely related hence this option is not correct

C. Level of materiality and level of audit risk is inversely related hence this is the correct option

D. This is not the correct option as option c is the correct option

64. Which of the following type of IS control, an Antivirus Software represents?

A. Preventive Control

B. Detective Control

C. Corrective Control

D. *All of the above*

A. An antivirus software represents all types of controls hence only preventive control is not the proper option to select

B. An antivirus software represents all types of controls hence only detective control is not the proper option to select

C. An antivirus software represents all types of controls hence only corrective control is not the proper option to select

D. An antivirus software represents all types of controls hence this is the best option to select

65. Which of the following is NOT provided by the Audit Charter?

A. Authority and scope of audit function

B. *Audit Materiality*

C. Mandate for performing audit function

D. Roles and Responsibility of audit function

A. Authority and scope of audit function is provided by the Audit Charter

B. Audit Materiality is not provided by audit charter

C. Mandate for performing audit function is provided by the Audit Charter

D. Roles and Responsibility of audit function is provided by the Audit Charter

66. 'Insurance Coverage' falls under which type of a specific risk mitigation strategy:

A. Risk Avoidance

B. Risk Acceptance

C. *Risk Transfer*

D. Risk Reduction

A. When insurance coverage is taken, risk is transferred to the third party hence this is not the correct option to choose from

B. When insurance coverage is taken, risk is transferred to the third party hence this is not the correct option to choose from

C. When insurance coverage is taken, risk is transferred to the third party hence Risk transfer is the correct option

D. When insurance coverage is taken, risk is transferred to the third party hence this is not the correct option to choose from

67. Enterprise governance, being the entire accountability framework of the organisation, lays most emphasis on which dimension?

A. Performance.

B. Conformance.

C. Governance.

D. Management.

A. Enterprise governance is the entire accountability framework of the organisation with the twin dimensions of conformance and performance of processes, with more emphasis on performance.

B. Being enterprise governance's more emphasis on performance, conformance is less suitable option.

C. Being enterprise governance's more emphasis on performance, governance is less suitable option.

D. Being enterprise governance's more emphasis on performance, management is less suitable option

68. Corporate Governance's effective implementation is dependent on all except _____

A. The right people.

B. The right place.

C. The right time.

D. The right decisions.

A. Corporate Governance's effective implementation is dependent on the right people.

B. Corporate Governance's effective implementation is not dependent on the right place.

C. Corporate Governance's effective implementation is dependent on the right time.

D. Corporate Governance's effective implementation is dependent on the right decisions

69. Which perspective of 'The Balanced Score Card' will allow the managers to determine how well the business is performing and whether their products meet customer requirements?

A. The Financial Perspective.

B. The Customer Perspective.

C. The Internal Business Process Perspective.

D. The Learning & Growth Perspective.

A. The Financial Perspective suggests financial data on risk assessment and costs versus benefits.

B. The Customer Perspective will indicate the extent of customer satisfaction with the products/services supplied.

C. *The Internal Business Process Perspective will allow the managers to determine how well the business is performing and whether their products meet customer requirements.*

D. The Learning & Growth Perspective creates a culture that support organisational change, employees training, corporate cultural attitudes, growth and innovation.

70. Which of the following is a part of information security governance?

A. *Confidentiality*.

B. Authenticity.

C. Accountability.

D. Reliability.

A. *Confidentiality is a part of information security governance.*

B. Authenticity is not involved in information security governance.

C. Accountability is not involved in information security governance.

D. Reliability is not involved in information security governance.

71. Enterprise Architecture involves documenting the organisation's IT assets in a systematic and structured method to promote all except _____.

A. Information Systems.

B. Management.

C. Planning.

D. Understanding IT investments.

A. Enterprise Architecture does not promote information systems.

B. Enterprise Architecture involves documenting the organisation's IT assets in a systematic and structured method to promote management from a technology and business perspective.

C. Enterprise Architecture involves documenting the organisation's IT assets in a systematic and structured method to promote planning from a technology and business perspective.

D. Enterpris Architecture involves documenting the organisation's IT assets in a systematic and structured method to promote understanding of IT investments from a technology and business perspective.

72. Which is the process of selecting and implementing measures to reduce risk?

A. Risk Appetite.

B. Risk Treatment.

C. Risk Management.

D. Risk Assessment.

A. Risk Appetite is the extent to which management is willing to take risks.

B. Risk Treatment is the process of selecting and implementing measures to reduce risk.

C. Coordinating activities in order to direct and control an organisation with respect to risk comprising, risk assessment and risk treatment is Risk Management.

D. Risk Assessment is the process of risk analysis and evaluation.

73. Which is not an advantage of forming the IS Steering Committee?

A. Establishes user focus in IS.

B. Promotes user ownership of systems.

C. User representation.

D. Decentralization of authority.

A. Establishing user focus in IS is an advantage of forming the IS Steering Committee.

B. Promotion of user ownership of systems is an advantage of forming the IS Steering Committee.

C. User representation is an advantage of forming the IS Steering Committee.

D. Decentralization of authority is never an advantage of forming the IS Steering Committee.

74. Which is most dynamic amongst the below options since it must reflect the regular changes in business focus and environment?

A. Guidelines.

B. Standards.

C. Procedures.

D. Policies.

A. Guidelines are not as dynamic as procedures are.

B. Standards are not as dynamic as procedures are.

C. Procedures are more dynamic than the parent policy since they must reflect the regular changes in business focus and environment. Hence they must be frequently reviewed and updated.

D. Policies are not as dynamic as procedures are.

75. Which is the process of providing a part or all of an organization's IS functions to multiple firms for a fee as well as an agreed service level?

A. Out-tasking.

B. Outsourcing.

C. Co-sourcing.

D. Multiple sourcing.

A. Out-tasking provides a part or all of an organization's IS functions to multiple firms for a fee as well as an agreed service level.

B. Outsourcing differs in a way that IS functions are transferred to a third party.

C. In Co-sourcing, client is responsible for the management of outsourced activities while the vendor provides consultancy services and experienced personnel when needed.

D. Multiple sourcing is not any type of sourcing in sourcing process.

76. Which persons are responsible for designing application systems based on user specifications, resulting in the development of functional specifications and other high level systems design documents?

A. Application Systems Programmers.

B. Application Systems Analysts.

C. Application Systems Development Manager.

D. Application Systems Officer.

A. Application Systems Programmers develops new application systems and maintain the existing production systems.

B. Application Systems Analysts are responsible for designing application systems based on user specifications, resulting in the development of functional specifications and other high level systems design documents.

C. Application Systems Development Manager oversee the work of application systems analysts and application programmers who design, develop and maintain new or existing application programs.

D. Application Systems Officer does not form part of IS Department.

77. An IS auditor discovers that several IT based projects were implemented that were not approved by the steering committee. What is the greatest concern for the IS Auditor

A. IT projects will not be adequately funded

B. IT projects are not following the SDLC process

C. IT projects are not consistently formally approved

D. The IT department may not be working towards a common goal of the organization

A. This is a concern but not as big as the risk of lack of goal orientation of the organization as a whole

B. This is a concern but not as big as the risk of lack of goal orientation of the organization as a whole

C. This is a concern but not as big as the risk of lack of goal orientation of the organization as a whole

D. If several projects are not approved by the IT Steering committee then IT department may not be working towards a common goal of the organization

78. Which of the following situation is mainly addressed by a Software Escrow Agreement:

A. Vendor of the Software goes out of business

B. IS auditor's requirement to access the code written by the organization

C. User's requirement of re-installing the application software in his PC

D. Organization's requirement to have offsite backup of source code

A. Software escrow agreement addresses the situation that if the vendor of software goes out of business then the trusted third party who is entrusted with the possession of code can be called upon to get the copies of originally written code

B. Software escrow agreement doesn't mainly addresses the given requirement

C. Software escrow agreement doesn't mainly addresses the given requirement

D. Software escrow agreement doesn't mainly addresses the given requirement

79. Organization's DRP head has entered into a reciprocal agreement as one of the strategy of Disaster Recovery Planning. Which of the following risk treatment approach does it indicate?

A. Risk Transfer

B. Risk Avoidance

C. Risk Mitigation

D. Risk Acceptance

A. Risk Transfer refers to the transfer of one's risk to a third party by paying appropriate risk premium. Reciprocal Agreement refers to an agreement between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site.

B. Risk avoidance refers to avoiding those actions or events that may lead to risk

C. Reciprocal Agreement refers to an agreement between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site. This is a strategy of Risk Mitigation

D. Risk acceptance is a good and necessary part of all risk management. It is preferable to accept risks temporarily once it is clear they cannot be resolved for a period of time.

80. An IS auditor, performing review of and organization's governance model, is MOST concerned about:

A. The organization doesn't have malware protection policy

B. Organization's information security policy is not periodically reviewed by senior management or the dedicated committee constituted by the board

C. A policy that the Systems must remain up-to-date by installing the latest available patch is not implemented

D. All the members of the board do not have a copy of Information Security Policy.

A. Not having a malware protection policy is a concern but not as serious as non consideration by the senior management

B. An IS auditor, performing review of and organization's governance model, is MOST concerned that the organization's information security policy is not periodically reviewed by senior management or the dedicated committee constituted by the board

C. System should be remained up-to-date by installing the latest patch however non maintenance of the same is not as big concern asnon consideration by the senior management

D. All the members of the board do not have a copy of Information Security Policy – is a trivial concern compared to the periodic review by senior management

81. Effective IT governance ensures that the IT plan is consistent with the Organization's:

A. Audit Plan

B. Business Plan

C. Investment Plan

D. Insurance Plan

A. IT plan has to be consistent with organization's business plan hence this is not the correct choice

B. Effective IT governance ensures that the IT plan is consistent with the Organization's Business Plan

C. IT plan has to be consistent with organization's business plan hence this is not the correct choice

D. IT plan has to be consistent with organization's business plan hence this is not the correct choice

82. IT governance is the primary responsibility of:

A. Board of Directors (BODs)

B. CEO

C. IT Steering Committee

D. IT Security Officer

A. IT governance is the primary responsibility of Board of Directors (BODs)

B. IT governance is the primary responsibility of Board of Directors (BODs) hence this is not the correct choice

C. IT governance is the primary responsibility of Board of Directors (BODs) hence this is not the correct choice

D. IT governance is the primary responsibility of Board of Directors (BODs) hence this is not the correct choice

83. An IS Auditor is reviewing the recently concluded recruitment process of an organization. Which of the following should be considered the BEST assurance mechanism to ensure the integrity aspect?

A. References given in the resume

B. Qualification listed in the resume

C. References

D. Background Screening

A. References given in the resumes don't give best assurance about the integrity of the proposed employee

B. Qualification listed in the resume don't give assurance about integrity aspect

C. References don't give best assurance about the integrity of the proposed employees

D. Background screening is the best choice to ensure the integrity aspect of recruitment process

84. To support an organization's goal, the IT department should have:

E. Long and short range plans

F. Philosophy of Cost effectiveness

G. Latest Technology

H. Hardware Acquisition Plan

A. To support organization's goal, the IT department should have primarily long and short range plans

B. Philosophy of cost effectiveness is important but primarily to have proper plans is more important

C. Latest Technologyis important but primarily to have proper plans is more important

D. Hardware Acquisition Planis important but primarily to have proper plans is more important

85. Which of the following is considered to be MOST important while evaluating organization's IT Strategy by an IS Auditor:

A. IT Strategy complies with hardware procurement procedures

B. IT strategy supports business objectives

C. IT Strategy is within the budget limits as specified by senior management

D. IT Strategy is approved by the CEO

A. Hardware procurement procedures should comply with IT Strategy. However, supporting business objective is most important

B. While evaluating organization's IT Strategy it is most important to see that it supports business objectives

C. To have IT strategy within the budget limit as specified by senior management is important butsupporting business objective is most important

D. IT Strategy should be approved by top management which may or may not involve only CEO. However, supporting business objective is most important

86. To ensure whether organization is complying with the privacy requirements, IS auditor should FIRST review:

A. Organizational policies

B. Organizational standards and procedures

C. Legal and Regulatory requirements

D. IT Infrastructure

A. The auditor may review organizational policies but first of all, legal and regulatory requirements should be reviewed

B. The auditor may review organizational standards and procedures but first of all, legal and regulatory requirements should be reviewed

C. To ensure whether organization is complying with the privacy requirements, IS auditor should FIRST review Legal and Regulatory requirements

D. The auditor may review IT infrastructure but first of all, legal and regulatory requirements should be reviewed

87. An IS auditor reviewing the role of IT Steering Committee is MOST concerned when IT Steering Committee:

A. Is responsible to determine business goals

B. Is responsible for project approval

C. Is responsible for long term IT plan

D. Is responsible for reporting of the IT Project status to senior management

A. Role of the IT Steering committee is to approve the project, making long term IT plan, reporting of IT project status to senior management etc. Hence, if it is made responsible to determine business goals, it is the biggest concern for IS Auditor

B. Role of the IT Steering committee is to approve the project, making long term IT plan, reporting of IT project status to senior management etc. Hence, this is not a concern for IS Auditor

C. Role of the IT Steering committee is to approve the project, making long term IT plan, reporting of IT project status to senior management etc. Hence, this is not a concern for IS Auditor

D. Role of the IT Steering committee is to approve the project, making long term IT plan, reporting of IT project status to senior management etc. Hence, this is not a concern for IS Auditor

88. Assessment of IT Risk is BEST achieved by:

A. Use of historic loss exposure data to assess the current scenario

B. Evaluation of associated threats and vulnerabilities

C. Review of Risk Management in previous year audit reports

D. Review of public evaluation reports about the organization's risks

A. Use of historic loss exposure data to assess the current scenario may not give proper risk assessment in the correct perspective

B. Evaluation of associated threats and vulnerabilities gives the best assessment of IT risk

C. Review of Risk Management in previous year audit reports may give an idea about the IT risk but it will not be all exhaustive as per the current threats and vulnerabilities

D. Review of public evaluation reports about the organization's risks may be useful in IT risk assessment but cannot be solely relied upon

89. A top-down approach in development of operational policies ensures:

A. They are reviewed periodically by top management

B. They adhere to the IT Security policy

C. They are consistent across the organization

D. Departmental requirements are considered first.

A. The essence of Top down approach is that organizational goals are always kept in consideration while carrying out any process from top node to bottom node. Periodic review by top management is not primarily ensured by the said approach

B. The essence of Top down approach is that organizational goals are always kept in consideration while carrying out any process from top node to bottom node. Adherence to IT security policy is not primarily ensured by the said approach

C. The essence of Top down approach is that organizational goals are always kept in consideration while carrying out any process from top node to bottom node. Hence it is consistent across the organization

D. The essence of Top down approach is that organizational goals are always kept in consideration while carrying out any process from top node to bottom node. Departmental requirements are not considered first. Organizational requirements are considered first in top-down approach

90. Which of the following is the MOST important element for successful implementation of IT Governance:

A. Performing Risk Assessment

B. Implementing IT balanced Scorecard

C. Identifying organizational strategies

D. Developing a good IT Security Policy

A. For successful implementation of IT Governance the most important thing is to identify organizational strategies. Risk Assessment is performed subsequently

B. For successful implementation of IT Governance the most important thing is to identify organizational strategies. IT balanced scorecard comes at a later point in time

C. For successful implementation of IT Governance the most important thing is to identify organizational strategies.

D. Mere development of a good IT security policy doesn't guarantee for successful implementation of IT Governance

91. Which of the following tool an IS auditor should recommend that helps BEST in achieving IT and business alignment:

A. IT Balanced Scorecard

B. Control Self Assessment

C. Business Process Reengineering

D. Business Impact Analysis

A. IT Balanced Scorecard helps best in achieving IT and business alignment. Hence, this should be recommended by an IS auditor

B. Control self assessment (CSA) is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes. It doesn't help primarily in aligning IT and business

C. Business Process Reengineering (BPR) is the analysis and redesign of workflows within and between enterprises in order to optimize end-to-end processes and automate non-value-added tasks. It doesn't help primarily in aligning IT and business

D. Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to criticalbusiness operations as a result of a disaster, accident or emergency. It doesn't help primarily in aligning IT and business

92. The primary control purpose of job rotations and allowing vacations is to:

A. Facilitate Cross-training

B. Boost employee morale

C. Provide competitive employee benefit

D. Detect improper or illegal employee acts

A. Cross training is one of the output of job rotation however is not the primary purpose of doing so

B. Boosting employee morale is not the purpose of job rotation and allowing vacations

C. Provide competitive employee benefit is not the purpose of job rotation and allowing vacations

D. Detect improper or illegal employee acts is the primary purpose of job rotation and allowing vacations

93. 'Rerun Procedure' and 'Hash Totals' respectively are example of _____ control and _____ control.

A. Corrective, Detective.

B. Corrective, Preventive.

C. Detective, Preventive.

D. Detective, Corrective.

A. Rerun Procedure is an example of corrective control as it is designed to correct an error when it is detected. Hash Totals is an example of detective control as it is designed to detect errors and malicious acts.

B. Rerun Procedure and Hash Totals are examples of corrective and detective controls respectively.

C. Rerun Procedure and Hash Totals are examples of corrective and detective controls respectively.

D. Rerun Procedure and Hash Totals are examples of corrective and detective controls respectively.

94. Power supply from external sources such as a grid and generators are subject to many quality problems. All of the following cleanse the incoming power supply and deliver clean power fit for the equipments except _____.

A. Surge Protectors.

B. Spike Busters.

C. Sag Cleanser.

D. Line Conditioners.

A. Surge protectors cleanse the incoming power supply and deliver clean power fit for the equipment.

B. Spike Busters cleanse the incoming power supply and deliver clean power fit for the equipment.

C. Sag Cleanser cannot function to cleanse the incoming power supply.

D. Line Conditioners cleanse the incoming power supply and deliver clean power fit for the equipment.

95. Which controls are protection mechanisms that limit users' access to data to what is appropriate for them?

A. Physical Access Controls.

B. Network Security Controls.

C. Application Controls.

D. Logical Access Controls.

A. Physical Access Controls restrict physical access to resources and protect them from intentional and unintentional loss or impairment.

B. Network Security Controls is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.

C. Application Controls safeguard assets, maintain data integrity and achieve organisational goals effectively and efficiently.

D. Logical Access Controls are protection mechanisms that limit users' access to data to what is appropriate for them.

96. Which is the appropriate example of Rounding Down Technique?

A. Turning Rs. 1008.02 to Rs. 1008.00.

B. Turning Rs. 1008.02 to Rs. 1008.10.

C. Turning Rs. 1008.02 to Rs. 1008.50.

D. Turning Rs. 1008.02 to Rs. 1008.05.

A. In Rounding Down Technique, the perpetrator rounds down the amounts in various transactions down to the nearest desired decimal place. In above example, the closest downward decimal place to Rs. 1008.02 is 1008.00.

B. Rounding Down Technique does not round the amounts upwards from Rs. 1008.02 to Rs. 1008.10.

C. Rounding Down Technique does not round the amounts upwards from Rs. 1008.02 to Rs. 1008.50.

D. Rounding Down Technique does not round the amounts upwards from Rs. 1008.02 to Rs. 1008.05.

97. Which malicious code is attached to a host program and propagates when an intended program is executed?

A. Worms.

B. Viruses.

C. Trojan Horses.

D. Logic Bombs.

A. Worms are malicious programs that attack a network by moving from device to device and create undesirable traffic.

B. Viruses are malicious codes are attached to a host program and propagate when an intended program is executed.

C. Trojan Horses are malicious codes which hide inside a host program that does something useful.

D. Logic Bombs are legitimate programs to which malicious code is added.

98. Which malicious code is difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection?

A. Polymorphic Viruses.

B. Stealth Viruses.

C. Macro Viruses.

D. Trojan Horses.

A. Polymorphic Viruses are malicious codes which are difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection

B. Stealth Viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves.

C. Macro Viruses infects an application and causes a sequence of actions to be performed automatically when the application is started or event triggers.

D. Trojan Horses are malicious codes which hide inside a host program that does something useful.

99. Which malicious code tracks the internet activities of the user usually for the purpose of sending targeted advertisements?

A. Stealth Viruses.

B. Polymorphic Viruses.

C. Adware and Spyware.

D. Macro Viruses.

A. Stealth Viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves.

B. Polymorphic Viruses hide themselves from antivirus software by altering their appearance after each infection.

C. Adware and Spyware are malicious codes which tracks the internet activities of the user usually for the purpose of sending targeted advertisements

D. Macro Viruses infects an application and causes a sequence of actions to be performed automatically when the application is started or event triggers.

100. If an intruder is able to bypass the network parameter security controls, which is the last barrier to be conquered for unlimited access to all the resources?

A. Application System.

B. Network System.

C. Logical Access System.

D. Operating System.

A. Application system is not the last barrier to be conquered for unlimited access to all the resources.

B. Network System is not the last barrier to be conquered for unlimited access to all the resources.

C. Logical Access System is not the last barrier to be conquered for unlimited access to all the resources.

D. Operating system provides the platform for an application to use various IS resources and perform a specific business function. If an intruder is able to bypass the network parameter security controls, operating system is the last barrier to be conquered for unlimited access to all the resources.

101. What ensures that a particular session can only be initiated from a particular location or computer terminal?

A. Automated terminal identification.

B. User identification and authentication.

C. Terminal log-on procedures.

D. Password management system.

A. Automated terminal identification ensures that a particular session can only be initiated from a particular location or computer terminal.

B. User identification and authentication ensures users must be identified and authenticated in a foolproof manner.

C. Terminal log-on procedures prevents misuse by an intruder.

D. Password management system enforces the use of strong passwords.

102. Which are the programs that help to manage critical functions of the operating system?

A. Clock Synchronization.

B. System Utility.

C. Event Logging.

D. Enforced Path.

A. Clock Synchronization synchronizes clock time to maintain event logs across the enterprise.

B. System Utilities are the programs that help to manage critical functions of the operating system.

C. Event logging does recording all the 'happenings' of local files on the system and it includes accessing, deleting, adding a file or an application, modifying the system's date, shuting down the system, changing the system configuration, etc.

D. An enforced path takes a user from their workstation to the services that they are authorised to use without risk of accessing, either by mistake or design, other services which they are not authorised to use.

103. Which mechanism of database control checks the destination of output obtained through authorized access?

A. Auditing.

B. Covert Channels.

C. Flow Controls.

D. Inference Controls.

A. Auditing reports security-related events in a structured format such as system journals, audit trails and system logs.

B. Covert Channels ensures DBMS does not have concealed channels.

C. Flow Controls checks the destination of output obtained through authorized access.

D. Inference Controls ensures DBMS assigns classification to aggregate information.

104. Which mechanism of database control allows the database to have multiple instances of objects, each having their own classification level?

A. Polyinstantiation.

B. Flow Controls.

C. Covert Channels.

D. Inference Controls.

A. Polyinstantiation allows the database to have multiple instances of objects, each having their own classification level.

B. Flow Controls checks the destination of output obtained through authorized access.

C. Covert Channels ensures DBMS does not have concealed channels.

D. Inference Controls ensures DBMS assigns classification to aggregate information.

105. Which mechanism of database control ensures DBMS provides a way to assign classifications to aggregate information?

A. No back doors.

B. Flow Controls.

C. Covert Channels.

D. Inference Controls.

A. No back doors ensures access to data be made available only via the DBMS.

B. Flow Controls checks the destination of output obtained through authorized access.

C. Covert Channels ensures DBMS does not have concealed channels.

D. Inference Controls ensures DBMS provides a way to assign classifications to aggregate information.

106. In which accounting audit trail, data can be traced from its source to the items it affects?

A. External Label.

B. Implosion Operation.

C. Internal Label.

D. Explosion Operation.

A. External Label labels on the storage devices that assist users by providing information about database name, creation, transaction file, back up information, etc.

B. In Implosion Operation, data can be traced from its source to the items it affects.

C. Internal Label identifies a table, file or a database by the application program access.

D. Explosion Operation reconstructs the sequence of events that have occurred in a data item in the database definition or the database.

107. In which accounting audit trail, the sequence of events that have occurred in a data item in the database definition or the database can be reconstructed?

A. Explosion Operation.

B. External Label.

C. Implosion Operation.

D. Internal Label.

A. In Explosion Operation, the sequence of events that have occurred in a data item in the database definition or the database can be reconstructed.

B. External Label labels on the storage devices that assist users by providing information about database name, creation, transaction file, back up information, etc.

C. In Implosion Operation, data can be traced from its source to the items it affects.

D. Internal Label identify a table, file or a database by the application program access.

108. What works on the principles of tables and relations and allows rules of integrity and access to be specified?

A. Pluggable Authentication Modules.

B. Data Dependent Access Control.

C. Granularity of Access Control.

D. Relational Database.

A. Pluggable Authentication Module framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system through the use of pluggable modules.

B. Data Dependent Access Control is an access-control decision based on the data contained in the records.

C. Granularity of Access Control is access control that can be imposed at various degrees of granularity in a system.

D. Relational Database works on the principles of tables and relations and allows rules of integrity and access to be specified.

109. What refers to gathering discrete bits of information from various sources and then putting them together to make a coherent whole?

A. Social Engineering.

B. Port Scan.

C. Reconnaissance.

D. Impersonation.

A. Social Engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and even actions that can lead to an attack.

B. Port Scan is an easy way to gather network information to use a port scanner, a program that, for a particular IP address, reports which ports respond to messages and which of the several known vulnerabilities are present.

C. Reconnaissance refers to gathering discrete bits of information from various sources and then putting them together to make a coherent whole.

D. Impersonation is a way to obtain information about a network by impersonating another person or process.

110. Which vulnerability is based on the thinking that not always only the message is sensitive but the fact that it exists is also sensitive?

A. Exposure.

B. Man-in-the-Middle Attack.

C. Traffic Analysis.

D. Session Hijacking.

A. Exposure is exposing content of a message in temporary buffers that build, format and present the message.

B. In Man-in-the-Middle Attack, one entity intrudes between two others.

C. Traffic Analysis is based on the thinking that not always only the message is sensitive but the fact that it exists is also sensitive.

D. Session Hijacking is intercepting and carrying on a session begun by another entity.

111. Which is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning?

A. Ping.

B. Traffic Redirection.

C. Connection Flooding.

D. DNS Attacks.

A. Ping is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning.

B. Traffic Redirection happens when router forwards traffic on its way through intermediate networks between a source host's network and destination's network.

C. Connection Flooding happens when an attacker sends more data than what a communication system can handle.

D. DNS Attacks are the attacks that convert domain names into network addresses.

112. Which two network security controls are similar in a way that both support authentication and confidentiality and also designed to be independent of specific cryptographic protocols?

A. SSL Encryption and IPSec.

B. SSL Encryption and Public Key Infrastructure.

C. Public Key Infrastructure and IPSec.

D. Public Key Infrastructure and Link Encryption.

A. IP Sec is similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above applications or below TCP protocols. Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

B. Incorrect pair of network security control for the specified situation.

C. Incorrect pair of network security control for the specified situation.

D. Incorrect pair of network security control for the specified situation.

113. Which of the following does give BEST protection against SQL Injection attacks in a website:

A. Avoid queries to the Database

B. Get the approval of DBA before firing a query

C. Input validations exist within the Web Application

D. SQL interface should not be allotted to the end user

A. Avoiding queries to the database will not solve the problem

B. Every time getting approval of DBA before firing a query will not solve the problem

C. Input validations within the web application can give the best protection against SQL injection attacks

D. Normally SQL interface in not directly allotted to the end user. It is routed through a good and validated User Interface

114. Which of the following is the BEST defense against the introduction of Trojan Horse software in an organization?

A. Anti-virus System

B. Intrusion Detection System

C. Firewall

D. Password protected screen saver

A. Trojan Horse is a kind of a malicious computer program which can be best prevented by anti-virus system

B. Intrusion Detection System is not the best defense for preventing malicious compute program. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station

C. Firewall cannot prevent malicious computer programs

D. Password protected screen saver cannot prevent malicious computer program

115. Which of the following is the BEST mechanism for minimizing unauthorized access to unattended user computers?

A. CCTV Camera surveillance system

B. Auto termination of sessions

C. Switching off the monitor

D. Use of Password protected screen saver

A. CCTV camera surveillance system will not minimize or prevent unauthorized access to unattended user computers

B. Auto termination of sessions is a mechanism to prevent unauthorized access but will be ineffective until session is terminated and nonetheless user computer will always allowed to be access physically

C. Switching off the monitor will not prevent/minimize unauthorized access to unattended user computers

D. Use of password protected screen saver is the best mechanism to minimize unauthorized access to unattended user computers

116. Which of the following is the BEST mechanism for minimizing unauthorized access to Network Administrator's Account?

A. Two Factor Authentication

B. Automatic password expiration

C. Password change alert every week

D. Password complexity rules

A. Two factor authentication is a technique wherein identification and authentication of the user takes place with two factors: One based on what user has and other based on what user knows. Hence that is the BEST mechanism for minimizing unauthorized access to network administrator's account

B. Automatic password expiration is not the best mechanism for minimizing unauthorized access to network administrator's account

C. Password change alert every weekis not the best mechanism for minimizing unauthorized access to network administrator's account

D. Password complexity rules are good mechanism but not as good as two factor authentication

117. An organization is currently planning to implement a new ERP Solution and wants its users to have access to the various system reports on a 'need to know' basis. Which of the following access control method BEST suits this requirement?

A. Discretionary Access Control

B. Role based Access Control

C. Mandatory Access Control

D. Single Sign On Access Control

A. Discretionary Access Control is a mechanism where a superior allocate the powers to use system to the subordinates depending on the user requirements however role based access control is a more precise choice

B. Role based access controls is the best method to suit the requirement of access control based on 'need to know' basis

C. Mandatory access control doesn't particularly support the requirements of 'need to know'

D. Single Sign On Access Control doesn't particularly support the requirements of 'need to know'

118. An employee of an organization received a digital book reader as a gift and connected the same to his work PC to transfer e-books. The primary risk that this scenario introduces is that:

A. The digital book reader may be incompatible with the user's PC

B. The employee may bring inappropriate books in the office

C. The digital book reader could be infected with virus

D. The digital book reader storage media could be used to steal corporate data

A. Incompatibility of digital book reader with user's pc is not a primary risk

B. The employee may bring inappropriate books in the office is a risk but not a primary one

C. Digital book reader could be infected with virus and the same may affect the network of the organization – this is the primary risk of the given scenario

D. The digital book reader storage media could be used to steal corporate data is a risk but not a primary one

119. A senior IT manager of the company has been terminated. The organization removed all his access to the company's resources. Yet, the IT manager is threatening the organization to disrupt the company's system if he is not paid a large sum of money. Which of the following could have been used by the IT manager to disrupt the Company's system:

A. Logic Bomb Attack

B. Virus Infection

C. Worm Infection

D. DOS Attack

A. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. This could have been used by the IT manager to disrupt the Company's System

B. Prospective virus infection is normally not possible if the access to all the resources is taken away.

C. Prospective worm infection is normally not possible if the access to all the resources is taken away.

D. Denial of Service attack may be possible if the system is connected to internet but logic bomb attack is a more serious threat

120. A company offers free Wi-Fi to all its guests whomsoever visit the company premises by authenticating them through a generic user id and password which was allotted at the reception desk. Which of the following control BEST suits this situation?

A. Change of password of wireless network on weekly basis

B. Installation of Firewall between wireless public network and company network

C. Installation of Intrusion Detection System (IDS) within wireless public network

D. Physical segregation of public wireless network from the company network

A. Change of password of wireless network on weekly basis will not prevent the threat

B. Installation of firewall between both the networks is a good solution but separate physical network is the most safe one

C. Installation of IDS will not prevent the threat.

D. Physical segregation of public wireless network from the company network is the best suitable control in the given situation

121. Which of the following tests simulates a real attack where penetration tester as well as the target both are not having any information of each other:

A. Blind Testing

B. Double Blind Testing

C. Targeted Testing

D. External Testing

A. In blind testing the tester is not having the information about the target but the target does have the information about the tester

B. In Double blind test tester as well as target is not having any information about each other

C. In targeted testing tester is having exhaustive information about the target but target doesn't have the information about the tester

D. External testing has got no concern with blinding effect

122. During the review of IDS logs, an IS auditor notices that some of the traffic coming from Internet appear to have originated from Internal IP address of the Company's Server. Which of the following activities precisely indicate such type of attack?

A. IP Spoofing

B. DOS Attack

C. Social Engineering Attack

D. Network Equipment Failure

A. IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to

conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. In current scenario IDS observes traffic from internet which appears to have IP address originated from company's server hence it's a IP spoofing attack

B. DOS attack refers to a attack where a machine or network resource is made unavailable to its intended users hence this is not the correct choice looking to the given scenario

C. Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Hence this is not the correct choice looking to the given scenario

D. Network Equipment Failure is not the correct choice looking to the given scenario

123. An IS Auditor wants to know that who has been given permission to use a particular system resource. He can BEST verify the same from:

A. Observation

B. Login ID - Password List

C. Access Control List

D. Activity List

A. Observation can be a method for verification of the authorization but access control list is a stronger evidence

B. Login ID - Password List can't be used to verify the required information

C. Access Control list is the best method to verify the permissions given to particular system resources

D. Activity list can't be used to verify the required information

124. An IS auditor, while performing logical access controls review, observed that there are some shared user accounts. The BIGGEST risk resulting from this situation is that:

A. Unauthorized person gaining access through the shared ID

B. User Access Management becomes complex

C. Passwords cannot be decided unanimously

D. User accountability may not be established

A. Using shared user accounts those who have shared the account can gain entry into the system but this is not the biggest risk

B. Complexity of User Access Management is not the risk

C. Undecided unanimous password is not the risk

D. User Accountability may not be established – is the biggest risk if shared user accounts exist

125. Which of the following conditions satisfies the requirements of a two-factor user authentication?

A. Ratina Scan + Fingerprint Scan

B. Smart Card + PIN

C. User ID + Password

D. System Resource ID + GPS

A. Two factor authentication is a technique wherein identification and authentication of the user takes place with two factors: One based on what user has and other based on what user knows. Ratina scan and finger print scan both belong to the first factor hence not the correct choice

B. Smart Card and PIN satisfies both the conditions as stated in choice a) above hence the correct choice

C. Two factor authentication talks only about authentication. User ID is used for identification purpose hence only password will lead to single factor authentication only hence not the correct choice

D. System Resource ID and GPS doesn't satisfy any factor of authentication hence not the correct choice

126. Which of the following is the responsibility of the owner of the Information Asset:

A. Implementation of Security policy within application system

B. Implementation of Access Rules to data and programs

C. Assignment of criticality levels to data

D. Arrange for Physical and Logical security for data

A. Implementation of security policy within application system is the ultimate responsibility of project sponsor

B. Implementation of access rules to data and program is the responsibility of database administrator

C. Assignment of criticality levels to data is the responsibility of owner of the information asset

D. Arrangement for physical and logical security for data is the responsibility of Chief Security Officer

127. During System administration procedures, following should be given 'Read-Only' access:

A. Security Log Files

B. Access Control Lists

C. Logging Options

D. User Profiles

A. Security log files are very important evidence which is useful to detect any unusual behavior or event hence it should be given 'Read-Only' access only.

B. Access Control list requires modification from time to time hence can't be given Read-Only access

C. Logging options require modification from time to time hence can't be given read-Only access

D. User profiles require modification from time to time hence can't be given read-Only access

128. A cracker could obtain passwords without the use of computer tools or programs through the technique of:

A. Phishing

B. Trojan Horse

C. Social Engineering

D. Back Doors

A. In phishing some program or tool is required to obtain password

B. In Trojan horsesome program or tool is required to obtain password

C. In Social Engineering a cracker could obtain passwords without the use of computer tools or programs

D. In Back Doors some program or tool is required to obtain password

129. Which of the following is the technique used in Digital Rights Management to protect Intellectual Property Rights?

A. Hashing

B. Digital Signature

C. Piggybacking

D. Steganography

A. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. However it is not used in digital rights management to protect IPR

B. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. However it is not used in digital rights management to protect IPR

C. Piggybacking is a situation when an authorized person allows (intentionally or unintentionally) others to pass through a secure door. However it is not used in digital rights management to protect IPR

D. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication-to hide the existence of a message from a third party. This technique used in Digital Rights Management to protect Intellectual Property Rights

130. Which of the following is an example of a passive attack initiated through the Internet?

A. Traffic Analysis

B. Email Spoofing

C. DOS Attack

D. Masquerading

A. A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. Traffic Analysis represents the attack

B. Email spoofing is the creation of email messages with a forged sender address. However, traffic analysis represents passive attack in a better manner

C. DOS attack refers to a attack where a machine or network resource is made unavailable to its intended users. However, traffic analysis represents passive attack in a better manner

D. Masquerading refers to pretending to be something/someone else than what actually is. However, traffic analysis represents passive attack in a better manner

131. Which of the following the MOST important accuracy measure for a biometric system:

A. Biometric System Response Time

B. False Acceptance Rate

C. False Rejection Rate

D. Input File Size

A. Biometric System Response time is not the accuracy measure

B. False Acceptance rate refers to rate at which unauthorized persons are accepted by the system. This is the most important accuracy measure

C. False Rejection rate refers to rate at which access of the authorized persons is denied by the bio metric system. However, this is not as critical as false acceptance rate.

D. Input file size is not the accuracy measure

132. The security level of a PKI (Public Key Infrastructure) System depends on:

A. Number of Encryption key bits

B. Length of message

C. Type of Channel being used to send the message

D. Number of Keys

A. Higher the encryption Key size (in bits), higher the security and more it would be difficult to crack the same. Hence security level of a PKI (Public Key Infrastructure) depends on number of encryption key bits

B. Length of message is not the factor to decide security level of PKI

C. Type of Channel being used to send the message is not the factor to decide security level of PKI

D. Number of Keys is not the factor to decide security level of PKI

133. Which of the following is NOT a characteristics of waterfall model of SDLC:

A. Emphasis on planning

B. Implementation of entire system at one time

C. Tight Control

D. Continuous user involvement

A. Emphasis on planning is a characteristics of waterfall model of SDLC

B. Implementation of entire system at one time a characteristics of waterfall model of SDLC

C. Tight Control is a characteristics of waterfall model of SDLC

D. Continuous user involvement is not a characteristics of waterfall model of SDLC

134. An organization having fluctuating and less experienced project teams should go for:

A. Waterfall Model

B. Prototyping Model

C. Agile Methodology

D. Spiral Model

A. Waterfall Model is a very well documented and structured manner and hence organization having fluctuating and less experienced project teams should go for Waterfall Model

B. Prototyping Model is not appropriate for fluctuating and less experienced project teams

C. Agile Methodology is not appropriate for fluctuating and less experienced project teams

D. Prototyping Model is not appropriate for fluctuating and less experienced project teams

135. In which of the following model, Risk Management is given highest importance:

A. Agile Methodology

B. Spiral Model

C. Waterfall Model

D. Prototyping Model

A. Risk Management is given highest importance in Spiral Model hence this is not the correct option

B. Risk Management is given highest importance in Spiral Model

C. Risk Management is given highest importance in Spiral Model hence this is not the correct option

D. Risk Management is given highest importance in Spiral Model hence this is not the correct option

136. Which of the following model of SDLC is said to be MOST adaptive to changing requirements:

A. Rapid Application Development

B. Prototyping Model

C. Agile Methodology

D. Incremental Model

A. Rapid Application Development is not the MOST adaptive to changing requirements

B. Prototyping model is not the MOST adaptive to changing requirements

C. Agile Methodology is the MOST adaptive to changing requirements

D. Incremental model is not the MOST adaptive to changing requirements

137. Which of the following general purpose notational language is used in OOSD (Object Oriented Software Development):

A. Unified Machine Language

B. Unified Modeling Language

C. Unique Modeling Language

D. Unified Object Oriented Language

A. Unified Machine Language is not the term that is used to refer general purpose notational language used in OOSD

B. Unified Modeling Language is the general purpose notational language used in OOSD

C. Unique Modeling Language is not the termthat is used to refer general purpose notational language used in OOSD

D. Unified Object Oriented Language is not term that is used to refer general purpose notational language used in OOSD

138. Which of the following process does start with the feasibility study and lasts even after the Implementation is over:

A. System Testing

B. Requirement Analysis

C. Benefit Realization

D. User Acceptance Testing

A. Benefit realization is the process which starts with the feasibility study and lasts even after the implementation is over hence this is not the correct option

B. Benefit realization is the process which starts with the feasibility study and lasts even after the implementation is over hence this is not the correct option

C. Benefit realization is the process which starts with the feasibility study and lasts even after the implementation is over hence this is the correct option

D. Benefit realization is the process which starts with the feasibility study and lasts even after the implementation is over hence this is not the correct option

139. During which of the following process users and analysts come to agreement as to 'What constitutes the Software to be developed':

A. Requirement Engineering

B. Product Selection

C. Vendor Selection

D. User Acceptance Testing

A. During Requirement engineering process users and analysts come to agreement as to 'What constitutes the Software to be developed'.

B. Before Product selection requirement of the system is already identified.

C. Before Vendor Selection requirement of the system is already identified.

D. User Acceptance testing takes place long after completion of development of the system

140. Which of the following is an example of non-functional requirement for a Hospital:

A. Processing of Patients records with respect to payments received from them

B. Separation of records for insured patients and uninsured patients

C. Department wise Installation of secured POS Terminals

D. Processing the doctors' prescriptions against medicines purchased from in-house medical shop.

A. Processing of Patients records with respect to payments received from them is an example of functional requirements

B. Separation of records for insured patients and uninsured patients is an example of functional requirements

C. Department wise installation of secured POS terminals is an example of non-functional requirement as it is not directly concerned with an operation of a hospital.

D. Processing the doctors' prescriptions against medicines purchased from in-house medical shop is an example of functional requirement.

141. Which of the following is NOT the criteria for vendor selection:

A. Constitution of Vendor

B. Financials of Vendor

C. Commitment to Service

D. Reliability

A. Constitution of vendor doesn't affect the service provided by any vendor hence it is not a criteria for vendor selection.

B. Financials of Vendor is a valid criteria for vendor selection

C. Commitment to service is a valid criteria for vendor selection

D. Reliability is a valid criteria for vendor selection

142. Which of the following method does use statistical approach to product evaluation:

A. Questionnaire Method

B. End User Acceptability

C. Proof of Concept (PoC)

D. Point Scoring Analysis

143. An application has seven modules. Out of them, 4th Module is changed by following a formal change management process. Which of the following testing should be performed to see that the 4th Module maintains integrity with other modules:

A. Stress Testing

B. Unit Testing

C. Regression Testing

D. Functional Testing

A. Stress testing is a software testing activity that determines the robustness of software by testing beyond the limits of normal operation.

B. Unit testing is a software development process in which the smallest testable parts of an application, called units, are individually and independently scrutinized for proper operation.

C. Regression testing is a type of software testing that seeks to uncover new software bugs, or regressions, in existing functional and non-functional areas of a system after changes such as enhancements, patches or configuration changes, have been made to them. Thus, the given scenario is falling under Regression Testing

D. Functional Testing is a testing technique that is used to test the features/functionality of the system or Software

144. In which of the following testing, concept of stubs (dummy entities) is used:

A. Top down testing

B. Bottom up testing

C. Stress Testing

D. Regression Testing

A. In Top Down testing concept of stubs (dummy entities) is used because when the higher level node is tested, the nextlower level of the same has to be assumed as a dummy entity to test the higher level node. Once the higher level nodes are tested the lower level stubs are replaced with the actual entity and it is tested further keeping stubs at the next lower level.

B. In bottom up testing stubs (dummy entities) are not required as the testing starts with the lowest level node.

C. In stress testing, concept of stubs (dummy entities) is not used.

D. In regression testing, particularly, concept of stubs (dummy entities) is not used.

145. Recovery Testing is normally a part of

A. Unit Testing

B. System Testing

C. Integration Testing

D. User Acceptance Testing

A. Recovery testing is normally conducted when the whole system is being tested hence it is not a part of unit testing

B. Recovery testing is normally conducted when the whole system is being tested hence System testing

C. Recovery testing is normally conducted when the whole system is being tested hence it is not a part of integration testing

D. Recovery testing is normally conducted when the whole system is being tested. User Acceptance Test is undertaken once the system testing is over

146. In which of the following type of testing, data is processed in production like systems and outcome is analyzed for real life conditions:

A. Automated Testing

B. Beta Testing

C. Integrated Test Facilities

D. Quality Assurance Testing

A. Automated Testing indicates the method of testing which is happening with some

automation. However, it has no concern with the type of data it is processing, whether real life conditions or fabricated ones.

B. Beta Testing has no concern with the type of data and style of processing

C. In Integrated test facilities (ITF) data is processed in production like systems and outcome is analyzed for real life conditions

D. Quality assurance testing has no concern withthe type of data and style of processing

147. Which of the following implementation approach is MOST risky and requires a great deal of planning:

A. Direct Cut off Implementation

B. Phased Implementation

C. Pilot Implementation

D. Parallel Implementation

A. In Direct cut off implementation approach, on one stroke only, old system is discontinued and new system is put into operation hence it is most risky and requires a great deal of planning

B. Phased implementation is a convenient option when resources are scarce and the shock of single stroke implementation and risk is to be avoided

C. Pilot Implementation is not a risky one as the system is implemented on a very small scale initially as a pilot version and upon success it is replicated all over the enterprise

D. Parallel approach is the safest approach however consumes much of the resources

148. A relatively small organization of risk averse nature but having ample resources, is consulting an IS Auditor for BEST implementation strategy for its newly developed ERP System. The IS Auditor should suggest:

A. Abrupt Change Over

B. Phased Change Over

C. Pilot Change Over

D. Parallel Change Over

A. Facts of the question says that the organization is of risk averse nature so abrupt change over couldn't be supported

B. Phased change over is relatively less risky, but if ample resources are available then parallel change over can be suggested as it will have minimum risk.

C. Looking to the small size organization, pilot change over may not be required

D. Looking to the risk averse nature and availability of ample resources, parallel change over looks the best implementation strategy

149. While reviewing a sample on change control procedure, IS Auditor is MOST concerned about the following fact:

A. A change is not made as per the Industry standards

B. The change is implemented by the developers, directly in the production libraries

C. The same change was requested two years back but was rolled back subsequently

D. Users are not trained to work in the changed environment

A. Non compliance with industry standards is a concern but not as big as the one when it's implemented by the developers directly in the production libraries

B. The change implemented by the developers, directly in the production libraries is the biggest concern as it may compromise the integrity aspect

C. Change request of a rolled back change is not a concern which is as big as one listed in option B.

D. Non trained users is not a concern which is as big as one listed in option B

150. During SDLC, when a project team has to develop an application using a particular technology which is new to them, it takes the help of:

A. Domain Specialist

B. Technology Specialist

C. Project Manager

D. Technology Designer

A. Domain specialist can be consulted when the area of work is new to the development team

B. Technology specialist is the proper person who can be consulted when a particular technology which is being used is new to the development team

C. Project Manager has the responsibility of the planning, execution and closing of any project

D. Normally, the term technology designer is not used anywhere to designate any person

151. _____ is responsible for monitoring and controlling costs, timelines and risks.

A. Programmer

B. Module/Team Leader

C. Project Manager

D. Quality Assurance Team

A. Programmer is a person who writes computer software. He is not responsible for monitoring and controlling costs, timelines and risks

B. A module/team leader is someone who provides guidance, instruction, direction and leadership to a group of other individuals for the purpose of achieving a key result or group of aligned results. The module/teamleader reports to a project manager

C. Project manager is responsible for monitoring and controlling costs, timelines and risks

D. Quality Assurance team is responsible for testing and monitoring software engineering processes and methods to ensure quality. It is not responsible for monitoring and controlling costs, timelines and risks

152. In which of the following testing, software is released as a trial version to get feedback from its users as regard to the improvements to be made in the software:

A. Quality Assurance Testing

B. Functional Testing

C. Alpha Testing

D. Beta Testing

A. Quality Assuranceincludes testing and monitoring software engineering processes and methods to ensure quality.

B. Functional testing verifies whether software is functioning the way it should function

C. In alpha testing, software is released as a trial version to get feedback from its users as regard to the improvements to be made in the software

D. In beta testing product/software is send outside the organization to get it tested in real world scenarios

153. What data should be used for regression testing:

A. Different data than used in the previous test

B. The most current production data

C. The data used in original test

D. Data produced by test data generator

A. Looking to the nature of regression testing, it should be carried out by using the data used in original test only hence this is not the correct choice

B. Looking to the nature of regression testing, it should be carried out by using the data used in original test only hence this is not the correct choice

C. Looking to the nature of regression testing, it should be carried out by using the data used in original test only

D. Looking to the nature of regression testing, it should be carried out by using the data used in original test only hence this is not the correct choice

154. Which of the following group/individuals should assume overall direction and responsibility for costs and timetables of system development projects:

A. Project Manager

B. Project Steering Committee

C. Senior Management

D. User Management

A. Project manager is responsible for monitoring and controlling costs, timelines and risks. However, overall responsibility for cost and time table remains with the project steering committee only

B. Project Steering committee assumes overall direction and responsibility for costs and timetables of system development projects

C. Senior management is a generic choice compared to project steering committee

D. User management doesn't assume overall direction and responsibility for costs and timetables of system development projects

155. An IS auditor is assigned to help design the data security aspects of an application under development. Which of the following provides the MOST reasonable assurance that corporate assets are protected when the application is being certified for production:

A. A review conducted by the internal auditor

B. A review conducted by the assigned IS auditor

C. Specifications by the user on the depth and content of the review

D. An independent review conducted by another equally experienced IS auditor

A. Most reasonable assurance can be obtained only if independent review is conducted by other IS auditor hence this is not the correct choice

B. Assigned IS Auditor, if conducts review, then independence will be compromised

C. Most reasonable assurance can be obtained only if independent review is conducted by other IS auditor hence this is not the correct choice

D. An independent review conducted by another equally experienced IS auditor provides the MOST reasonable assurance

156. The PRIMARY role of an IS auditor during the system design phase of an application development project is to:

A. ensure all necessary controls are included in the initial design.

B. advise the development manager on adherence to the schedule.

C. advise on specific and detailed control procedures.

D. ensure that the design accurately reflects the requirement.

A. Design is the blue print for all future development of the system and should primarily reflect the requirements of the organization hence this is not the best choice

B. advising the development manager on adherence to the schedule is not the primary role of IS auditor during system design phase

C. Advising on specific and detailed control procedures are important but primary role is to ensure that the design reflects the requirements

D. Design is the blue print for all future development of the system and should primarily reflect the requirements of the organization hence the primary role of an IS auditor during system design phase of an application development is to ensure that the design accurately reflects the requirement

157. Which of the following relationship among the programmes facilitates effective program maintenance:

A. Less cohesive and loosely coupled programs

B. More cohesive and strongly coupled programs

C. More cohesive and loosely coupled programs

D. Less cohesive and strongly coupled programs

A. Coupling is the manner and degree of interdependence between software modules; a measure of how closely connected two routines or modules are.Whereas cohesion measures the strength of relationship between pieces of functionality within a given module. A first-order principle of software architecture is to increase cohesion and reducecoupling. Hence this is not the correct choice

B. As per the description in choice a), this is not a correct choice

C. Coupling is the manner and degree of interdependence between software modules; a measure of how closely connected two routines or modules are.Whereas cohesion measures the strength of relationship between pieces of functionality within a given module. A first-order principle of software architecture is to increase cohesion and loosen coupling. Hence this is the correct choice

D. As per the description in choice a), this is not a correct choice

158. At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. Recommend that problem resolution be escalated.

B. Ignore the error, as it is not possible to get objective evidence for the software error.

C. Report the error as a finding and leave further exploration to the auditee's discretion.

D. Attempt to resolve the error

A. If IS auditor observes that an intermittent software error has not been taken up for correction he must recommend that problem resolution be escalated

B. IS auditor should not ignore the error

C. Reporting is good but first choice is more appropriate

D. It is not IS auditor's job to resolve the error unless specifically required by the engagement terms

159. Which of the following is a technique that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality:

A. Rapid application development

B. Critical path methodology

C. Function point analysis

D. Program evaluation review technique

A. Rapid Application Development is a system development methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality

B. Critical path methodology is not a system development methodology/technique

C. Function Point Analysis is not a system development methodology/technique

D. Program evaluation review technique is not a system development methodology/technique

160. When a systems development life cycle (SDLC) methodology is inadequate, the MOST serious immediate risk is that the new system will:

A. be completed late.

B. exceed the cost estimates.

C. be incompatible with existing systems.

D. not meet business and user needs.

A. This may be a risk but not meeting business and user needs is most serious immediate risk

B. This may be a risk but not meeting business and user needs is most serious immediate risk

C. This may be a risk but not meeting business and user needs is most serious immediate risk

D. When a systems development life cycle (SDLC) methodology is inadequate, the MOST serious immediate risk is that the new system will not meet business and user needs

161. Which of the following should be reviewed FIRST by an IS Auditor in audit of application software:

A. Business Model

B. Business Application

C. Business Laws

D. Business Controls

A. It is important to review business model first while auditing application software for a business entity

B. Business Application itself is being audited hence this is not correct choice

C. Business Laws are important but first, business model has to be reviewed

D. Business Controls are important to verify but first, business model has to be seen

162. Initial adoption of Business Model adopted by an organization is dependent upon:

A. Business Application

B. Business Objective

C. Controls in business applications

D. Business Laws

A. Reverse is the truth. Adoption of business application is dependent upon adoption of business model. Hence this is not a correct choice

B. Objective of the business decides the adoption of business model hence this is a correct choice

C. Controls in business applications do not decide the adoption of business model

D. Business laws are important factors for adoption of business model but business objective is more important deciding factor for adoption of business model

163. Which of the following data validation edits is effective in detecting transposition and transcription errors:

A. Range Check

B. Validity Check

C. Check Digit

D. Redundancy Check

A. Range Check is used to see that the input is within predetermined range or not hence this is not the correct choice

B. Validity check is used to see that only allowed input is entered and taken by the system for processing

C. Check Digit is a redundant bit which takes care of the arrangement of bits within the word so that transposition and transcription error is detected hence this is a correct choice

D. A redundancy check is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Check Digit is a kind of redundancy check only and appears more specific to the situation given in the question

164. Which of the following controls can BEST validate a transaction:

A. Authorization of a transaction by supervisory personnel in adjacent department.

B. Authorization of transaction by department supervisor prior to sending it for batch processing.

C. Key field verification during Data Entry.

D. Use of programs to check the transaction against the criteria set by the management.

A. Validation of a transaction by a supervisory personnel will not be as effective as validation by a computer program

B. Pre-process validation of a transactionby a supervisory personnel will not be as effective as validation by a computer program

C. Key field verification during data entry would be a good input control, however, transaction validation could be best handled by a computer program

D. Use of programs to check the transaction against the criteria set by the management can BEST validate a transaction

165. System Administrator of a public utility company has to change the access rights of users frequently due to changes in roles, on account of leaves and/or transfer of employees. Which of the following system administrator should do first?

A. Verify authorization.

B. Create new user id.

C. Change access rights.

D. Grant the new role.

A. Before carrying out any change to the access rights of users, authorization should be verified first

B. Before creating a new user id, authorization should be verified

C. Before carrying out any change to the access rights of users, authorization should be verified first

D. Before granting the new role, authorization should be verified

166. Programmers frequently create entry points into a program for debugging purposes and/or insertion of new program course at a later date. This entry points are called:

A. Logic bombs

B. Trap doors

C. Trojan horses

D. Worms

A. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

B. A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. Trap doors have been used legitimately for many years by programmers to debug and test programs.

C. Trojan Horses are malicious codes which hide inside a host program that does something useful.

D. Worms are malicious programs that attack a network by moving from device to device and create undesirable traffic.

167. Which of the following would BEST ensure proper updating of critical fields in a master record?

A. Field checks.

B. Control Totals.

C. Reasonableness checks.

D. Before and after maintenance report.

A. Field Check is the validation technique that ensures the proper updating of critical fields in a master record

B. Control total is a total, composed of several numbers taken from a file, which is calculated before, during, and after processing

C. Reasonableness check is a test to determine whether a value conforms to specified criteria

D. Before and after maintenance report will not ensure proper updating of critical fields in a master record as effective as field check will do

168. An IS auditor was asked to audit ERP implementation. The auditor did not have prior experience of ERP implementation. The auditor should:

A. Refuse the assignment in absence of required skills.

B. Attend the training program on implementation of ERP.

C. Conduct the audit with due professional care.

D. Take help of independent skilled professional.

A. IS audit is all about team work. A person cannot be the expert of all the fields. If

he is not having prior experience, help can be taken from skilled professional. There is no need to refuse the assignment

B. Attending the training program on implementation of ERP can be a part of requirements for future assignment, however, currently one may go ahead with the help of independent skilled professional

C. If one is not having prior ERP implementation know how then even due professional care may not come at help if a critical issue arises

D. If the auditor did not have prior experience of ERP implementation, he should take help of independent skilled professional

169. Centralized data base server is being accessed by users from various geographical locations. Concurrency controls provided in this system primarily ensures:

A. Integrity of data.

B. Usability of data.

C. Confidentiality of data.

D. Availability of data.

A. Concurrency control is a database management systems (DBMS) concept that is used to address conflicts with the simultaneous accessing or altering of data that can occur with a multi-user system. Thus it helps to maintain integrity of data

B. Concurrency control doesn't ensure usability of data

C. Concurrency control, primarily doesn't ensure confidentiality of data

D. Concurrency control, primarily doesn't ensure availability of data

170. Exception reports generated by application systems are useful to the management:

A. As compensating control for segregation of duties.

B. As feedback on the processing status.

C. In resolving problems in data processing.

D. In evaluating supervisory performance.

A. It is not a compensating control for segregation of duties as it's detective control in nature at the first place

B. An exception report is a type of summary report that identifies any events that are outside the scope of what is considered a normal range. They are useful to the management as a feedback on the processing status

C. Exception reports may help in resolving problem in data processing but primarily they are useful to the management as a feedback on the processing status

D. Exception reports are not primarily useful in evaluating supervisory performance

171. Which of the following will help IS auditor in determining the effectiveness of help desk operations:

A. Problem aging analysis

B. Problem escalation report.

C. Query log maintained by help desk.

D. Awareness level of end users.

A. Effectiveness of helpdesk operations can't be verified by problem aging analysis as there are many factors affecting aging analysis apart from effectiveness of help desk operations

B. Problem escalation report will not help the IS auditor in determining the effectiveness of help desk operations primarily

C. Effectiveness of helpdesk operations can be determined by reviewing query log maintained by help desk

D. Awareness level of end users has nothing to do with effectiveness of help desk operations

172. A company disposing of personal computers that once were used to store confidential data should first:

A. Demagnetize the hard disk.

B. Low level format the hard disk.

C. Delete all data contained on the hard disk.

D. Defragment the data contained on the hard disk.

A. Hard disk is a magnetic media. Demagnetization of hard disk is the safest way to prevent exposure of confidential data that was once stored on it

B. Low level formatting the hard disk can be applied but demagnetization is more safe

C. Data contained on the hard disk, although deleted, can still be recovered from it using some tools available in the market

D. Defragmentation optimizes the storage space and doesn't remove the data. It is used for maintenance of file system

173. A tax calculation program maintains several hundred tax rates. The BEST control to ensure that Tax rates entered into the program are accurate is:

A. Independent review of the transaction listing.

B. Programmed edit check to prevent entry of invalid data.

C. Programmed reasonableness checks with 20% data entry range.

D. Visual verification of data entered by the processing department.

A. Independent review of the transaction listing should better be reviewed when processing controls are verified

B. Programmed edit check to prevent entry of invalid data is the best input control to ensure that tax rates entered into the program are accurate

C. Programmed reasonableness checks with 20% data entry range in the current scenario is not as effective as programmed edit check

D. Visual verification of data by the processing department is not as effective as the edit check is while entering the tax rate. Moreover, the same is subject to error due to manual intervention

174. Which of the following Data Base Administrator activities is unlikely to be recorded on detective control logs:

A. Deletion of a record.

B. Change of a password.

C. Disclosure of a password.

D. Changes to access rights.

A. If record is deleted in the database, it can be recorded in the control log

B. If password is changed, it can be recorded in the control log

C. Disclosure of the password may not happen on the system and is unlikely to be recorded on detective control log

D. If access rights are changed, it can be recorded in the control log

175. The primary reason for replacing cheques with electronic fund transfer(EFT) systems in the accounts payable area is to:

A. Make the payment process more efficient.

B. Comply with international EFT banking standards.

C. Decrease the number of paper based payment forms.

D. Reduce the risk of unauthorized changes to payment transactions.

A. Due to EFT, payment process becomes more efficient. However, the primary purpose to replace cheques with EFT was to decrease number of paper based payment forms

B. Compliance with International EFT banking standards was not the reason for replacing cheques with EFT System. Rather as we moved from cheques to EFT systems, international EFT banking standards were required to be complied with

C. To decrease the number of paper based payment forms was the primary reason for replacing cheques with electronic fund transfer(EFT) systems in the accounts payable area

D. Reduce the risk of unauthorized changes to payment transactions was not the reason for replacing cheques with EFT System

176. Which of the following is an implementation risk within the process of decision support systems(DSS):

A. Management control.

B. Semi structured dimensions.

C. Changes in decision processes.

D. Inability to specify purpose and usage patterns.

A. Management control is not the implementation risk within the process of decision support system

B. Semi structured dimensions themselves are not the implementation risk within the process of decision support system (DSS)

C. Changes in decision processes are not the implementation risk within the process of decision support system

D. Inability to specify purpose and usage patterns is an implementation risk within the process of decision support systems(DSS)

177. Which of the following is a strength of client/server security system:

A. Change control and change management procedures are inherently strong.

B. User can manipulate data without controlling resources on the main frame.

C. Network components seldom become obsolete.

D. Access to confidential data or data manipulation is strongly controlled.

A. Inherently strong change control and change management procedures is a very important strength of client server security system

B. User can manipulate data without controlling resources on the main frame is one of the regular features of client server security system

C. Network components seldom become obsolete - is not the strength of client server security system

D. Access to confidential data or data manipulation is strongly controlled - isone of the regular features of client server security system

178. While auditing IT application infrastructure, the IS auditor observed that there were no procedure defined for the performance monitoring of a third party vendor who was assigned the maintenance of hardware with a clause for 99% uptime during business hours. The BEST course for the auditor is:

A. To suggest procedures to functional management and report to top management.

B. To consult legal counsel for non performance by the vendor.

C. To request the vendor management to provide necessary uptime reports.

D. To evaluate the performance of third party vendor for estimating expected performance.

A. The best course for the auditor is to suggest procedures to functional management and report to top management

B. No facts regarding non performance of vendor are given in the question. Hence this choice is not proper

C. Reliability aspect is very crucial while requesting the vendor management to provide necessary uptime reports relating to his work only

D. Evaluation of the performance of third party vendor for estimating expected performance is not the proper course of action for the auditor in the absence of any procedure

179. While posting a message on facebook, if user posts the same message again, facebook gives a warning. The warning indicates following type of control:

A. Limit check.

B. Dependency check.

C. Range check.

D. Duplicate check.

A. Limit check means a check to determine if a value entered into a computer system is within acceptable minimum and maximum values

B. DependencyCheck is a utility that identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities

C. A range check is a check to make sure a number is within a certainrange

D. Duplicate check is a check that keeps track of the events to see that they don't happen more than once except intended by the user. Hence a warning raised by facebook on posting of same message again is the example of duplicate check

180. Company's billing system does not allow billing to those dealers who have not paid advance amount against proforma invoice. This check is BEST called as:

A. Limit check.

B. Dependency check.

C. Range check.

D. Duplicate check.

A. Limit check means a check to determine if a value entered into a computer system is within acceptable minimum and maximum values

B. Dependency Check is a utility that identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities. Thus if system doesn't allow billing to dealers who have not paid advance amount against proforma invoice is an example of dependency check

C. A range check is a check to make sure a number is within a certainrange

D. Duplicate check is a check that keeps track of the events to see that they don't happen more than once except intended by the user.

181. While auditing e-commerce transactions auditors key concern includes all except:

A. Authorization.

B. Authentication.

C. Major supplier.

D. Confirmation.

A. While auditing e-commerce transactions, authorization is one of the key concerns

B. While auditing e-commerce transactions, authentication is one of the key concerns

C. Major supplier is not the key concern of auditor while auditing e-commerce transactions

D. While auditing e-commerce transactions, confirmation/acknowledgements is one of the key concerns

182. An IS auditor processes a dummy transaction to check whether the system is allowing cash payment exceeding Rs.20000. This check represents which of the following evidence collection techniques:

A. Inquiry and confirmation.

B. Recalculation.

C. Inspection.

D. Re-performance.

A. Inquiry and confirmation is normally applied when some information is to be retrieved from some department or a person or a group of persons

B. Recalculation refers to checking the mathematical accuracy of documents or records

C. Inspection refers to, most generally, an organized examination or formal evaluation exercise

D. Re-performance is the auditor's independent execution of procedures or controls that were originally performed as part of the entity's internal control, either manually or through the use of CAATs. Here auditor processes a dummy transaction to check whether the system is allowing cash payment exceeding Rs.20000. This represents re-performance technique of evidence collection

183. Which of the following audit tool is most useful to an IS auditor when an audit trail is required:

A. Integrated Test Facility (ITF)

B. Continuous and intermittent Simulation.(CIS)

C. Audit Hooks.

D. *Snapshots*.

A. An integrated test facility (ITF) creates a fictitious entity in a database to process test transactions simultaneously with live input. It can be used to incorporate test transactions into a normal production run of a system

B. Continuous and intermittent simulation (CIS) is a mean of collecting audit evidence concurrently with application system processing when the application system uses a database management system to support updating and querying of application files

C. Audit hooks are embedded in application systems to function as RED flags and to induce internal auditors to act before an error or irregularity gets out of hand.

D. A snapshot is a virtual image of the content of a set of data at the instant of creation. Physically, a snapshot may be a full (complete bit-for-bit) copy of the data set, or it may contain only those elements of the data set that have been updated since snapshot creation. This is most useful to an IS auditor when an audit trail is required

184. An employee has left the company. The first thing to do is to :

A. Hire a replacement employee.

B. Disable his/her access rights.

C. Ask the employee to clear all dues/ advances.

D. Escort employee out of the company premises.

A. Hiring a replacement employee may be made but first of all, his/her access rights should be disabled

B. If an employee left the company, first thing to do is to disable his/her access rights

C. The employee may be asked to clear all dues/advances but first of all, his/her access rights should be disabled

D. Employee may or may not be escorted out of the company premises but first of all,his/her access rights should be disabled

185. Which of the following is the first step in compliance testing? To review:

A. Access security controls.

B. Input controls.

C. Processing controls.

D. Output controls.

A. The first step in compliance testing is to review access security controls

B. Input controls may be reviewed for compliance testing but the first step is to review access security controls

C. Processing controls may be reviewed for compliance testing but the first step is to review access security controls

D. Output controls may be reviewed for compliance testing but the first step is to review access security controls

186. The cashier of a company has rights to create bank master in tally. This error is a reflection of poor definition for which type of control:

A. User control.

B. Application control.

C. Input control.

D. Output control.

A. The cashier of a company should not have right to create bank master in tally, if it has happened, it indicates poor definition of user control

B. The cashier of a company should not have right to create bank master in tally, if it has happened, it indicates poor definition of user control hence, this is not a correct choice

C. The cashier of a company should not have right to create bank master in tally, if it has happened, it indicates poor definition of user control hence, this is not a correct choice

D. The cashier of a company should not have right to create bank master in tally, if it has happened, it indicates poor definition of user control hence, this is not a correct choice

187. What is the first step in preparing a new Business Continuity Plan or in updating an existing one:

A. Risk Management of key business processes

B. Identification of strategically important processes

C. Identification of potential vulnerabilities

D. Business Impact Analysis

A. Risk management is a subsequent step after carrying out identification.

B. Identification of the strategically important processes is the FIRST step in preparing a new BCP or updating an existing one as only after identifying the processes, risk management, vulnerability assessment and business impact analysis can be done.

C. Vulnerability identification is one of the subsequent steps after identification.

D. Business Impact Analysis is undertaken along with Risk Management but after identification.

188. Which of the following BEST suggests the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP):

A. DRP is a sub component of BCP

B. BCP is a sub component of DRP

C. Both BCP and DRP are mutually exclusive

D. BCP and DRP both have almost the same meaning

A. DRP is normally a technological aspect to restore critical processes/IT Services in the event of interruption. And this aspect is a part of overall Business Continuity Planning.

B. BCP is not a sub component of DRP, however, the inverse is true.

C. BCP and DRP are not mutually exclusive. DRP is a part of BCP.

D. *BCP and DRP are different and DRP is part of BCP.*

189. Which of the following plan is MOST specifically used to recover a facility rendered inoperable, including relocating operations into a new location?

A. Disaster Recovery Plan

B. Business Continuity Plan

C. Back Up Plan

D. Contingency Plan

A. DRP is a technological aspect to restore critical processes/IT Services in the event of interruption. Hence DRP is most specifically used to recover a facility rendered inoperable, including relocating operations into a new location.

B. BCP also covers the given scenario as it includes DRP. However, DRP is MOST specific to the given scenario.

C. Backup plan has got no relevance with the given scenario.

D. Contingency Plan covers the steps to be followed immediately after the disaster occurs. Thus not having direct link with the given scenario.

190. While evaluating Business Continuity Plan, "An IS auditor should evaluate an organization's preparedness for pandemic outbreaks", what does 'pandemic' mean in the above statement?

A. Terrorist events

B. Malicious acts

C. Epidemics or outbreaks of infectious disease in humans

D. Natural disasters

A. Pandemic is not a terrorist event.

B. Pandemic is not a malicious act.

C. Pandemic refers to the infectious disease in humans which must be considered while preparing BCP.

D. Pandemic disaster can't purely be a natural disaster.

191. An organization running a critical information system and cannot afford the down time of more than 10 seconds will have _____ in case of a disaster.

A. Lessen recovery costs, higher downtime costs

B. Lessen downtime costs, higher recovery costs

C. Higher downtime costs, higher recovery costs

D. Lessen downtime costs, lessen recovery costs

A. This will happen when affordable downtime is very high.

B. When allowable downtime is 10 seconds or less, system needs to be up and running in not more than 10 seconds of the disaster. To make this possible, recovery cost i.e. cost incurred to resume the system - as it was before the disaster - will have to be incurred much higher. And consequently due to less downtime, downtime cost i.e. cost incurred due to down system will be minimal.

C. Normally both the costs are not high simultaneously.

D. Normally both the costs are not less simultaneously when there is a critical system to be restored.

192. Absence of which of the following is the BIGGEST concern for an IS auditor who is auditing a Business Continuity Plan?

A. Procedure for declaring a disaster

B. Identification for contract information

C. Circumstances under which a disaster should be declared

D. Explanation of the recovery process

A. This is also an important concern but it comes to use only once circumstances for declaring the disaster are declared.

B. Absence of Identification for contract information is a concern but not as critical as declaring the circumstances for BCP invocation.

C. Without specifying the trigger points for invoking BCP/DRP, no BCP/DRP will make a sense and it will become useless. Without this, all remaining concerns are of no value.

D. Absence of Explanation of the recovery process is a concern but not as critical as declaring the circumstances for BCP invocation.

193. One of the MOST important outcomes of Business Impact Analysis is a way to group information systems according to their_____

A. Recovery time

B. Down time

C. Value

D. Maintenance Requirements

A. Recovery strategy is selected based on the outcome of BIA. If multiple assets are having the same Recovery time then they are put together under a single recovery strategy in BCP.

B. Downtime is generally not the criteria to group the information system in BIA.

C. Value of the assets is generally not the criteria to group the information system in BIA.

D. Maintenance Requirements is generally not the criteria to group the information system in BIA.

194. Which of the following Business Continuity Insurance Plan covers loss from dishonest or fraudulent acts by employees?

A. Transparency coverage

B. Loyalty coverage

C. Honesty coverage

D. Fidelity coverage

A. Transparency coverage is not a formal name for such insurance.

B. Loyalty coverage is not a formal name for such insurance.

C. Honesty coverage is not a formal name for such insurance.

D. Fidelity refers to faithfulness of a person demonstrated by continuing loyalty and support. Fidelity coverage is a type of insurance plan that covers loss from dishonest or fraudulent acts by employees.

195. _____ is a method for Systems' Risk Ranking, where probability of adverse disruptions is multiplied with monetary impact of disruptions to determine maximum reasonable cost of prevention.

A. Loss Prevention Expectancy (LPE)

B. Risk Loss Product (RLP)

C. Weighted Loss Assessment (WLA)

D. Annualized Loss Expectancy (ALE)

A. Loss Prevention Expectancy (LPE) is not a method for Systems' Risk Ranking.

B. Risk Loss Product (RLP) is not a method for Systems' Risk Ranking.

C. Weighted Loss Assessment (WLA) is not a method for Systems' Risk Ranking.

D. Annualized Loss Expectancy (ALE) is the method for Systems' Risk Ranking where probability of adverse disruptions is multiplied with monetary impact of disruptions to determine maximum reasonable cost of prevention.

196. Which of the following is the BIGGEST concern for an IS auditor while evaluating the Business Continuity Plan?

A. The plan contains conflicting responsibilities

B. The plan is not tested

C. The plan is not read by the team members

D. The plan is not updated for last six months

A. A plan containing conflicting responsibility is a concern but not as big as the one which is not tested.

B. BCP, even though thoughtfully designed and developed, provides no guarantee for its successful execution unless it is tested with the appropriate method. Hence, non-tested BCP is the BIGGEST concern for the IS auditor.

C. If plan is not read by the team members, it is not a biggest concern for the IS Auditor.

D. Requirements for updation of a plan depend on the System and technology changes. It might be possible that it is reviewed for updation once in a year or two. Hence, this is not a biggest concern for the auditor.

197. When an enterprise has an insurance coverage as a part of its Disaster Recovery Plan, which risk treatment approach is followed?

A. Risk avoidance

B. Risk mitigation

C. Risk transfer

D. Risk acceptance

A. Risk avoidance seeks to avoid compromising events entirely. Insurance coverage is not following the risk avoidance approach of risk treatment.

B. Risk mitigation is defined as taking steps to reduce adverse effects of possible threats. Insurance coverage is not following the risk mitigation approach of risk treatment.

C. Risk transfer is a risk management and control strategy that involves the contractual shifting of a pure risk from one party to another. Insurance policy is one such example where by paying premium the risk of loss due to disaster is transferred from policy holder to the insurer.

D. Accepting risk occurs when the cost of managing a certain type of risk is accepted, because the risk involved is not adequate enough to warrant the added cost it will take to avoid that risk. Insurance coverage is not following the risk acceptance approach of risk treatment.

198. Which of the following Business Continuity Planning test is a cost-effective way of simulating a system crash locally without causing much harm to the actual facilities?

A. Preparedness test

B. Paper test

C. Desk based evaluation

D. Pre-test

A. Preparedness test is a localized version of full operational test wherein actual resources are applied in the simulation of system crash and thereby giving a cost-effective way to gradually obtain evidence about the working of plan.

B. In paper test, plan walk through takes place to get idea about the possible service disruption by major participants involved in plan execution. It precedes preparedness test.

C. Desk based evaluation is just another name of paper test.

D. Pre-test is not a type of test. Rather it is a phase of test execution which contains necessary actions to set the stage for the actual test.

199. Effectiveness of Business Continuity Planning (BCP) can be BEST verified by an IS auditor by:

A. Reviewing the alignment of BCP with that of peers in the same industry

B. Reviewing the test results of BCP

C. Verifying cost benefit analysis of BCP

D. Confirming that BCP is approved by Board Of Directors having expertise in the field

A. Different peers have got different needs of having BCP depending upon the type of assets and nature of business. Hence this option is not proper.

B. BCP, even though thoughtfully designed and developed, can be verified for its effectiveness only by reviewing its test results obtained through appropriate test methods.

C. Cost benefit analysis of BCP and test results of BCP are having no bearing on each other. However, effectiveness of BCP can be verified by BCP tests only.

D. Approval by the expert BODs is not as effective as the test results to verify effectiveness of BCP.

200. Which of the following is most suitable method for ensuring up-to-date Business Continuity Plan (BCP)?

A. Yearly full functional tests

B. Continuous Liaison among BCP team members

C. Regular structured walk through tests

D. Keep on changing the team members with the more experienced ones

A. Yearly fully functional tests are quite expensive as well as damaging the system resource many a times as it actually imitates the disaster. Hence, fully functional test is not advisable.

B. Continuous Liaison among BCP team members may initiate the change in BCP but to keep it up-to-date, regular structured walk through tests are must.

C. Regular Structured walk through tests takes place to get idea about the possible service disruption by major participants involved in plan execution. It helps in keeping the plan up-to-date.

D. Keep on changing the team members with the more experienced ones will not make the BCP up-to-date.

ANSWER-SHEET

MCQ No.	Key	MCQ No.	Key	MCQ No.	Key	MCQ No.	Key
1	D	51	B	101	C	151	B
2	B	52	A	102	B	152	C
3	B	53	A	103	D	153	A
4	D	54	C	104	B	154	C
5	A	55	B	105	A	155	D

6	C	56	C	106	A	156	A
7	A	57	A	107	C	157	B
8	B	58	D	108	D	158	A
9	C	59	D	109	B	159	D
10	A	60	B	110	C	160	A
11	D	61	C	111	D	161	C
12	C	62	A	112	A	162	B
13	A	63	B	113	B	163	B
14	C	64	C	114	C	164	A
15	D	65	A	115	B	165	D
16	A	66	C	116	C	166	A
17	B	67	D	117	A	167	B
18	A	68	A	118	C	168	C
19	C	69	B	119	A	169	A
20	D	70	A	120	D	170	B
21	C	71	C	121	C	171	C
22	D	72	D	122	A	172	C
23	C	73	A	123	B	173	A
24	A	74	B	124	C	174	D
25	B	75	C	125	A	175	A
26	D	76	A	126	D	176	B
27	A	77	D	127	B	177	C
28	B	78	B	128	B	178	D
29	A	79	A	129	C	179	A
30	A	80	D	130	D	180	B
31	C	81	C	131	C	181	A
32	A	82	C	132	B	182	D
33	C	83	A	133	D	183	A
34	D	84	A	134	D	184	B
35	A	85	C	135	C	185	C

36	C	86	B	136	A	186	A
37	D	87	C	137	A	187	B
38	A	88	C	138	D	188	C
39	C	89	D	139	C	189	C
40	A	90	B	140	A	190	D
41	A	91	D	141	D	191	A
42	B	92	A	142	A	192	A
43	C	93	D	143	B	193	D
44	A	94	C	144	C	194	B
45	A	95	B	145	A	195	C
46	B	96	C	146	D	196	D
47	D	97	C	147	B	197	D
48	C	98	D	148	A	198	B
49	A	99	A	149	C	199	A
50	B	100	D	150	D	200	A

Mock Assessment Test Paper 3

1. The level of on-line system response time is best determined by which of the following

   A. System planning phase

   B. System Design Phase

   C. System Programming phase

   D. System testing phase

   Option B is the correct answer. On line time indicates how much time is taken between entry of query and its reply and deals with utilisation of system resources which need to be considered during system design phase. Option A is incorrect because it is too early to determine online system response and C and D are incorrect because it is too late to determine on line system response

2. Which of the following tools is most useful in detecting security intrusions

   A. Data mining Tools.

   B. Data optimisation Tools

   C. Data reorganisation tools.

   D. Data access tools.

   Option A is the correct answer. Data mining is a set of automated tools that convert data in the warehouse to some useful information. Data mining techniques could also be used for fraud detection, intrusion detection, abnormal patterns in data. Data optimisation tools improves performance of the database. Data access as the name suggests helps in accessing the right data. Data reorganisation tools helps relocate the data for faster access

3. Which of the following is not a proper definition of workload from a computer capacity perspective

   A. Transactions

   B. Storage

   C. Communications Traffic

   D. Bandwidth

   Option D is the correct answer. Workload is basically the request of the users submitted to the computing resources. Bandwidth describes capacity and not workload. The remaining three options represent the workload.

4. Database application systems have similarities and differences from traditional flat file application systems. Database systems differ most in which of the following control areas.

   A. Referential integrity

   B. Access Controls.

   C. Data editing and validation routines.

   D. Data Recovery

   Option A is the correct answer. Referential integrity means that no record will have reference to the primary key of the non exsistent record. When a record is deleted all other referenced records are automatically deleted. Options B, C and D are incorrect because they are same for flat file and database systems.

5. Which of the following statements is not true?

   A. With a multiplexer the total bandwidth entering the device is normally different from the bandwidth leaving it.

   B. With a concentrator the total bandwidth entering the device is normally different from the bandwidth leaving it.

   C. Devices are available that perform the functions of both concentrators and multiplexers.

   D. Concentrators can give much better utilisation of the available bandwidth than a multiplexer.

   Option A is the correct answer. In case of a multiplexer the total bandwidth entering and leaving are roughly equivalent. Option B is incorrect with a concentrator total bandwidth entering the device and leaving are different. Choice C is incorrect as there are devices that perform the functions of both concentrators and multiplexers. Choice D is incorrect as concentrators can give better utilisation of the bandwidth than a multiplexer.

6. Which of the following is a simple networking device that interconnects two or more local area networks :

   A. Router

   B. Bridge.

   C. Gateway.

   D. Brouter

   Option B is the correct answer. Bridges are networking devices that connect two LANs. Routers regulate traffic between two LANs. Gateways connect dissimilar networks. Brouters combine the features of routers and bridges.

7. Which of the following components of the database structured query language hold the actual data in the database

   A. Schemas

   B. Subschemas.

   C. Tables.

   D. Views.

   Option C is the correct answer. A schema describes (option A) the structure of related tables and views whereas actual data is stored in tables. Views (option D) are derived from tables and are composed as subset of table. A subschema (option B) presents data views of the user.

8. Magnetic storage media sanitization is important to protect sensitive information. Which of the following is not a general method of purging magnetic storage media.

   A. Overwriting.

   B. Clearing.

   C. Degaussing

   D. Destruction.

   Option B is the correct answer. Clearing information means rendering it unrecoverable by keyboard attack with data remaining on the storage media. Option A, C and D are the three general methods of purging magnetic storage media.

9. The possible security threats inherent in a LAN environment include passive and active threats. Which of the following is a passive threat

   A. Denial of message service.

   B. Masquerading

   C. Traffic Analysis

   D. Modification of message service

   Option C is the correct answer. Passive threats do not alter any data in a system. Messages are simply read to gain some knowledge. Since no alteration of data takes place passive threats are difficult to detect. Option A, B and D are examples of active threats. Active threats alter the data rather than simply reading the contents of the signals. A denial of service (option A) occurs when an attacker either destroys or delays the message. Masquerading (option B) is an attempt to gain access to the system by posing as an authorised user. Option D occurs when the attacker modifies, delete the original message and adds fake messages.

10. Which of the following statements is true in a LAN environment

    A. The gateway is responsible for returning acknowledgements

    B. The destination station is responsible for returning acknowledgements

    C. The originating station is responsible for returning acknowledgements

    D. The network operating system is responsible for returning acknowledgements

    Option A is the correct answer. A gateway is a device used for connecting two dissimilar networks. Option b, c and d are incorrect since the gateway are responsible for returning acknowledgements.

11. Which of the following data models is suitable for predetermined data relationships

    A. Hierarchical model

    B. Network model

    C. Relational model

    D. Distributed model

    Option A is the correct answer. Option B provides somewhat general structures compared to hierarchical model Option C relational model is widely accepted as most suitable for end users because its basic formulation is easily understood. Option D can be visualised as having many networks nodes and access paths between the central and local computers. However data security is a major security concern in a distributed environment.

12. Which of the following is a disadvantage of client/server computing

    A. open systems

    B. Freedom

    C. Specialisation

    D. Complexity

    Option D is the correct answer. The disadvantage is technical immaturity and complexity in designing compared with other traditional systems. Option A, C and D are the advantage of client/server computing hence incorrect.

13. Data normalisation is typically found in which of the following database models

    A. Hierarchy data model

    B. Relational data model

C. Net work data model

D. Object data model

Option B is the correct answer. Normalisation is the formal process for eliminating access and update anomalies. Hierarchy data model is incorrect because it can be related to a family tree concept. Network is incorrect because it is depicted using blocks and arrows. Object model is incorrect because it is a model of attributes, relationships in a system.

14. When constructing the communications infrastructure for moving data over a local area network the major implementations choices involve decisions about all of the following except

A. Terminal controllers

B. Repeaters

C. File servers

D. Bridges.

Option A is the correct answer. The controller is a logic device that directs all the tasks that the terminal must perform. Repeaters (option B) merely repeat data packets or electrical signals between cable segments. They basically regenerate the signal at its original strength. File server (option C) send and receive data between a workstation and server and its main purpose is to make files, printers available to users. Bridge (option D) connects similar or dissimilar LANs together to form a extended LAN.

15. Which of the following transmission media is unsuitable for handling intra-building data or voice communications

A. Twisted pair

B. Coaxial Cable

C. Optical fibre

D. Microwave transmission.

Option D is the correct answer. Microwave communication is a point to point transmission using radio frequency signals and is more appropriate for long distance transmission. Option A and B is the most widely used medium for data transmission in local area networking. Option C uses light signals to carry a stream of data at extremely high modulation rates though highly secure and sturdy.

16. If any link should fail only the terminal on that specific link will be affected by the line outage is true with which of the following network topologies

A. Star

B. Tree

C. Ring

D. Mixed.

Option A is the correct answer. The star topology uses Central Hub which connects workstation and servers. Now because of the Central Hub even if one of the workstation fails rest all are active. A tree topology is a variation of bus. A disadvantage of this topology is if one of the workstation goes down all other workstation fails because of interdependency. In Ring topology (option C) there is no central hub and all personal computers are connected successively forming a ring. A disadvantage of this topology is if one of the workstation goes down all other workstations fail. A mixed topology (option D) is a combination of star, bus, tree or ring topologies

17. Which of the following network topologies is best suited where each terminal has a large volume of data traffic and must operate at a high data rate on a leased line

A. Star

B. Tree

C. Ring

D. Mixed.

Option A is the correct answer. Tree topology (option B) is incorrect due to installation of the long single main cable. Ring topology (option C) is incorrect as data is looped around a ring till it reaches the proper host computer. Mixed topology (option D) is incorrect because of mixed structures resulting in unpredictable performance rates.

18. A sophisticated network line monitoring device is called

A. Line Monitor

B. Protocol Analyzer

C. Barometer

D. Voltmeter.

Option B is the correct answer. A protocol analyser is a sophisticated networking line monitoring tool as it traps data or performs statistical analysis of data. Line monitior (option A) is a passive device and not as sophisticated as protocol analyser. Barometer (option C) is used for measuring atmospheric pressure and voltmeter (Option D) is used for measuring current.

19. Wireless Local area networks operate in which of the following layers of the ISO/OSI Reference model

A. Physical and data layers

B. Data and network link layers

C. Transport and presentations layers

D. Application and session layers

Option A is the correct answer. The physical layer addresses areas such as frequencies used and modulation techniques employed and data link layer deals with how the network is shared between links.

20. During the acceptance testing of a new LAN installation which of the following test plan items requires proactive thinking.

A. Connectivity and interoperability.

B. Network performance

C. Cable plant integrity

D. User application systems

Option C is the correct answer. In cable plant integrity it is helpful to test each section of the cable as finding cable faults after installation can be difficult and tedious. Choice A is incorrect as many LANs provide a variety of connectivity and interoperability. Choice B is incorrect as most LANs support many users and hence need to provide many services concurrently. User application system (option D) is incorrect as it is important to thoroughly exercise LAN software to be sure that there are no memory-cram problems at the workstations.

21. The Database administrator is not responsible for which of the following functions

A. Physical design of the database.

B. Logical design of the database

C. Security of the database

D. Performance of the database

Option B is the correct answer. DBA is responsible for physical design (option A) security (option C) and performance (option D).

22. Which of the following is often the greatest failing of distributed system management solutions.

A. Scalability.

B. Heterogeneity

C. Security

D. Synchronization

Option C is the correct answer. Managing security is a major problem since distributed system operate in hostile environments. Option A is incorrect because scalability can be achieved by allowing more units to be added to the system. Option B is incorrect as heterogeneity can be handled properly with open system designs. Choice D is incorrect as synchronisation are standard problems of distributed systems and can be handled properly.

23. Which of the following client/server implementation approaches is the least complex.

A. File transfer.

B. Applications programming interface

C. GUI based operating system

D. Peer-to-peer communications

Option A is the correct answer. Option B is incorrect application programming interface is often selected as a first step in moving to more complex client/server strategies. Option C is incorrect because GUI based operating systems is the next step in complexity after API. Option D is incorrect as because peer-to-peer communication is most complex of all.

24. Payroll master file updates are sent from a remote terminal to a mainframe program on a realtime system. A control which works to ensure accuracy of the transmission is a

A. Echo Checking.

B. Protection ring

C. Hash total

D. Integrated test facility

Option A is the correct answer. An echo check provides a feedback loop by transmitting data received back to the source unit for validation with the original data. It is a hardware control. A protection ring (option B) prevents accidental writing on a tape file for most batch systems hence should not be utilised for real time systems. Option C is incorrect as hash totals are utilised to control data sent to a batch system and not real time system. option D is incorrect as integrated test facility are useful in testing real time systems but cannot be utilised to ensure completeness of data transmission.

25. An insurance firm uses a wide area Network to allow agents away from home office to obtain current rates and client information and to submit approved claims using notebook computers and dial in modems. In this situation which of the following methods would provide the best data security.

    A. Dedicated phonelines.

    B. Call back features

    C. Frequent changes of user IDS and passwords

    D. End to end data encryption

    Option D is the correct answer. Option A is incorrect as dedicated phonelines would not be effective or available to field agents. Option B is incorrect as field agents would not always be located at the same phone line to permit dial up call back usage. Option C is incorrect as passwords may be compromised by computer software.

26. The information systems and audit directors agreed that maintaining the integrity of the system that kept inventory data was crucial for distributing correct product quantities to stores. The best way to ensure the integrity of this application software is through.

    A. Access controls for terminals in the receiving department.

    B. Audit trails for items sold and received

    C. Change controls for inventory software

    D. Monitoring software for the network

    Option C is the correct answer. Change control would ensure that only authorised and tested programs are run in production. Access controls (Option A) would ensure only authorised persons have access to the system but is not enough in itself to ensure integrity of application software. Audit trails (option B) permits audit of transactions update to data files and not programs. Monitoring software (option D) is designed to monitor performance for specified functions.

27. A dial up order entry system is used by salesmen to enter customer orders from the customers location via portable computers assigned to each salesman. However unauthorised persons using their own system have entered frauduent transactions in to the order entry system. A control that would permit only authorised persons using portable computers to access the system is:

    A. A callback procedure

    B. An error correcting code

    C. Frequent access code revalidation

D. Modem equalisation

Option C is the correct answer. Required access code revalidation on a recurring basis would prevent unauthorised persons to enter unauthorised transactions. Option A is incorrect since the salesman have no fixed telephone number call back procedures would not control this access. Error correcting codes (option B) repair damaged transmissions but cannot detect or prevent unauthorised access. Modem equalisation (option D) controls for line errors but cannot detect or prevent unauthorised access.

28. Compared to closed systems open systems are characterized by

A. Less expensive components

B. Decreased interoperability

C. More dependence on particular vendors

D. More restricted portability

Option A is the correct answer

29. A major risk involving the use of the packet switching network technique is that

A. it is possible for the packets to arrive at their destinations out of sequence

B. it is not possible to vary the routing of packets depending on network conditions

C. Terminals that are attached to a public data network may not have enough intelligence

D. Terminals that are attached to a public data network may not have enough storage capacity

Option A is the correct answer. Terminals that are attached directly to a public data network (Options C and D) must have enough intelligence and storage capacity to break the large messages in packets and reassemble them in proper sequence.

30. Protocols would not address which of the following

A. Message size, sequence and format

B. Message routing instructions

C. Error detection and correction

D. Message authentication

Option D is the correct answer. A protocol is a set of rules governing a specific sequence of events and defines method of formatting bits of data and messages for transmission, routing and identification of messages including error detection and correction. However it does not address message authentication.

31. Which of the following is an inappropriate control over telecommunication hardware

    A. Logical Access controls

    B. Security over wiring closets

    C. Contingency plans

    D. Restricted access to test equipment

    Option A is the correct answer. Logical access control is a software based control whereas option B, C and D are physical security controls over telecommunications hardware.

32. Which of the following statements is true with respect to data dictionaries

    A. A data dictionary must be always be active to be useful

    B. An active data dictionary must be dependant on database management systems

    C. A passive data dictionary is an important feature of database management systems

    D. A data dictionary can exist only with a database system

    Option B is the correct answer. In case of active dictionary there is no option which means that data dictionary and the database management system go together. Option A is incorrect since both active and passive dictionaries are useful. Option C is incorrect as a passive data dictionary may or may not require a check for currency of data description before execution of program. Option D is incorrect because non database systems can have data dictionaries.

33. Which of the following layers of the ISO/OSI Reference Model handles error detection and correction

    A. Data link

    B. Physical

    C. Network

    D. Application

    Option A is the correct answer. Option B is incorrect because physical layer addresses transmission medium, medium access etc. Option C is incorrect as network layer addresses deadlocks, etc. Option D is incorrect as application layer addresses dataflow modelling, file management etc.

34. Which of the following allows transmission of sequential elements with or without interruption

A. Serial to parallel conversion

B. Parallel to serial conversion

C. Serial Transmission

D. d Parallel transmission

Option C is the correct answer. Option A is incorrect because serial to parallel conversion is the conversion of a stream of data elements received one at a time into a stream consisting of multiple data elements transmitted simultaneously. Option B is incorrect because it entails conversion of multiple data elements received simultaneously to a stream of data elements transmitted in time sequence i. e one at a time. Option D is incorrect as parallel transmission is the simultaneous transmission of the signal elements and may involve two or more separate paths.

35. An asynchronous transfer mode type of network is not good for which of the following situations

A. Wide area networks

B. Small networks

C. Backbones

D. Multimedia applications

Option B is he correct answer. Option A is incorrect as asynchronous mode is recommended for wide area networks because of high performance integration of LANs and WANs. Option C is incorrect as asynchronous mode is recommended for backbones because of scalabilty, high performance and security. Option D is incorrect as asynchronous mode is recommended for multimedia applications because of its ability to dedicate allocated bandwidth to applications and its data prioritization capability.

36. To reduce security exposure when transmitting proprietary data over communication lines a company should select

A. Asynchronous modems

B. Authentication techniques

C. Call back techniques

D. Cryptographic devices

Option D is the correct answer. Option A is incorrect as asynchronous modems handle data stream from peripheral devices to a central processor. Option B is incorrect authentication techniques confirm that only valid users have access to the system.

Option C is incorrect as call back techniques are used to ensure that incoming calls are from authorised locations.

37. Encryption protection is least likely to be used in which of the following situations

A. When transactions are transmitted over local area networks

B. When wire transfers are made between banks

C. When confidential data are sent by satellite transmission

D. When financial data are sent over dedicated leased lines

Option A is the correct answer. Encryption is important when confidential data are transmitted between geographically separate locations. Even though encryption may be used in local LAN however it is more important in case of option B, C and D.

38. A superstore has 8 personal computers four printers and one plotter all networked together in one building. This type of network is called

A. Ring

B. Star

C. Local area

D. Wide area

Option C is the correct answer.

39. Which of the following functions can be performed by an intelligent terminal

A. Validating the conceptual schema and storing data formats

B. Validating data input and monitoring the data dictionary

C. Validating the external schema and storing data records

D. Validating data input and storing processed error messages

Option D is the correct answer. Option A is incorrect as smart terminals can store data formats but do not validate the conceptual schema. Option B is incorrect because smart terminals can validate input but do not monitor the data dictionary. Option C is incorrect because smart terminals can store data records but do not validate the external schema.

40. The most difficult aspect of using Internet resources is

A. Making the physical connection

B. Locating the best information source

C. Obtaining the equipment required

D. Getting authorisation for access

Option B is the correct answer. Option A is incorrect as there is no limitation on number of access ports. Option C is incorrect as simple and easily available equipment is required. Option D is incorrect as a individual can can easily obtain access through individual subscriptions to commercial information service providers

41. The scope of an IS Audit affects which of the following

A. Audit Schedules

B. Audit objectives

C. Audit summary

D. Audit programme

Option A is the correct answer. Scope defines the boundaries of the audit. The audit schedules will be longer if the audit scope is bigger and vice versa

42. Which one of the following items includes the other three items

A. Inherent Risk

B. Control risk

C. Audit risk

D. Detection Risk

Option C is the correct answer. Audit Risk is an all inclusive term. It is the product of inherent risk multiplied by control risk multiplied by detection risk.

43. Which of the following would not be considered in performing a risk analysis excercise

A. System complexity

B. Results of prior audits

C. Auditor skills

D. System changes

Option C is the correct answer. Auditors skills become a consideration during audit scheduling where as risk analysis is done prior to the start of an audit

44. The major purpose of an exit conference is:

A. Communication with all affected parties

B. Correction of deficiencies found

C. Assessment of Audit staff's performance

D. Presentation of the final audit report

Option A is the correct answer. The major purpose of exit conference is to discuss problems, conclusions and recommendations and to ensure that there is no misunderstanding or misrepresentation of facts.

45. During an Audit an IS Auditor found no written procedures for an application system. What should the auditor do:

A. Cancel the audit immediately since it is hard to do an audit without documentation

B. Reschedule the audit when the procedures are written

C. Report the issue to the management

D. Document the procedures and audit against them

Option D is the correct answer. The auditor can document the procedures based on interviews and observation of employees work. The other three options are effective in completing the current audit

46. The objective of control tests of details of the transactions performed by the IS Auditor is to:

A. Determine the nature timing and extent of substantive tests to be performed on the IS records and files

B. Determine material control weaknesses in the IS operations

C. Evaluate whether an IS control policy or procedure is working effectively

D. Inquire whether all IS employees have an access card to enter the computer room

Option C is the correct answer. IS test of controls are designed to assess the effectiveness of IS and user control policy or prodcedure in preventing or detecting material errors or control weaknesses in IS systems and operations.

47. Which of the following is the technique used to obtain evidential matter about tests of controls:

A. Re-performance

B. Analysis

C. Comparisons

D. Calculations

Option A is the correct answer. These techniques are used in compliance testing. Option B, C and D are examples of substantive testing.

48. Sample size:

A. Increases with use of higher confidence levels

B. Decreases with use of higher confidence levels

C. Remains unchanged with changes in confidence levels

D. Increases with the use of lower confidence levels

Option A is the correct answer. Sample size is directly related to the confidence level.

49. The appropriate sampling plan to use to identify at least one irregularity assuming some number of irregularities exists in a population and then to discontinue sampling when one irregularity is observed is:

A. Stop or go sampling

B. Discovery sampling

C. Variables sampling

D. Attributes sampling

Option B is the correct answer. Stop or go sampling (option A) involves identifying characteristics that could include single instances of suspected irregularities. Option C is incorrect because variable sampling involves reducing sample size by separating the population in to groups of items with similar values. Option D is incorrect because attributes sampling involves identifying characteristics of the sample and projecting those to the population.

50. The primary reason for an auditor to use statistical sampling is to:

A. Obtain a smaller sample than would be required by non statistical sampling techniques

B. Obtain a sample more representative of the population than would be obtained by non statistical techniques

C. Allow auditor to quantify and thus control the risk of making an incorrect decision based on sample evidence

D. Meet auditing standards

Option C is the correct answer. The results of statistical sampling are objective hence risk can be quantified.

51. An auditor wishes to determine if the error rate on travel reimbursement claims is within the five percent tolerance level set by management. what sampling plan should the auditor use:

    A. Variables sampling

    B. Attributes sampling

    C. Judgemental Sampling

    D. Dollar unit sampling

    Option B is the correct answer. Option A is incorrect as variable sampling is used to determine amounts and quantities. Choice C is incorrect as it does not use any statistical sampling criteria. Choice D is incorrect as it is a combination of attribute and variable sampling

52. Which of the following is not an audit procedure that is commonly used in conducting IS tests of controls (Compliance reviews and tests):

    A. Confirmations

    B. Inquiry

    C. Observations

    D. Inspection

    Option A is the correct answer. It is an example of substantive testing. Option B, C and D are examples of compliance testing.

53. Which of the following represents the correct sequence of performing the IS audit procedure:

    A. Substantive tests

    B. Interviews of personnel

    C. Compliance tests

    D. Preliminary evaluation

        A. 1, 2, 3, 4

        B. b 3, 4, 2, 1

        C. c 4, 2, 3, 1

        D. d. 2, 4. 3, 1

    Option D is the correct answer.

54. Which one of the following if material would be an irregularity:

A. Application programmers forgot to indicate file retention periods

B. IS operation analyst did not follow a procedure due to an oversight

C. Tape librarian forgot to log tape movement

D. An IS auditor knowingly approved an invoice for his friend's IS Consulting firm for a significant amount of time not actually worked

Option D is the correct answer. It is an example of irregularity which is a deliberate action, falsification, alteration of records or documents. Option A, B and C are examples of errors.

55. An IS auditor's primary consideration regarding internal control policies, procedures and standards available in the IS Department is whether they are :

A. Documented

B. Distributed

C. Followed

D. Approved

Option C is the correct answer

56. Comparing job runs logs to computer job schedules will provide critical evidences that :

A. All recorded jobs were completed

B. Only scheduled jobs were run

C. Some jobs were completed ahead of schedule

D. Some jobs were overridden by computer operators

Option D is the correct answer.

57. In an IT environment which of the following is not a substantive review and/or test

A. Determining whether program changes are approved

B. Performing system aging analysis

C. Performing program activity analysis

D. Performing job activity analysis

Option A is the correct answer. Option B, C and D are examples of substantive testing

58. Indicate the order in which primary questions must be addressed when an organization is determined to audit for fraud :

A. How vulnerable is the organisation

B. How can organisation detect fraud

C. How might someone go about defrauding the organisation

D. What does the organisation have that someone would want to defraud

A. 1, 2, 3, 4

B. b 3, 4, 2, 1

C. c 2, 4, 1, 3

D. d. 4, 3, 1, 2

Option D is the correct answer

59. Senior management has requested that an IS auditor assist the departmental management in the implementation of necessary controls. The IS auditor should:

A. refuse the assignment since it is not the role of the IS auditor.

B. inform management of his/her inability to conduct future audits.

C. perform the assignment and future audits with due professional care.

D. obtain the approval of user management to perform the implementation and follow-up.

Answer: B. inform management of his/her inability to conduct future audits.

In this situation the IS auditor should inform management of the impairment of independence in conducting further audits in the auditee area. An IS auditor can perform non-audit assignments where the IS auditor's expertise can be of use to management; however, by performing the non-audit assignment, the IS auditor cannot conduct the future audits of the auditee as his/her independence may be compromised. However, the independence of the IS auditor will not be impaired when suggesting/recommending controls to the auditee after the audit.

60. In a computer centre environment which of the following is not a compliance review and/or test

A. Performing system outage analysis

B. Determining whether job run logs are reviewed

C. Determining whether the disaster recovery plan is tested

D. Determining whether the job accounting log is reviewed

Option A is the correct answer. It is an example of substantive testing. Option B, C and D are examples of compliance testing.

61. Which of the following is not a benefit of using information technology in solving audit

Problems

A. It reduces audit risk

B. It improves the timeliness of the audit

C. It increases audit opportunities

D. It improves the auditor's judgement

Option D is the correct answer.

Use of IT cannot improve the auditor's judgement. All other options are benefits of IT.

62. Which of the following pre-processing controls is least likely to provide the auditor with assurance about the validity of transactions.

A. Verification of the requester

B. Authentication of information

C. Exception processing

D. Decryption of data

Option D is the correct answer. Option A is incorrect as identity of the requester should be verified. Authentication of information (option B) should be done before transfer. Option C is incorrect as information that is not authenticated is an exception which should be identified for additional processing.

63. The source of evidence to determine if ex employees continue to have access to a company's automated databases is:

A. Discuss the password removal process with the database administrator

B. Reviewing computer logs of access attempts

C. Reconciling current payroll lists with database access lists

D. Reviewing access control software to determine whether the most current version is implemented

Option C is the correct answer. Option A is incorrect as discussion will not reveal all facts and be conclusive. Option B is incorrect a log of access attempts will not reveal identity if a person accessing a database is no longer an employee. Option D is incorrect as review of access control software is not a specific test designed to identify who has access to the databases

64. An IS auditor involved in the requirements phase of a new application development project should ensure that:

A. programmers provide input to the functional requirements.

B. security requirements have been defined.

C. payback for the system is within an acceptable range.

D. a turnkey solution for the system requirements is available.

Answer: B. security requirements have been defined.

While the IS auditor provides an assurance on various other aspects, one of the key assurances at this stage is the security requirements. Programmers are generally not involved in the definition of functional requirements. The financial evaluation of a project is the responsibility of the IS steering committee. Searching for a turnkey solution at this stage is neither warranted nor is it the responsibility of an IS auditor.

65. Which of the following is often an advantage of using prototyping for systems development?

A. The finished system will have adequate controls.

B. The system will have adequate security/audit trail.

C. It reduces time to deployment.

D. It is easy to achieve change control.

Answer: C. It reduces time to deployment.

Prototyping is the process of creating systems through controlled trial and error. This method of system development can provide the organization with significant time and cost savings. By focusing mainly on what the user wants and sees, developers may miss some of the controls that come from the traditional systems development approach; therefore, a potential risk is that the finished system will have poor controls. In prototyping, changes in the designs and requirements occur quickly and are seldom documented or approved; hence, change control becomes more complicated with prototyped systems.

66. In addition to controls over access, programming, program changes and other functions a computerized system needs to establish an audit trail of information. Which of the following information would generally be not included in an audit trail log designed to summarise unauthorised system access logs:

A. A list of authorised users

B. The type of event or transaction attempted

C. The terminal used to make the attempt

D. The data in the programme sought

Option A is the correct answer. The list of users and their passwords would not be included in an audit trail log

67. Which of the following best represents Corporate Governance?

A. To protect shareholders' interest.

B. To protect management interest.

C. To protect Stakeholders interest.

D. To protect auditors interest.

Option C is the correct answer. Stakeholders interest is an all inclusive term.

68. Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are managed.

B. A knowledge base on customers, products, markets and processes is in place.

C. A structure is provided that facilitates the creation and sharing of business information.

D. Top management mediate between the imperatives of business and technology.

Answer: D. Top management mediate between the imperatives of business and technology.

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

69. Computer operators should not be given access to which of the following

A. Computer Console Terminal

B. Operations Documentation

C. Programming Documentation

D. Disk Drives

Option C is the correct answer. Computer operator should not be given access to programming documentation and production data files since he could perform maintenance to them for unauthorised purposes

70. Which of the following statements is true with regards to Corporate Governance Dimension.

A. Corporate Governance dimension is proactive

B. Corporate Governance Dimension is business oriented.

C. Corporate Governance Dimension focuses on strategy and value creation.

D. Corporate Governance Dimension is historic

Option D is the correct answer. Option A, B and C relate to Business Governance

71. Which of the following principles are most relevant for Governance Domain

A. Benefit Realisation, Risk Optimisation, Resource Optimisation.

B. Four Dimensions of balance score card

C. Evaluate, Direct, Monitor.

D. Plan, Build, Run and monitor.

Option C is the correct answer. Option A is incorrect as it relates to objectives of Governance. Option B is incorrect as it relates to performance measurement. Option D is incorrect as it relates to management objectives.

72. From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authority.

B. are current, documented and readily available to the employee.

C. communicate management's specific job performance expectations.

D. establish responsibility and accountability for the employee's actions.

Answer: D. establish responsibility and accountability for the employee's actions.

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

73. Which of the following is a compatible function for database administrator

A. Capacity Planning

B. Computer operations

C. Application Development

D. Application maintenance

Option A is the correct answer. the other options would cause incompatible situations leading to fraud and other irregularities.

74. Risk is the possibility of something adverse happening to an organisation. Which of the following steps is most difficult to accomplish in a risk management process.

A. Risk identification.

B. Risk Assessment

C. Risk mitigation

D. Risk maintenance

Option B is the correct answer. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. option A and D are not the most difficult steps to accomplish. Option C risk mitigation comes after completion of risk assessment process.

75. Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

A. System analysis

B. Authorization of access to data

C. Application programming

D. Data administration

Answer: B. Authorization of access to data

The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

76. Organisation Capacity to sustain loss due to uncertainity and expressed in Monetary terms is best known as:

A. Risk Appetite

B. Risk Tolerance.

C. Risk acceptance.

D. Risk Mitigation

Option A is the correct answer. This is the definition of Risk appetite

77. Cobit 5 is the model for which of the following

A. IT Planning.

B. IT governance

C. IT standards

D. IT infrastructure

Option B is the correct answer. COBIT 5 is the latest edition of ISACA's globally accepted framework. It provides an end-to-end business view of the governance of enterprise IT, reflecting the central role of information and technology in creating value for enterprises of all sizes.

78. The most likely to attract and retain IS security staff is

A. Special Training Sessions

B. Annual Conferences

C. Competitive salaries

D. Flexible Work schedules

Option D is the correct answer. Flexible work schedules are the biggest motivator to attract and retain IS Security staff.

79. During a logical access controls review, the IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

A. an unauthorized user may use the id to gain access.

B. user access management is time-consuming.

C. passwords are easily guessed.

D. user accountability may not be established.

Answer: D. user accountability may not be established.

The use of a single user id by more than one individual precludes knowing who in fact used that id to access a system; therefore, it is literally impossible to hold anyone accountable. All user ids, not just shared ids, can be used by unauthorized individuals. Access management would not be any different with shared ids, and shared user ids do not necessarily have easily guessed passwords.

80. Which of the following is an example of lead indicator

A. Financial Results

B. Market share retained over three years

C. Improvement in Customer Satisfaction survey

D. Regular training hours of employees.

Option D is the correct answer. Option A, B and C are examples of Lag indicators.

81. Which of the following are the major benefits of security measures, training and education programs that accrue to an organisation

A. Reducing fraud

B. Reducing Unauthorised actions

C. Improving Employee behaviour

D. Reducing errors and Omissions

Option C is the correct answer. Improved employee behaviour would ensure reduction in frauds, Unauthorised actions and errors and omissions.

82. When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.

B. integrity is maintained if the main power is interrupted.

C. immediate power will be available if the main power is lost.

D. hardware is protected against long-term power fluctuations.

Answer : A. hardware is protected against power surges.

A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

83. The quality assurance group is typically responsible for:

A. ensuring that the output received from system processing is complete.

B. monitoring the execution of computer processing tasks.

C. ensuring that programs and program changes and documentation adhere to established standards.

D. designing procedures to protect data against accidental disclosure, modification or destruction.

Answer: C. ensuring that programs and program changes and documentation adhere to established standards.

The quality assurance group is typically responsible for ensuring that programs, program changes and documentation adhere to established standards. Choice A is the responsibility of the data control group, choice B is the responsibility of computer operations, and choice D is the responsibility of data security.

84. The Security manager is responsible for

A. Planning and managing overall needs for data resources

B. Ensuring the integrity of data in shared environment

C. Determining and monitoring controls over access to data

D. Making data available to users when and where it is needed.

Option C is the correct answer. Option A, B and D are not the role of security manager.

85. Which of the following groups/individuals should assume overall direction and responsibility for costs and timetables of system development projects?

A. User management

B. Project steering committee

C. Senior management

D. Systems development management

Answer: B. Project steering committee

The project steering committee is ultimately responsible for all costs and timetables. User management assumes ownership of the project and the resulting system. Senior management commits to the project and approves the resources necessary to complete the project. System development management provides technical support for the hardware and software environments by developing, installing and operating the requested system.

86. Which of the following is most essential to implement IT governance within organisation

A. IT Department reports to steering committee.

B. IT Budget is based on percent of business budget.

C. IT strategy is aligned with business objectives.

D. IT issues are part of agenda on board meeting.

Option C is the correct answer. The ultimate aim of IT initiatives is to meet business objectives.

87. Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

A. Function point analysis

B. Earned value analysis

C. Cost budget

D. Program Evaluation and Review Technique

Answer: B. Earned value analysis

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule, and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work-breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

88. From a risk management view point which of the following options is not acceptable

A. Accept the risk.

B. Assign the risk.

C. Avoid the risk.

D. Defer the risk.

Option D is the correct answer. Defer risk means ignoring risk at hand or postponing further consideration of issue.

89. The responsibility for designing, implementing and maintaining a system of internal control lies with:

A. the IS auditor.

B. management.

C. the external auditor.

D. the programming staff.

Answer: B. management.

Designing, implementing and maintaining a system of internal controls, including the prevention and detection of fraud is the responsibility of management. The IS auditor assesses the risks and performs tests to detect irregularities created by weaknesses in the structure of internal controls.

90. Security can be lax under which of the following organisational structures or management practices

A. Right sizing.

B. Upsizing

C. Downsizing.

D. Budget sizing

Option C is the correct answer. Under downsizing there will be fewer employees performing basic duties and thus more who ignore the controls or bypass them

91. Which of the following items is most important in controlling the risks of operating a computer based information system.

A. a vulnerability inducing a threat

B. Asset valuation

C. Threat identification

D. Vulnerability analysis

Option A is the correct answer. Vulnerabilities are weakness in the system. Hence to control the risks of operating an information system managers and users need to know the vulnerabilities of the system and the threats that might exploit them.

92. An IS auditor involved in the requirements phase of a new application development project should ensure that:

A. programmers provide input to the functional requirements.

B. security requirements have been defined.

C. payback for the system is within an acceptable range.

D. a turnkey solution for the system requirements is available.

Answer: B. security requirements have been defined.

While the IS auditor provides an assurance on various other aspects, one of the key assurances at this stage is the security requirements. Programmers are generally not involved in the definition of functional requirements. The financial evaluation of a project

is the responsibility of the IS steering committee. Searching for a turnkey solution at this stage is neither warranted nor is it the responsibility of an IS auditor.

93. Data corruption can be prevented by which of the following.

A. Redundancy

B. Isolation

C. Policies

D. Procedures

Option A is the correct answer. Redundancy in data should be designed so that it cannot be removed. Isolation is just the opposite of redundancy. Policies and procedures are not effective against data corruption.

94. Data leakage cannot be prevented by which of the following.

A. Redundancy

B. Encryption

C. Access controls

D. Cryptography

Option A is the correct answer. Preventive controls include cryptography, encryption and access controls.

95. An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

A. Pilot

B. Parallel

C. Direct cut-over

D. Phased

Answer: C. Direct cut-over

Direct cut-over implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

96. For e commerce applications which of the following forms the foundation for building secure on line application systems

A. Client security

B. Secure transport protocols

C. Operating system security

D. Server Security

Option C is the correct answer. The operating system is the foundation on which commercial on line applications are built. Weakness in the foundation can be exploited to compromise the server regardless of the security attributes of the application.

97. Which of the following is not a primary component or aspect of firewall systems

A. Protocol filtering

B. Application gateways

C. Extended logging capability

D. Packet Switching

Option D is the correct answer. Packet switching is a message delivery technique. Option A, B and C are the primary components or aspects of firewall systems.

98. A message authentication code (MAC) is a

A. Data checksum

B. Cryptographic checksum

C. Digital Signature

D. Cyclic Redundancy Check

Option B is the correct answer. A MAC is a cryptographic checksum with the highest form of security against attacks. The Public Key is used to encrypt the message before transmission and knowledge of private key is needed to decrypt the received message. A Data Checksum (option A) is incorrect as it catches errors that are the result of noise or other natural or unintentional sources. The key difference between MAC and the digital signature is whereas MAC requires private key to verify, digital signatures are verifiable with a public key. A cyclic redundancy check (option D) is incorrect as it uses a algorithm for generating error detection bits and the receiving station performs the same calculation done by the transmitting station and in case results differ then one or more bits are in error.

99. Which of the following provide both integrity and confidentiality services for data and messages

A. Digital signature

B. Encryption

C. Cryptographic checksums

D. Granular access control

Option B is the correct answer.

Encryption provide both integrity and confidentiality services for data and messages.

100. The principle of least priviledge refers to the security objective of granting users only those accesses they need to perform their job duties. which of the following actions is inconsistent with the principle of least priviledge.

A. Authorisation creep

B. Reauthorisation when employees change positions

C. Users have little access to the system

D. Users have significant access to the systems

Option A is the correct answer. Authorisation creep occurs when employees continue to maintain access rights for previously held positions in the organisation. This practice is inconsistent with the principle of least privilege.

101. Which of the following user identification and authentication techniques depend on reference profiles or templates.

A. Memory tokens

B. Smart tokens

C. Cryptography

D. Bio metric systems

Option D is the correct answer.

Bio metric systems techniques depend on reference profiles or templates.

102. Which of the following attacks take advantage of dynamic system actions and the ability to manipulate the timing of those actions.

A. Active attacks

B. Passive attacks

C. Asynchronous attacks

D. Tunneling attacks

Option C is the correct answer. In case of Asynchronous attacks users request are placed in a queue an attacker can penetrate the queue and modify the data that is waiting to be processed and printed. He might change a queue entry to replace someones name or data with his own. Here the time variable is manipulated. With a active attack (option A) the intruder modifies the intercepted message. In case of

passive attack (option B) an intruder intercepts the message to view the data. This intrusion is also known as eavesdropping. Tunnelling attacks (option D) are used to transfer unauthorised data in legitimate data packets. Tunnelling exploits a weakness in the system at a low level of abstraction

103. Secure gateways block or filter access between two networks. Which of the following benefits resulting from the use of secure gateways is not true.

A. Secure gateways prevent the spread of computer viruses

B. Secure gateways reduce risks from malicious hackers

C. Secure gateways reduce internal system security overhead

D. Secure gateways can centralize management services

Option A is the correct answer. Option A is false rest all options are true.

104. Attacks by hackers are a major problem. Which of the following control techniques prevent hackers from trying to log into computer systems.

A. Access control list and smart tokens

B. Dial back modems and firewalls

C. Access control lists and dial back modems

D. Dial back modems and smart tokens

Option B is the correct answer. Smart tokens would not be applicable to hackers who would not have them. Access control lists refer to a register of users who have given access to use a particular system resource. Access control lists and smart tokens are applicable to insiders and not to outsiders.

105. Which of the following is an operating system access control function?

A. Logging user activities

B. Logging data communication access activities

C. Verifying user authorization at the field level

D. Changing data files

Answer : A. Logging user activities

General operating system access control functions include log user activities, log events, etc. Choice B is a network control feature. Choices C and D are database- and/or application-level access control functions.

106. Which of the following is a direct example of social engineering from a computer security viewpoint

a. Involvement in computer fraud

B. Involvement in trickery or coercion techniques

C. Involvement in computer theft

D. Involvement in computer sabotage

Option B is the correct answer. Social Engineering is the process of tricking or coercing people in to divulging their passwords.

107. Name the damaging act that uses a computer program to trigger an unauthorised malicious activity when some predefined condition occurs

A. Logic Bombs

B. Computer viruses

C. Worm

D. Nak attack

Option A is the correct answer. A logic bomb is set trigger at a particular condition, event or command. Option B is incorrect a computer virus reproduces by making copies of itself and inserting them in to other programs. choice C is incorrect because a worm searches for idle computing resources and uses them to execute the program in small segments. Option D is incorrect because a nak attack capitalises on potential weakness in an operating system that does not handle asynchronous interrupts properly leaving the system in an unprotected state during such interrupts.

108. In a database management system (DBMS), the location of data and the method of accessing the data are provided by the:

A. data dictionary.

B. metadata.

C. directory system.

D. data definition language.

Answer: C. directory system.

A directory system describes the location of data and the access method. A data dictionary contains an index and description of all the items stored in the database. Metadata are the data elements required to define an enterprisewide data warehouse. The data definition language processor allows the database administrator (DBA) to create/modify a data definition for mapping between external and conceptual schemes.

109. The most common concern regarding a physical security area is:

A. Fire suppression system

B. b Piggybacking

C. c Locks and Keys

D. d Natural disasters

Option B is the correct answer. Piggybacking occurs when unauthorised access is gained to a computer system via another users legitimate connection. Thereafter both authorised and unauthorised person can enter the sensitive area.

110. A universal serial bus (USB) port:

A. connects the network without a network card.

B. connects the network with an Ethernet adapter.

C. replaces all existing connections.

D. connects the monitor.

Answer: B. connects the network with an Ethernet adapter.

The USB port connects the network without having to install a separate network interface card inside a computer by using a USB Ethernet adapter.

111. An attack in which someone manipulates others in to revealing information that can be used for personal gain is called:

A. Social Engineering

B. Electronic trashing

C. Electronic piggybacking

D. Electronic harassment

Option A is the correct answer. Electronic Trashing (option B) is incorrect as it involves accessing residual data after a file has been deleted. The data still there for a skilled person to retrieve and benefit from. Option C is incorrect because it involves gaining access to a computer system via another users legitimate connection. Electronic Harassment (option D) is incorrect because it involves sending threatening e mail messages etc through say internet.

112. An attack that attempts to exploit a weakness in the system at a low level of abstraction is called:

A. Technical attack

B. Tunneling attack

C. Nak attack

D. Active attack

Option B is the correct answer.

113. Which of the following is the most effective method for password creation:

A. Use Password generators

B. Use password advisors

C. Assign passwords to users

D. Implement user selected passwords

Option B is the correct answer. Password advisors are computer programs that examine user choices for passwords and inform the users if the passwords are weak.

114. The world wide web on the internet can be protected against the risk of eavesdropping in an economical and conventional manner through the use of :

A. Link and document encryption

B. Secure socket layer and secure HTTP

C. Link encryption and secure socket layer

D. Document encryption and secure HTTP

Option B is the correct answer. The risk of eavesdropping occurs on the internet in two ways: traffic analysis and stealing of sensitive information. Secure socket Layer provides an encrypted TCP/IP pathway between two hosts on the internet. SSL can be used to encrypt any TCP/IP protocol such as http, telnet etc can use a variety of public key and token based systems for exchanging a session key.

115. A source of eavesdropping on the world Wide web server is :

A. Access Logs

B. System Logs

C. Agent Logs

D. Error Logs

Option b is the correct answer. System logs are vulnerable to traffic analysis. These log files contain information about each request made to server. These logs are analysed by the attacker to find out confidential information. Agent logs (option C) provide a list of programs that have been used to access the server.

116. In a TCP/IP-based network, an IP address specifies a:

A. network connection.

B. router/gateway.

C. computer in the network.

D. device on the network.

Answer: A. network connection.

An IP address specifies a network connection. An IP address encodes both a network and a host on that network; it does not specify an individual computer, but provides a connection to a network. A router/gateway connects two networks and has two IP addresses. Hence, an IP address cannot specify a router. A computer in the network can be connected to other networks as well. It will then use many IP addresses. Such computers are called multihomed hosts. Here, again, an IP address cannot refer to the computer. IP addresses do not refer to individual devices on the network, but refer to the connections by which they are connected to the network.

117. Which of the following statements about encryption is not true :

A. Software encryption degrades system performance

B. Hardware encryption is faster

C. Encryption is a desirable option in a LAN

D. Key management is an administrative burden

Option C is the correct answer. Encryption is not a desirable option in case of LAN because of performance problems. Although hardware encryption is faster it degrades the performance of the system similar to software based encrytption. In addition keys used in encryption require management attention entailing additional management burden.

118. Ensuring data and programme integrity is important. Which of the following controls apply the separation of duties principle most in an automated computer environment

A. File placement controls

B. Data file naming conventions

C. Program library controls

D. Program and job naming conventions

Option C is the correct answer. Program library controls allow only assigned programs to run in production environment. File placement Controls (option A) ensure that files reside on the proper direct access storage device so that datasets do not go to a wrong device by accident. Option B and D implement the separation of duties principle by uniquely identifying each production and test data file name, job name as well as terminal usage.

119. Identify the damaging act where the network is searched for idle computing resources and executes the program in small segments.

A. Computer Viruses

B. Trojan Horses

C. Worms

D. Asynchronous attacks

Option C is the correct answer. Trojan horse (option B) is a program that looks normal but contains harmful program code within it hence incorrect. Option D is incorrect because asynchronous attacks perform indirect attacks on the program by altering legitimate data or codes at a time when the program is idle, then causes the changes to be added to the target program at later execution.

120. Cryptography provides all of the following except:

A. Authentication

B. Confidentiality

C. Integrity

D. Availability

Option D is the correct answer.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries and it primarily takes care of Authentication, Confidentiality and Integrity.

121. Which of the following layers does not provide confidentiality services:

A. Presentation Layer

B. Transport Layer

C. Network layer

D. Session Layer

Option D is the correct answer. The presentation layer (Option A) provides authentication and confidentiality services. The Transportation layer (option B) is incorrect as it provides confidentiality, authentication, data integrity and access control services. The network layer (option C) is incorrect as it provides confidentiality, authentication, data integrity and aceess control services.

122. Which of the following identification techniques provides the best means of user authentication:

A. What the user is

B. What the user has

C. What the user knows

D. What the user has and what the user knows

Option D is the correct answer as it is two factor authentication which is better that one factor authentication that is Option A, B and C.

123. Which of the following methods provides the highest security to protect access from Unauthorised people:

A. Encryption

B. Call Back or dial back systems

C. Magnetic cards with identification number

D. User ID and Password

Option A is the correct answer.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries and it primarily takes care of Authentication, Confidentiality and Integrity.

124. Which of the following password related factors cannot be tested with automated vulnerability testing tools:

A. Password length

B. Password lifetime

C. Password secrecy

D. Password storage

Option C is the correct answer. No automated vulnerability testing tool can ensure that system users have not disclosed their passwords so secrecy cannot be guaranteed.

125. Which of the following ISO/OSI layers provides access control services:

A. Transport layer

B. Presentation Layer

C. Session layer

D. Data link Layer

Option A is the correct answer. The Transport layer ensures error free exchange of data

between end points. It is the only layer listed in the question that provides access control services.

126. Which of the security codes is the longest thereby making it difficult to guess:

A. Passphrases

B. Passwords

C. Lockwords

D. Passcodes

Option A is the correct answer. Passphrases have virtue of length making them difficult to guess and discover by trial and error attack on the system

127. Indicate the most objective and relevant evidence of fraud in a computer environment:

A. Physical examination

B. Physical observation

C. Inquiries of people

D. Computer Logs

Option D is the correct answer.

128. Programmers frequently create entry points into a program for debugging purposes and/or insertion of new program codes at a later date. These entry points are called:

A. Logic bombs

B. Worms

C. Trapdoors

D. Trojan Horses

Option C is the correct answer all other options are incorrect and already discussed.

129. In a fire extinguishing environment a dry pipe is:

A. A sprinkler system in which the water does not enter the pipes until the automatic sensor indicates that there is a fire in the area

B. A sprinkler system in which the water is in the pipe but the outside of the pipe is dry

C. A Halon gas system that contains a dry pipe

D. A carbon dioxide gas system that has a dry chemical to extinguish a fire

Option A is the correct answer. This is the basic way a Dry pipe functions.

130. What is the name of the malicious act involving a computer program looking normal but containing harmful code:

A. Trapdoor

B. Trojan Horse

C. Worm

D. Time Bomb

Option B is the correct answer. Option D time Bomb is incorrect because a time bomb is part of logic bomb that triggers the damaging act at some period of time after the bomb is set.

131. Which of the following would BEST support 24/7 availability?

A. Daily backup

B. Offsite storage

C. Mirroring

D. Periodic testing

Answer : C. Mirroring

Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

132. Which of the following combination controls would not be appropriate in extinguishing fires:

A. Smoke/fire detectors

B. Water sprinklers

C. Uninterruptible power supply equipment

D. Fire or evacuation drills

Option C is the correct answer. Option A, B and D are appropriate in extinguishing fires

133. If end users find errors and omissions during acceptance testing of software who should make corrections to an application system:

A. End users

B. Quality assurance speacialist

C. Database application specialist

D. Application programmer/analyst

Option D is the correct answer. The system is not introduced in live environment when the system is going through the acceptance testing and application programmers and analysts are responsible for correcting the systems for error.

134. If a database is restored using before-image dumps, where should the process be started following an interruption?

A. Before the last transaction

B. After the last transaction

C. As the first transaction after the latest checkpoint

D. As the last transaction before the latest checkpoint

Answer: A. Before the last transaction

If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

135. Which of the following phases of a system development life cycle should not be compressed for the proper development of a prototype.

A. System initiation

B. System definition

C. System testing

D. System Design

Option C is the correct answer. In the prototype environment there is tendency to compress system initiation, definition, design etc. However the testing phase should not be compressed for quality reasons.

136. Which of the following is not part of software quality metrics.

A. Completeness

B. Ergonomics

C. Correctness

D. Reliability

Option B is the correct answer. Ergonomics has nothing to do with software quality. Its scope includes designing computer screens, considering the table height, positioning of

table, lighting and ventilation at the workstation so that user is comfortable while working with computers.

137. Which of the following items is most difficult to manage in a system development life cycle project.

A. Project member turnover

B. Changes in hardware

C. Creeping Functions

D. Changes in project funding

Option C is the correct answer. Creeping function is the act of continually adding function enhancements to a software product throughout the development process hence most difficult to manage.

138. Which of the following system development approaches best brings the operational viewpoint to the requirement specification phase.

A. Waterfall model

B. Incremental development model

C. Evolutionary development model

D. Rapid prototyping model

Option D is the correct answer. Due to iterative process and end user involvement the rapid prototype model brings the operational view point to the requirements specification phase. Option A is incorrect as the waterfall model will not bring the operational view point to the requirement phase until the system is completely implemented. Option B and C are incorrect even though incremental development model and the evolutionary model are better than the waterfall they are not as good as rapid prototyping in terms of bringing the operational view point to the requirement phase

139. In object oriented technology an object is the unit of work. which of the following is not a key concept of object oriented technology

A. Encapsulation

B. Reusability

C. Messaging

D. Inheritance

Option B is the correct answer. Reusability is the benefit of object oriented technology where the technology can be extended to system analysis, design, programming and

database management systems. Encapsulation (Option A) is incorrect because it is one of the key concepts of object oriented technology. It means that the methods of an object are hidden from some other objects. (Option C) is incorrect because it is one of the key concepts of object oriented technology. Messages are the means by which objects communicate. (Option D) is incorrect because it is one of the key concepts of object oriented technology. It is a mechanism that allows objects of a class to acquire part of their definition from another class.

140. The software test objective of verifying that each required capability is implemented correctly is achieved in which of the following types of software testing approaches

A. Conversion test

B. Function test

C. Parallel test

D. Volume test

Option B is the correct answer as these tests are conducted by end users who are familiar with the system functions. Option A is incorrect because conversion test determine whether old data files and record balances can be carried forward accurately, properly and completely to the new system Option C is incorrect because parallel test verifies that the results of old and new systems are compared with each other. Option D is incorrect because volume test verifies whether simultaneous users can overload the system.

141. Which of the following reasons is most compelling to get rid of legacy application system

A. More flexible computing platforms are needed

B. the operating systems software is no longer supported

C. Program modifications are difficult

D. the hardware platform is no longer supported

Option C is the correct answer. While all options are good reason to get rid of legacy system however the fact that program modifications are difficult to make is a major risk.

142. The architecture of an expert system does not include which one of the following

A. Knowledge base

B. Computing environment

C. Inference Engine

D. End user interface

Option B is the correct answer. The computing environment includes hardware, programming languages, editors etc which are outside the expert systems architecture since it will change depending on each organisation. However option A, C and D are the integral parts of an expert systems architecture.

143. An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.

B. regular hardware maintenance is performed.

C. offsite storage of transaction and master files exists.

D. backup processing facilities are fully tested.

Answer: C. offsite storage of transaction and master files exists.

Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

144. Which of the following is not used in software requirements, design, programming and the project management processes :

A. Prototyping

B. Test Data generators

C. Simulation

D. Modeling

Option B is the correct answer. test data generators are used only in the testing process not in the software requirements, design, programming and the project management processes. Option A, C and D can be used in developing software requirements and design.

145. Software reverse engineering can do all of the following except:

A. Software requirements

B. Software planning

C. Software documentation

D. Software reusability

Option B is the correct answer. Software planning is a activity requiring human judgement and experience and is not a mechanical exercise as in reverse engineering.

146. Rapid prototyping is not useful in which of the following phases of a system development life cycle :

A. Requirements

B. Design

C. Implementation

D. Maintainence

Option D is the correct answer. Rapid prototyping builds a system with respect to users criteria in less time compared to a traditional development approach. It is not applied to maintenance because basic requirements are already in place except for the additions and changes.

147. Which of the following testing techniques can be used in all phases of a system development life cycle :

A. Performance testing

B. Regression analysis and testing

C. Back to Back testing

D. Stress Testing

Option B is the correct answer. Regression analysis and testing is used to revaluate requirements and design issues whenever any significant change code is made. It involves retesting a software product to detect faults made during modifications. Option A, C and D are used in the testing phase of SDLC.

148. Which of the following software development models became the basis for the other models :

A. Waterfall Model

B. Prototyping model

C. Spiral model

D. Incremental model

Option A is the correct answer. All other options are variant of waterfall model. A prototype is working model of a system improved by system definitions from users. Spiral Model is a system that is put together as a series of builds. An incremental model addresses the development of successive versions or enhancements.

149. A company performs full backup of data and programs on a regular basis. The primary purpose of this practice is to:

A. maintain data integrity in the applications.

B. restore application processing after a disruption.

C. prevent unauthorized changes to programs and data.

D. ensure recovery of data processing in case of a disaster.

Answer: B. restore application processing after a disruption.

Backup procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Backup procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures are a necessary part of the recovery process following a disaster, they are not sufficient in themselves.

150. The correct sequence of application software testing is :

A. Integration test, unit test, systems test, acceptance test

B. Unit test, Systems test, integration test, acceptance test

C. Acceptance test, unit test, integration test, systems test

D. Unit test, integration test, systems test, acceptance test

Option D is the correct answer.

151. Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.

B. validation checks.

C. input controls.

D. database commits and rollbacks.

Answer: D. database commits and rollbacks.

Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

152. Which of the following system development approaches best captures the reality of the way people actually work

A. Object oriented development model

B. Waterfall development model

C. Incremental development model

D. Evolutionary development model

Option A is the correct answer. The object oriented development model uses the composition principle where one starts from something known and adding to it gradually and deleting undesired portion hence closer to the way people work. Option B is incorrect because waterfall model uses the decomposition principle which is not the way people work. Option C and D are incorrect even though better than waterfall model they are not as good as the way people actually work.

153. When developing a backup strategy, the FIRST step is to:

A. identify the data.

B. select the storage location.

C. specify the storage media.

D. define the retention period.

Answer: A. identify the data.

Archiving data and backups is essential for the continuity of business. Selection of the data to be backed up is the first step in the process. Once the data have been identified, an appropriate retention period, storage media and location can be selected.

154. During the planning stage of an IS audit, the PRIMARY goal of the IS auditor is to:

A. address audit objectives.

B. collect sufficient evidence.

C. specify appropriate tests.

D. minimize audit resources.

Answer: A. address audit objectives.

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

155. In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools is MOST suitable for performing that task?

A. CASE tools

B. Embedded data collection tools

C. Heuristic scanning tools

D. Trend/variance detection tools

Answer: D. Trend/variance detection tools

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

156. The IS auditors participation in which of the following system development life cycle activities would provide the most benefit to the organisation:

A. Program development

B. Configuration planning

C. System requirements definition

D. Program testing

Option C is the correct answer. The system requirements definition activity is very useful to the auditor since in this activity need for controls are identified. Option A, B and D are incorrect are program oriented and very detailed and not conducive to the auditors role.

157. Beta test sites for software products are usually defined as:

A. Locations and environments with personnel able to measure programmer productivity

B. Environments within which to satisfy early commitments to customer shipments of new software products

C. Sites willing to help the software vendor evaluate product completeness and correctness

D. Sites used to test product demand

Option C is the correct answer. Options A, B and D are incorrect because beta test sites have nothing to do with measuring productivity shipping or testing the product demand.

158. Both White Box testing and Black Box testing are performed in which of the following

A. Unit testing

B. Integration Testing

C. System Testing

D. Acceptance testing

Option A is the correct answer. A unit test is a test of software elements at the lowest level of development. Since the unit test is the first test conducted its scope should include both black box and white box testing. Option B is incorrect as integration test comes after unit test. Option C is incorrect because the system test comes after completion of integration test. Option D is incorrect as acceptance test comes after completion of integration tests.

159. Which of the following tests is driven by system requirements

A. Black Box testing

B. White Box testing

C. Gray box Testing

D. Integration testing

Option A is the correct answer. Black box testing executes part or all of the system to validate that the user requirement is satisfied. White Box testing examines the logic of the units. Option C Gray Box is a distractor or say looks at anything not tested by white box and black box. option D is incorrect because integration test is performed to examine how units interface and interact with each other.

160. Attributes of software product quality do not include:

A. Design

B. Documents

C. Code

D. Tools

Option D is the correct answer. Tools is not a parameter of quality of software product.

161. One class of data processing error is the failure to enter all the data that should be presented to the system. Which one of the following would you expect management to install in their effort to detect this class of error:

A. Existence check

B. Control Totals

C. Limit Check

D. Reasonableness check

Option B is the correct answer. Option A, C and D are incorrect as they are test of accuracy.

162. A company's wage distribution report requires extensive corrections each month because of labour hours charged to inactive jobs. Which of the following data processing input controls appears to be missing:

A. Completeness test

B. Validity test

C. Limit test

D. Control total

Option B is the correct answer. Validity checks ensure that transaction contain valid transaction codes, characters and field size. Completeness ensure that the input has the prescribed amount of data in all data fields. Limit tests are used to determine whether the data exceeds predefined limits. Control totals are used to reconcile input to the source document totals.

163. Which one of the following could an IS auditor use to validate the effectiveness of edit and validation routines?

A. Domain integrity test

B. Relational integrity test

C. Referential integrity test

D. Parity checks

Answer: A. Domain integrity test

Domain integrity testing is aimed at verifying that the data conform to definitions, i. e. , the data items are all in the correct domains. The major objective of this exercise is to verify that the edit and validation routines are working satisfactorily. Relational integrity tests are performed at the record level and usually involve calculating and verifying various calculated fields, such as control totals. Referential integrity tests involve ensuring that all references to a primary key from another file actually exist in their original file. A parity check is a bit added to each character prior to transmission. The parity bit is a function of the bits making up the character. The recipient performs the same function on the received character and compares the result to the transmitted parity bit. If it is different, an error is assumed.

164. An on line bank teller system permitted withdrawals from inactive accounts. The best control for denying such withdrawals is a:

A. Proof calculation

B. Check digit verification

C. Master file lookup

D. Duplicate record check

Option C is the correct answer. Option A is incorrect as proof calculation is the use of a predefined algorithm to be performed on the information in a telecommunications transmission to verify that no transmission errors occurred. Option B is incorrect a check digit verification is used to control the accuracy of the input of the reference numbers but does not deny access to an inactive but valid account. Option D is incorrect as a duplicate record check ensures that duplicate records are not processed.

165. In a critical server, an IS auditor discovers a Trojan horse that was produced by a known virus that exploits a vulnerability of an operating system. Which of the following should an IS auditor do FIRST?

A. Investigate the virus's author.

B. Analyze the operating system log.

C. Ensure that the malicious code is removed.

D. Install the patch that eliminates the vulnerability.

Answer: C. Ensure that the malicious code is removed.

The priority is safeguarding the system; therefore, the IS auditor should suggest corrective controls, i.e., remove the code. The IS auditor is not responsible for investigating the virus. The IS auditor may analyze the virus information and determine if it has affected the operating system, but this is an investigative task that would take place after ensuring that the malicious code has been removed. Installing the patch that eliminates the vulnerability should be done by technical support.

166. Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence

B. Time and cost savings

C. Efficiency and effectiveness

D. Ability to search for violations of intellectual property rights

Answer: A. The preservation of the chain of custody for electronic evidence

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Time and cost savings, choice B, and efficiency and effectiveness,

choice C, are legitimate concerns and differentiate good from poor forensic software packages. The ability to search for intellectual property rights violations, choice D, is an example of a use of forensic software.

167. Before each employee pay raise was effective a data entry operator entered a new wage rates for salaried and hourly employees. The operator by mistake entered Rs. 100 instead of Rs. 10 for an hourly rate. The best control for preventing this error from resulting in overpayment of wages to employees is use of

A. A reasonableness Check

B. Self checking digit

C. Prior data matching.

D. A mathematical accuracy check.

Option A is the correct answer. Option B is incorrect as self checking digit detects account number transposition. Option C is incorrect as there is no prior data for matching. Option D is incorrect a mathematical accuracy check verifies the result of computation but will not detect this error.

168. In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, an IS auditor should:

A. identify and assess the risk assessment process used by management.

B. identify information assets and the underlying systems.

C. disclose the threats and impacts to management.

D. identify and evaluate the existing controls.

Answer: D. identify and evaluate the existing controls.

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

169. A data entry clerk typed the account number as 124356 in to the computer for a customers payment on account when the account number that should have been typed was 123456 resulting in wrong customer account being updated. What input control would have prevented this error :

A. Check Digit

B. Control Totals

C. Limit Check.

D. Value test.

Option A is the correct answer. The check digit control is meant to catch transposition errors. Control Totals are intended to ensure completeness of processing. Limit Checks are intended to determine whether a data value falls with in certain limits. A value test is designed to check a data field for a certain value.

170. Which of the following should be of MOST concern to an IS auditor?

A. Lack of reporting of a successful attack on the network

B. Failure to notify police of an attempted intrusion

C. Lack of periodic examination of access rights

D. Lack of notification to the public of an intrusion

Answer: A. Lack of reporting of a successful attack on the network

Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire, or lack thereof, to make the intrusion known.

171. During a review of the controls over the process of defining IT service levels, an IS auditor would MOST likely interview the:

A. systems programmer.

B. legal staff.

C. business unit manager.

D. application programmer.

Answer: C. business unit manager.

Understanding the business requirements is key in defining the service levels. While each of the other entities listed may provide some definition, the best choice here is the business unit manager because of this person's knowledge of the requirements of the organization.

172. The best control for identifying missing and duplicate transactions over long time periods is :

A. manual agreement of a batch register

B. Computer agreement of batch totals

C. A batch sequence check.

D. A commulative sequence check.

Option D is the correct answer. In case of cumulative sequence check transaction tables are flagged by sequence number when transactions are processed so that there is record of which transactions are processed. Option A and B gives assurance that the batch totals agree but does not identify the specific missing or duplicate transactions. Option C is incorrect as batch sequence checks perform sequence checks within single batches only.

173. A computer operator has been removing the last page of a printed report before its distribution to authorised users. The operator is handing over this page containing inventory turnover summary to a competitor. The best corrective action is to employ:

A. Retention control

B. Spooler control

C. Distribution logs.

D. End of job markers

Option D is the correct answer.

This option would permit control section staff and users to verify that they have received the entire report and take appropriate action if entire report is not received. Retention control (option A) is the practice of collecting and destroying output after its useful life has expired. Spooler controls (option B) prevent access to disk copies of printed output as it waits to be printed. Distribution Logs (option C) govern the manner of delivering whole reports to authorised users.

174. An auditor wishes to determine the extent to which invalid data can be contained in a human resources computer system. Examples are invalid job classification, age in excess of retirement age. The best approach to determine the extent of the potential problem is to:

A. Submit test data to test the effectiveness of edit controls over the input of data

B. Review and test access controls to ensure that access is limited to authorised individuals.

C. Use generalised audit software to develop a detailed report of all data outside specified parameters.

D. Use generalised audit software to select a sample of employees. Use sample to

determine the validity of test data items and project the result to the population as a whole

Option C is the correct answer. This is both most effective and most efficient procedure as it provides a comprehensive analysis of the extent of obviously incorrect data included in the database.

175. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware:

A. of the point at which controls are exercised as data flow through the system.

B. that only preventive and detective controls are relevant.

C. that corrective controls can only be regarded as compensating.

D. that classification allows an IS auditor to determine which controls are missing.

Answer: A. of the point at which controls are exercised as data flow through the system.

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

176. Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings

B. Source program listings

C. Program change requests

D. Production library listings

Answer: D. Production library listings

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be time intensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

177. The auditor wants to determine whether or not the computer program is appropriately matching the purchase receipts and vendor invoices throughout the

year. Which one of the following computerised audit techniques would be most efficient and effective in accomplishing this objective:

A. Use the test data method during the last quarter

B. use of an integrated test facility throughout the year

C. Use parallel simulation and apply on a monthly basis.

D. Use the System Control and Audit review file on a daily basis

Option B is the correct answer. The ITF allows the auditor to submit data periodically during the year to determine how well the program works throughout the year. The Test data method (option A) is limited to a point in time in which the testing is accomplished. Using it at the end of quarter is not going to be effective. Option C is incorrect as parallel simulation causes the auditor to develop a massive parallel system. Option D is incorrect the SCARF method is to identify transactions with unusual characteristics or transactions that are processed even though they do not pass normal edit controls, it simply writes these transactions to a file for further investigation.

178. Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee

B. The results of a test performed by an IS auditor

C. An internally generated computer accounting report

D. A confirmation letter received from an outside source

Answer: D. A confirmation letter received from an outside source

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

179. Which of the following information systems auditing technique processes real transaction data through auditor developed test programs.

A. Integrated test facility

B. Tracing

C. Parallel simulation

D. Mapping

Option C is the correct answer. Parallel simulation processes real transactions through

auditor developed test program. Integrated test facility involves the use of test data and also the creation of fictitious entities. Tracing (option B) provides a detailed listing of program sequence execution. Mapping is a procedure for reporting code usage within a program.

180. In auditing an online perpetual inventory system an auditor selected certain file updating transactions for detailed testing. The audit technique which will provide a computer trail of all relevant processing steps applied to a specific transaction is described as :

A. Simulation

B. Snapshot

C. Code comparison

D. Tagging and Tracing

Option D is the correct answer. Tagging is an audit technique to obtain computer trail of processing steps relevant to a given transaction.

181. An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.

B. investigating various communication channels.

C. understanding the responsibilities and authority of individuals.

D. investigating the network connected to different employees.

Answer: C. understanding the responsibilities and authority of individuals.

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

182. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.

B. Determine the risks/threats to the data center site.

C. Review business continuity procedures.

D. Test for evidence of physical access at suspect locations.

Answer: B. Determine the risks/threats to the data center site.

During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

183. The primary reason auditors are reluctant to use Integrated Test Facility is that it requires them to :

A. Reserve specific master file records and process them at regular intervals

B. Collect transaction and master file records in a separate file

C. Notify user personnel so they can make manual adjustments to output

D. Identify and reverse the fictitious entries to avoid contamination of the master file.

Option D is the correct answer. This is one of the prime reasons for not using ITF.

184. Embedded audit modules :

A. Identify unexpected computer code

B. Aid in debugging application systems

C. Analyze the efficiency of programming

D. Enable continuous monitoring of transaction processing.

Option D is the correct answer. Option A is incorrect as it is a characteristic of snapshot. Option B is incorrect as it is a characteristic of tracing. Option C is incorrect as it is a characteristic of mapping.

185. An internal auditor was assigned to confirm whether operating personel had corrected several errors in transaction files that were discovered during a recent audit. Which of the following automated tools is the auditor most likely to use :

A. On line enquiry

B. Parallel simulation

C. Mapping

D. Tracing

Option A is the correct answer. On line enquiry is an interactive procedure that allows an auditor or other authorised personnel to select and view individual records or transactions.

186. An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.

B. interview programmers about the procedures currently being followed.

C. compare utilization records to operations schedules.

D. review data file access records to test the librarian function.

Answer: B. interview programmers about the procedures currently being followed.

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

187. Disaster recovery plans protect against which of the following

A. Physical Losses.

B. Economic Losses.

C. Equipment Losses.

D. Inventory Losses.

Option B is the correct answer. Economics losses is an all inclusive term

188. The least critical factor in estimating the maximum tolerable downtime during a disaster is:

A. Availability of Cold site during the disaster.

B. Time of the disaster.

C. Applications affected by the disaster.

D. Length of the disaster.

Option A is the correct answer. The maximum tolerable downtime depends on time of the disaster, applications affected by the disaster and length of the disaster. A hot site is more relevant and needed compared to cold site during disaster.

189. Which of the following is not an assumption made during the development of a disaster recovery and contingency plan?

A. Testing and maintenance of the contingency plan should be continual.

B. All resources and materials required to restore the processing capability at the backup recovery site should be obtainable off-site.

C. All the less critical jobs need not be recovered

D. In a multisite environment a separate set of recovery plans should be developed for each computer centre.

Option C is the correct answer. The basic assumption of any disaster recovery and contingency plan is recover all applications but in the recovery priority decided by the management that is from most critical to least critical.

190. Business functions that can be done manually but only for a brief period of time:

A. Vital.

B. Sensitive

C. Critical

D. Non Critical

Option A is the correct answer as it is the definition of Vital systems.

191. identify the correct statement

A. Both differential and incremental backups take the same amount of time

B. Incremental backups take longer to complete than differential backups

C. Differential backups take longer to complete than incremental backups

D. Incremental backups take longer when using tape drives

Option C is the correct answer. Rest all are false.

192. Which is the most rigorous form of Disaster Recovery Plan Testing

A. Checklist test

B. Simulation testing

C. Full interruption test

D. Parallel Testing

Option C is the correct answer as full interruption test is conducted after disrupting normal operations and should be very carefully planned.

193. There are several reasons for a company to develop and implement a disaster recovery plan. What is the most important goal of disaster recovery.

A. Protect human life

B. Protect the integrity of the business

C. Protect critical operating systems.

D. Protect customer relationships

Option A is the correct answer as paramount objective of any Disaster Recovery plan is protection of organisation employees and public at large

194. What is the inherent limitation of a disaster recovery planning excercise?

A. Inability to include all types of disasters.

B. Assembling disaster management and recovery teams.

C. Developing early warning monitors that will trigger alerts and responses.

D. Conducting periodic drills.

Option A is the correct answer. There are many type of disasters which can occur it is not practical to consider all such disasters. Moreover it is not possible to visualise all kinds of disaster scenarios.

195. The most effective way to ascertain the hot site vendor's integrity in practices and priorities in the resource sharing area is to :

A. Review all subscriber contracts with the hot site vendor

B. Observe an actual disaster at the hot site vendor

C. Request a copy of the annual external audit report

D. Request the hot site vendor's compliance in writing

Option C is the correct answer. It is a report given by an independent professional who would carry out audit procedures and report them accordingly.

196. Which of the following rationales is not a sound one. Disaster recovery plan should be tested

A. By Simulation

B. In stages.

C. In an unannounced manner.

D. In actual use.

Option D is the correct answer. A real disaster should not have to occur before the plan weaknesses are revealed. The other three options are valid approaches to testing.

197. If the recovery time objective (RTO) increases:

A. the disaster tolerance increases.

B. the cost of recovery increases.

C. a cold site cannot be used.

D. the data backup frequency increases.

Correct Answer Option A the disaster tolerance increases

Explanation: The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

198. In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

A. Disaster tolerance is high.

B. Recovery time objective is high.

C. Recovery point objective is low.

D. Recovery point objective is high.

Option C is correct

Explanation: A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data . If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of the disaster tolerance. The lower the RTO, the lower the disaster tolerance. Therefore, choice C is the correct answer.

199. Which of the following is the best method for determining the criticality of each application system in the production environment

A. Interview the application programmers

B. Perform Gap analysis

C. Review the most recent application audit.

D. Perform a Business Impact Analysis.

Option D is the correct answer. BIA will give the impact of each application to an organisation. Interview with application programmers, Gap Analysis and reviewing of recent application audits will provide only limited information.

200. Which of the following represents the greatest risk created by reciprocal agreement for disaster recovery made between two companies:

A. Developments may result in hardware and software incompatibility

B. Resources may not be available when needed

C. The recovery plan cannot be tested

D. the security infrastructures in each company may be different

Option A is the correct answer. If one organisation upgrades its hardware and software

configurations then the other party will not be able to use their facilities as compatibility issues will crop. This indicates that both the companies will not be able to use each other facilities in case of a disaster.

Answers with explanations

1. Option B is the correct answer. On line time indicates how much time is taken between entry of query and its reply and deals with utilisation of system resources which need to be considered during system design phase. Option A is incorrect because it is too early to determine online system response and C and D are incorrect because it is too late to determine on line system response

2. Option A is the correct answer. Data mining is a set of automated tools that convert data in the warehouse to some useful information. Data mining techniques could also be used for fraud detection, intrusion detection, abnormal patterns in data. Data optimisation tools improves performance of the database. Data access as the name suggests helps in accessing the right data. Data reorganisation tools helps relocate the data for faster access.

3. Option D is the correct answer. Workload is basically the request of the users submitted to the computing resources. Bandwidth describes capacity and not workload. The remaining three options represent the workload

4. Option A is the correct answer. Referential integrity means that no record will have reference to the primary key of the non exsistent record. When a record is deleted all other referenced records are automatically deleted. Options B, C and D are incorrect because they are same for flat file and database systems.

5. Option A is the correct answer. In case of a multiplexer the total bandwidth entering and leaving are roughly equivalent. Option B is incorrect with a concentrator total bandwidth entering the device and leaving are different. Choice C is incorrect as there are devices that perform the functions of both concentrators and multiplexers. Choice D is incorrect as concentrators can give better utilisation of the bandwidth than a multiplexer.

6. Option B is the correct answer. Bridges are networking devices that connect two LANs. Routers regulate traffic between two LANs. Gateways connect dissimilar networks. Brouters combine the features of routers and bridges.

7. Option C is the correct answer. A schema describes (option A) the structure of related tables and views whereas actual data is stored in tables. Views (option D) are derived from tables and are composed as subset of table. A subschema (option B) presents data views of the user.

8. Option B is the correct answer. Clearing information means rendering it unrecoverable by keyboard attack with data remaining on the storage media. Option A, C and D are the three general methods of purging magnetic storage media.

9. Option C is the correct answer. Passive threats do not alter any data in a system. Messages are simply read to gain some knowledge. Since no alteration of data takes place passive threats are difficult to detect. Option A, B and D are examples of active threats. Active threats alter the data rather than simply reading the contents of the signals. A denial of service (option A) occurs when an attacker either destroys or delays the message. Masquerading (option B) is an attempt to gain access to the system by posing as an authorised user. Option D occurs when the attacker modifies, delete the original message and adds fake messages.

10. Option A is the correct answer. A gateway is a device used for connecting two dissimilar networks. Option b, c and d are incorrect since the gateway are responsible for returning acknowledgements.

11. Option A is the correct answer. Option B provides somewhat general structures compared to hierarchical model Option C relational model is widely accepted as most suitable for end users because its basic formulation is easily understood. Option D can be visualised as having many networks nodes and access paths between the central and local computers. However data security is a major security concern in a distributed environment.

12. Option D is the correct answer. The disadvantage is technical immaturity and complexity in designing compared with other traditional systems. Option A, C and D are the advantage of client/server computing hence incorrect.

13. Option B is the correct answer. Normalisation is the formal process for eliminating access and update anomalies. Hierarchy data model is incorrect because it can be related to a family tree concept. Network is incorrect because it is depicted using blocks and arrows. Object model is incorrect because it is a model of attributes, relationships in a system.

14. Option A is the correct answer. The controller is a logic device that directs all the tasks that the terminal must perform. Repeaters (option B) merely repeat data packets or electrical signals between cable segments. They basically regenerate the signal at its original strength. File server (option C) send and receive data between a workstation and server and its main purpose is to make files, printers available to users. Bridge (option D) connects similar or dissimilar LANs together to form a extended LAN.

15. Option D is the correct answer. Microwave communication is a point to point transmission using radio frequency signals and is more appropriate for long distance transmission. Option A and B is the most widely used medium for data transmission in local area networking. Option C uses light signals to carry a stream of data at extremely high modulation rates though highly secure and sturdy.

16. Option A is the correct answer. The star topology uses Central Hub which connects workstation and servers. Now because of the Central Hub even if one of the workstation

fails rest all are active. A tree tapology is a variation of bus. A disadvantage of this topology is if one of the workstation goes down all other workstation fails because of interdependency. In Ring topology (option C) there is no central hub and all personal computers are connected successively forming a ring. A disadvantage of this topology is if one of the workstation goes down all other workstations fail. A mixed topology (option D) is a combination of star, bus, tree or ring topologies

17. Option A is the correct answer. Tree topology (option B) is incorrect due to installation of the long single main cable. Ring topology (optionC) is incorrect as data is looped around a ring till it reaches the proper host computer. Mixed topology (option D) is incorrect because of mixed structures resulting in unpredictable performance rates.

18. Option B is the correct answer. A protocol analyser is a sophisticated networking line monitoring tool as it traps data or performs statistical analysis of data. Line monitior (option A) is a passive device and not as sophisticated as protocol analyser. Barometer (option C) is used for measuring atmospheric pressure and voltmeter (Option D) is used for measuring current.

19. Option A is the correct answer. The physical layer addresses areas such as frequencies used and modulation techniques employed and data link layer deals with how the network is shared between links.

20. Option C is the correct answer. In cable plant integrity it is helpful to test each section of the cable as finding cable faults after installation can be difficult and tedious. Choice A is incorrect as many LANs provide a variety of connectivity and interoperability. Choice B is incorrect as most LANs support many users and hence need to provide many services concurrently. User application system (option D) is incorrect as it is important to thoroughly exercise LAN software to be sure that there are no memory-cram problems at the workstations.

21. Option B is the correct answer. DBA is responsible for physical design (option A) security (option C) and performance (option D).

22. Option C is the correct answer. Managing security is a major problem since distributed system operate in hostile environments. Option A is incorrect because scalability can be achieved by allowing more units to be added to the system. Option B is incorrect as heterogeneity can be handled properly with open system designs. Choice D is incorrect as synchronisation are standard problems of distributed systems and can be handled properly.

23. Option A is the correct answer. Option B is incorrect application programming interface is often selected as a first step in moving to more complex client/server strategies. Option C is incorrect because GUI based operating systems is the next step in complexity after API. Option D is incorrect as because peer-to-peer communication is most complex of all.

24. Option A is the correct answer. An echo check provides a feedback loop by transmitting data received back to the source unit for validation with the original data. It is a hardware control. A protection ring (option B) prevents accidental writing on a tape file for most batch systems hence should not be utilised for real time systems. Option C is incorrect as hash totals are utilised to control data sent to a batch system and not real time system. option D is incorrect as integrated test facility are useful in testing real time systems but cannot be utilised to ensure completeness of data transmission.

25. Option D is the correct answer. Option A is incorrect as dedicated phonelines would not be effective or available to field agents. Option B is incorrect as field agents would not always be located at the same phone line to permit dial up call back usage. Option C is incorrect as passwords may be compromised by computer software.

26. Option C is the correct answer. Change control would ensure that only authorised and tested programs are run in production. Access controls (OptionA) would ensure only authorised persons have access to the system but is not enough in itself to ensure integrity of application software. Audit trails (option B) permits audit of transactions update to data files and not programs. Monitoring software (option D) is designed to monitor performance for specified functions.

27. Option C is the correct answer. Required access code revalidation on a recurring basis would prevent unauthorised persons to enter unauthorised transactions. Option A is incorrect since the salesman have no fixed telephone number call back procedures would not control this access. Error correcting codes (option B) repair damaged transmissions but cannot detect or prevent unauthorised access. Modem equalisation (option D) controls for line errors but cannot detect or prevent unauthorised access.

28. Option A is the correct answer.

29. Option A is the correct answer. Terminals that are attached directly to a public data network (Options C and D) must have enough intelligence and storage capacity to break the large messages in packets and reassemble them in proper sequence.

30. Option D is the correct answer. A protocol is a set of rules governing a specific sequence of events and defines method of formatting bits of data and messages for transmission, routing and identification of messages including error detection and correction. However it does not address message authentication.

31. Option A is the correct answer. Logical access control is a software based control whereas option B, C and D are physical security controls over telecommunications hardware.

32. Option B is the correct answer. In case of active dictionary there is no option which means that data dictionary and the database management system go together. Option A is incorrect since both active and passive dictionaries are useful. Option C is incorrect

as a passive data dictionary may or may not require a check for currency of data description before execution of program. Option D is incorrect because non database systems can have data dictionaries.

33. Option A is the correct answer. Option B is incorrect because physical layer addresses transmission medium, medium access etc. Option C is incorrect as network layer addresses deadlocks, etc. Option D is incorrect as application layer addresses dataflow modelling, file management etc.

34. Option C is the correct answer. Option A is incorrect because serial to parallel conversion is the conversion of a stream of data elements received one at a time into a stream consisting of multiple data elements transmitted simultaneously. Option B is incorrect because it entails conversion of multiple data elements received simultaneously to a stream of data elements transmitted in time sequence i. e one at a time. Option D is incorrect as parallel transmission is the simultaneous transmission of the signal elements and may involve two or more separate paths.

35. option B is he correct answer. Option A is incorrect as asynchronous mode is recommended for wide area networks because of high performance integration of LANs and WANs. Option C is incorrect as asynchronous mode is recommended for backbones because of scalabilty, high performance and security. Option D is incorrect as asynchronous mode is recommended for multimedia applications because of its ability to dedicate allocated bandwidth to applications and its data prioritization capability.

36. Option D is the correct answer. Option A is incorrect as asynchronous modems handle data stream from peripheral devices to a central processor. Option B is incorrect authentication techniques confirm that only valid users have access to the system. Option C is incorrect as call back techniques are used to ensure that incoming calls are from authorised locations.

37. Option A is the correct answer. Encryption is important when confidential data are transmitted between geographically separate locations. Even though encryption may be used in local LAN however it is more important in case of option B, C and D.

38. Option C is the correct answer.

39. Option D is the correct answer. Option A is incorrect as smart terminals can store data formats but do not validate the conceptual schema. Option B is incorrect because smart terminals can validate input but do not monitor the data dictionary. Option C is incorrect because smart terminals can store data records but do not validate the external schema.

40. Option B is the correct answer. Option A is incorrect as there is no limitation on number of access ports. Option C is incorrect as simple and easily available equipment is

required. Option D is incorrect as a individual can can easily obtain access through individual subscriptions to commercial information service providers.

41. Option A is the correct answer. Scope defines the boundaries of the audit. The audit schedules will be longer if the audit scope is bigger and vice versa.

42. Option C is the correct answer. Audit Risk is an all inclusive term. It is the product of inherent risk multiplied by control risk multiplied by detection risk.

43. Option C is the correct answer. Auditors skills become a consideration during audit scheduling where as risk analysis is done prior to the start of an audit.

44. Option A is the correct answer. The major purpose of exit conference is to discuss problems, conclusions and recommendations and to ensure that there is no misunderstanding or misrepresentation of facts.

45. Option D is the correct answer. The auditor can document the procedures based on interviews and observation of employees work. The other three options are effective in completing the current audit.

46. Option C is the correct answer. IS test of controls are designed to assess the effectiveness of IS and user control policy or prodcedure in preventing or detecting material errors or control weaknesses in IS systems and operations.

47. Option A is the correct answer. These techniques are used in compliance testing. Option B, C and D are examples of substantive testing.

48. Option A is the correct answer. Sample size is directly related to the confidence level.

49. Option B is the correct answer. Stop or go sampling (option A) involves identifying characteristics that could include single instances of suspected irregularities. Option C is incorrect because variable sampling involves reducing sample size by separating the population in to groups of items with similar values. Option D is incorrect because attributes sampling involves identifying characteristics of the sample and projecting those to the population.

50. Option C is the correct answer. The results of statistical sampling are objective hence risk can be quantified.

51. Option B is the correct answer. Option A is incorrect as variable sampling is used to determine amounts and quantities. Choice C is incorrect as it does not use any statistical sampling criteria. Choice D is incorrect as it is a combination of attribute and variable sampling.

52. Option A is the correct answer. It is an example of substantive testing. Option B, C and D are examples of compliance testing.

53. Option D is the correct answer.

54. Option D is the correct answer. It is an example of irregularity which is a deliberate action, falsification, alteration of records or documents. Option A, B and C are examples of errors.

55. Option C is the correct answer.

56. Option D is the correct answer.

57. Option A is the correct answer. Option B, C and D are examples of substantive testing.

58. Option D is the correct answer.

59. Option D is the correct answer.

60. Option A is the correct answer. It is an example of substantive testing. Option B, C and D are examples of compliance testing.

61. Option D is the correct answer.

62. Option D is the correct answer. Option A is incorrect as identity of the requester should be verified. Authentication of information (option B) should be done before transfer. Option C is incorrect as information that is not authenticated is an exception which should be identified for additional processing.

63. Option C is the correct answer. option A is incorrect as discussion will not reveal all facts and be conclusive. Option B is incorrect a log of access attempts will not reveal identity if a person accessing a database is no longer an employee. Option D is incorrect as review of access control software is not a specific test designed to identify who has access to the databases.

64. Option B is the correct answer.

65. Option B is the correct answer.

66. Option A is the correct answer. The list of users and their passwords would not be included in an audit trail log.

67. Option C is the correct answer. Stakeholders interest is an all inclusive term.

68. Option B is the correct answer.

69. Option C is the correct answer. Computer operator should not be given access to programming documentation and production data files since he could perform maintenance to them for unauthorised purposes.

70. Option D is the correct answer. Option A, B and C relate to Business Governance.

71. Option C is the correct answer. Option A is incorrect as it relates to objectives of Governance. Option B is incorrect as it relates to performance measurement. Option D is incorrect as it relates to management objectives.

72. Option D is the correct answer.

73. Option A is the correct answer. the other options would cause incompatible situations leading to fraud and other irregularities.

74. Option B is the correct answer. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. option A and D are not the most difficult steps to accomplish. Option C risk mitigation comes after completion of risk assessment process.

75. Option A is the correct answer.

76. Option A is the correct answer. This is the definition of Risk appetite.

77. Option B is the correct answer.

78. Option D is the correct answer. Flexible work schedules are the biggest motivator to attract and retain IS Security staff.

79. Option D is the correct answer.

80. Option D is the correct answer. Option A, B and C are examples of Lag indicators.

81. Option C is the correct answer. Improved employee behaviour would ensure reduction in frauds, Unauthorised actions and errors and omissions.

82. Option C is the correct answer.

83. Option B is the correct answer.

84. Option C is the correct answer. Option A, B and D are not the role of security manager.

85. Option B is the correct answer.

86. Option C is the correct answer. The ultimate aim of IT initiatives is to meet business objectives.

87. Option C is the correct answer.

88. Option D is the correct answer. Defer risk means ignoring risk at hand or postponing further consideration of issue.

89. Option C is the correct answer.

90. Option C is the correct answer. Under downsizing there will be fewer employees performing basic duties and thus more who ignore the controls or bypass them.

91. Option A is the correct answer. Vulnerabilities are weakness in the system. Hence to control the risks of operating an information system managers and users need to know the vulnerabilities of the system and the threats that might exploit them.

92. Option C is the correct answer.

93. Option A is the correct answer. Redundancy in data should be designed so that it cannot be removed. Isolation is just the opposite of redundancy. Policies and procedures are not effective against data corruption.

94. Option A is the correct answer. Preventive controls include cryptography, encryption and access controls.

95. Option D is the correct answer.

96. Option C is the correct answer. The operating system is the foundation on which commercial on line applications are built. Weakness in the foundation can be exploited to compromise the server regardless of the security attributes of the application.

97. Option D is the correct answer. Packet switching is a message delivery technique. Option A, B and C are the primary components or aspects of firewall systems.

98. Option B is the correct answer. A MAC is a cryptographic checksum with the highest form of security against attacks. The Public Key is used to encrypt the message before transmission and knowledge of private key is needed to decrypt the received message. A Data Checksum (option A) is incorrect as it catches errors that are the result of noise or other natural or unintentional sources. The key difference between MAC and the digital signature is whereas MAC requires private key to verify, digital signatures are verifiable with a public key. A cyclic redundancy check (option D) is incorrect as it uses a algorithm for generating error detection bits and the receiving station performs the same calculation done by the transmitting station and in case results differ then one or more bits are in error.

99. Option B is the correct answer.

100. Option A is the correct answer. Authorisation creep occurs when employees continue to maintain access rights for previously held positions in the organisation. This practice is inconsistent with the principle of least priviledge.

101. Option D is the correct answer.

102. Option C is the correct answer. In case of Asynchronous attacks users request are placed in a queue an attacker can penetrate the queue and modify the data that is waiting to be processed and printed. He might change a queue entry to replace someones name or data with his own. Here the time variable is manipulated. With a active attack (option A) the intruder modifies the intercepted message. In case of passive attack (option B) an intruder intercepts the message to view the data. This intrusion is also known as eavesdropping. Tunneling attacks (option D) are used to transfer unauthorised data in legitimate data packets. Tunneling exploits a weakness in the system at a low level of abstraction

103. Option A is the correct answer.

104. Option B is the correct answer. Smart tokens would not be applicable to hackers who would not have them. Access control lists refer to a register of users who have given access to use a particular system resource. Access control lists and smart tokens are applicable to insiders and not to outsiders.

105. Option B is the correct answer.

106. Option B is the correct answer. Social Engineering is the process of tricking or coercing people in to divulging their passwords.

107. Option A is the correct answer. A logic bomb is set trigger at a particular condition, event or command. Option B is incorrect a computer virus reproduces by making copies of itself and inserting them in to other programs. choice C is incorrect because a worm searches for idle computing resources and uses them to execute the program in small segments. Option D is incorrect because a nak attack capitalises on potential weakness in an operating system that does not handle asynchronous interrupts properly leaving the system in an unprotected state during such interrupts.

108. Option C is the correct answer

109. Option B is the correct answer. Piggybacking occurs when unauthorised access is gained to a computer system via another users legitimate connection. Thereafter both authorised and unauthorised person can enter the sensitive area.

110. Option D is the correct answer.

111. Option A is the correct answer. Electronic Trashing (option B) is incorrect as it involves accessing residual data after a file has been deleted. The data still there for a skilled person to retrieve and benefit from. Option C is incorrect because it involves gaining access to a computer system via another users legitimate connection. Electronic Harassment (option D) is incorrect because it involves sending threatening e mail messages etc through say internet.

112. Option B is the correct answer.

113. Option B is the correct answer. Password advisors are computer programs that examine user choices for passwords and inform the users if the passwords are weak.

114. Option B is the correct answer. The risk of eavesdropping occurs on the internet in two ways :traffic analysis and stealing of sensitive information. Secure socket Layer provides an encrypted TCP/IP pathway between two hosts on the internet. SSL can be used to encrypt any TCP/IP protocol such as http, telnet etc can use a variety of public key and token based systems for exchanging a session key.

115. Option b is the correct answer. System logs are vulnerable to traffic analysis. These log files contain information about each request made to server. These logs are analysed by the attacker to find out confidential information. Agent logs (option C) provide a list of

programs that have been used to access the server.

116. Option B is the correct answer.

117. Option C is the correct answer. Encryption is not a desirable option in case of LAN because of performance problems. Although hardware encryption is faster it degrades the performance of the system similar to software based encrytption. In addition keys used in encryption require management attention entailing additional management burden.

118. Option C is the correct answer. Program library controls allow only assigned programs to run in production environment. File placement Controls (option A) ensure that files reside on the proper direct access storage device so that datasets do not go to a wrong device by accident. Option B and D implement the separation of duties principle by uniquely identifying each production and test data file name, job name as well as terminal usage.

119. Option C is the correct answer. Trojan horse (option B) is a program that looks normal but contains harmful program code within it hence incorrect. Option D is incorrect because asynchronous attacks perform indirect attacks on the program by altering legitimate data or codes at a time when the program is idle, then causes the changes to be added to the target program at later execution.

120. Option D is the correct answer.

121. Option D is the correct answer. The presentation layer (Option A) provides authentication and confidentiality services. The Transportation layer (option B) is incorrect as it provides confidentiality, authentication, data integrity and access control services. The network layer (option C) is incorrect as it provides confidentiality, authentication, data integrity and aceess control services.

122. Option D is the correct answer.

123. Option A is the correct answer.

124. Option C is the correct answer. No automated vulnerability testing tool can ensure that system users have not disclosed their passwords so secrecy cannot be guaranteed.

125. Option A is the correct answer. The Transport layer ensures error free exchange of data between end points. It is the only layer listed in the question that provides access control services.

126. Option A is the correct answer. Passphrases have virtue of length making them difficult to guess and discover by trial and error attack on the system

127. Option D is the correct answer.

128. Option C is the correct answer all other options are incorrect and already discussed.

129. Option A is the correct answer. This is the basic way a Dry pipe functions.

130. Option B is the correct answer. Option D time Bomb is incorrect because a time bomb is part of logic bomb that triggers the damaging act at some period of time after the bomb is set.

131. Option A is the correct answer.

132. Option C is the correct answer. Option A, B and D are appropriate in extinguishing fires.

133. Option D is the correct answer. The system is not introduced in live environment when the system is going through the acceptance testing and application programmers and analysts are responsible for correcting the systems for error.

134. Option A is the correct answer.

135. Option C is the correct answer. In the prototype environment there is tendency to compress system initiation, definition, design etc. However the testing phase should not be compressed for quality reasons.

136. Option B is the correct answer. Ergonomics has nothing to do with software quality. Its scope includes designing computer screens, considering the table height, positioning of table, lighting and ventilation at the workstation so that user is comfortable while working with computers.

137. Option C is the correct answer. Creeping function is the act of continually adding function enhancements to a software product throughout the development process hence most difficult to manage.

138. Option D is the correct answer. Due to iterative process and end user involvement the rapid prototype model brings the operational view point to the requirements specification phase. Option A is incorrect as the waterfall model will not bring the operational view point to the requirement phase until the system is completely implemented. Option B and C are incorrect even though incremental development model and the evolutionary model are better than the waterfall they are not as good as rapid prototyping in terms of bringing the operational view point to the requirement phase

139. Option B is the correct answer. Reusability is the benefit of object oriented technology where the technology can be extended to system analysis, design, programming and database management systems. Encapsulation (Option A) is incorrect because it is one of the key concepts of object oriented technology. It means that the methods of an object are hidden from some other objects. (Option C) is incorrect because it is one of the key concepts of object oriented technology. Messages are the means by which objects communicate. (Option D) is incorrect because it is one of the key concepts of object oriented technology. It is a mechanism that allows objects of a class to acquire

part of their definition from another class.

140. Option B is the correct answer as these tests are conducted by end users who are familiar with the system functions. Option A is incorrect because conversion test determine whether old data files and record balances can be carried forward accurately, properly and completely to the new systemOption C is incorrect because parallel test verifies that the results of old and new systems are compared with each other. Option D is incorrect because volume test verifies whether simultaneous users can overload the system.

141. Option C is the correct answer. While all options are good reason to get rid of legacy system however the fact that program modifications are difficult to make is a major risk.

142. Option B is the correct answer. The computing environment includes hardware, programming languages, editors etc which are outside the expert systems architecture since it will change depending on each organisation. However option A, C and D are the integral parts of an expert systems architecture.

143. Option A is the correct answer.

144. Option B is the correct answer. test data generators are used only in the testing process not in the software requirements, design, programming and the project management processes. Option A, C and D can be used in developing software requirements and design.

145. Option B is the correct answer. Software planning is a activity requiring human judgement and experience and is not a mechanical exercise as in reverse engineering.

146. Option D is the correct answer. Rapid prototyping builds a system with respect to users criteria in less time compared to a traditional development approach. It is not applied to maintenance because basic requirements are already in place except for the additions and changes.

147. Option B is the correct answer. Regression analysis and testing is used to revaluate requirements and design issues whenever any significant change code is made. It involves retesting a software product to detect faults made during modifications. Option A, C and D are used in the testing phase of SDLC.

148. Option A is the correct answer. All other options are variant of waterfall model. A prototype is working model of a system improved by system definitions from users. Spiral Model is a system that is put together as a series of builds. An incremental model addresses the development of successive versions or enhancements.

149. Option C is the correct answer.

150. Option D is the correct answer.

151. Option D is the correct answer. Big bang approach puts and tests all units together at once and there is no systematic approach to testing in case any failure is observed there are few clues available for locating the fault. Option A, B and C use incremental approach for testing and utilise systematic approach.

152. Option A is the correct answer. The object oriented development model uses the composition principle where one starts from something known and adding to it gradually and deleting undesired portion hence closer to the way people work. Option B is incorrect because waterfall model uses the decomposition principle which is not the way people work. Option C and D are incorrect even though better than waterfall model they are not as good as the way people actually work.

153. Option A is the correct answer.

154. Option B is the correct answer.

155. Option B is the correct answer.

156. Option C is the correct answer. The system requirements definition activity is very useful to the auditor since in this activity need for controls are identified. Option A, B and D are incorrect are program oriented and very detailed and not conducive to the auditors role.

157. Option C is the correct answer. Options A, B and D are incorrect because beta test sites have nothing to do with measuring productivity shipping or testing the product demand.

158. Option A is the correct answer. A unit test is a test of software elements at the lowest level of development. Since the unit test is the first test conducted its scope should include both black box and white box testing. Option B is incorrect as integration test comes after unit test. Option C is incorrect because the system test comes after completion of integration test. Option D is incorrect as acceptance test comes after completion of integration tests.

159. Option A is the correct answer. Black box testing executes part or all of the system to validate that the user requirement is satisfied. White Box testing examines the logic of the units. Option C Gray Box is a distractor or say looks at anything not tested by white box and black box. option D is incorrect because integration test is performed to examine how units interface and interact with each other.

160. Option D is the correct answer.

161. Option B is the correct answer. Option A, C and D are incorrect as they are test of accuracy.

162. Option B is the correct answer. Validity checks ensure that transaction contain valid transaction codes, characters and field size. Completeness ensure that the input has the prescribed amount of data in all data fields. Limit tests are used to determine

whether the data exceeds predefined limits. Control totals are used to reconcile input to the source document totals.

163. Option A is the correct answer.

164. Option C is the correct answer. Option A is incorrect as proof calculation is the use of a predefined algorithm to be performed on the information in a telecommunications transmission to verify that no transmission errors occurred. Option B is incorrect a check digit verification is used to control the accuracy of the input of the reference numbers but does not deny access to an inactive but valid account. Option D is incorrect as a duplicate record check ensures that duplicate records are not processed.

165. Option B is the correct answer.

166. Option B is the correct answer.

167. Option A is the correct answer. Option B is incorrect as self checking digit detects account number transposition. Option C is incorrect as there is no prior data for matching. Option D is incorrect a mathematical accuracy check verifies the result of computation but will not detect this error.

168. Option C is the correct answer.

169. Option A is the correct answer. The check digit control is meant to catch transposition errors. Control Totals are intended to ensure completeness of processing. Limit Checks are intended to determine whether a data value falls with in certain limits. A value test is designed to check a data field for a certain value.

170. Option A is the correct answer.

171. Option A is the correct answer.

172. Option D is the correct answer. In case of cumulative sequence check transaction tables are flagged by sequence number when transactions are processed so that there is record of which transactions are processed. Option Aand B gives assurance that the batch totals agree but does not identify the specific missing or duplicate transactions. Option C is incorrect as batch sequence checks perform sequence checks within single batches only.

173. Option D is the correct answer. This option would permit control section staff and users to verify that they have received the entire report and take appropriate action if entire report is not received. Retention control (option A) is the practice of collecting and destroying output after its useful life has expired. Spooler controls (option B) prevent access to disk copies of printed output as it waits to be printed. Distribution Logs (option C) govern the manner of delivering whole reports to authorised users.

174. Option C is the correct answer. This is both most effective and most efficient procedure

as it provides a comprehensive analysis of the extent of obviously incorrect data included in the database.

175. Option D is the correct answer.

176. Option A is the correct answer.

177. Option B is the correct answer. The ITF allows the auditor to submit data periodically during the year to determine how well the program works throughout the year. The Test data method (option A) is limited to a point in time in which the testing is accomplished. Using it at the end of quarter is not going to be effective. Option C is incorrect as parallel simulation causes the auditor to develop a massive parallel system. Option D is incorrect the SCARF method is to identify transactions with unusual characteristics or transactions that are processed even though they do not pass normal edit controls, it simply writes these transactions to a file for further investigation.

178. Option A is the correct answer.

179. Option C is the correct answer. Parallel simulation processes real transactions through auditor developed test program. Integrated test facility involves the use of test data and also the creation of fictitious entities. Tracing (option B) provides a detailed listing of program sequence execution. Mapping is a procedure for reporting code usage within a program.

180. Option D is the correct answer. Tagging is an audit technique to obtain computer trail of processing steps relevant to a given transaction.

181. Option C is the correct answer.

182. Option A is the correct answer.

183. Option D is the correct answer. This is one of the prime reasons for not using ITF.

184. Option D is the correct answer. Option A is incorrect as it is a characteristic of snapshot. Option B is incorrect as it is a characteristic of tracing. Option C is incorrect as it is a characteristic of mapping.

185. Option A is the correct answer. On line enquiry is an interactive procedure that allows an auditor or other authorised personnel to select and view individual records or transactions.

186. Option C is the correct answer.

187. Option B is the correct answer. Economics losses is an all inclusive term

188. Option A is the correct answer. The maximum tolerable downtime depends on time of the disaster, applications affected by the disaster and length of the disaster. A hot site is more relevant and needed compared to cold site during disaster.

189. Option C is the correct answer. The basic assumption of any disaster recovery and

contingency plan is recover all applications but in the recovery priority decided by the management that is from most critical to least critical.

190. Option A is the correct answer as it is the definition of Vital systems.

191. Option C is the correct answer.

192. Option C is the correct answer as full interruption test is conducted after disrupting normal operations and should be very carefully planned.

193. Option A is the correct answer as paramount objective of any Disaster Recovery plan is protection of organisation employees and public at large.

194. Option A is the correct answer. There are many type of disasters which can occur it is not practical to consider all such disasters. Moreover it is not possible to visualise all kinds of disaster scenarios.

195. Option C is the correct answer. It is a report given by an independent professional who would carry out audit procedures and report them accordingly.

196. Option D is the correct answer. A real disaster should not have to occur before the plan weaknesses are revealed. The other three options are valid approaches to testing.

197. Option A is the correct answer.

198. Option C is the correct answer.

199. Option D is the correct answer. BIA will give the impact of each application to an organisation. Interview with application programmers, Gap Analysis and reviewing of recent application audits will provide only limited information.

200. Option A is the correct answer. If one organisation upgrades its hardware and software configurations then the other party will not be able to use their facilities as compatibility issues will crop. This indicates that both the companies will not be able to use each other facilities in case of a disaster.

Summary

Following is summary of Module wise questions given in the AT Mock Test Paper.

1. Module 1 Question No 1 to 40
2. Module 2 Question No 41 to 66
3. Module 3 Question No 67 to 92
4. Module 4 Question No 93 to 132
5. Module 5 Question No 133 to 160
6. Module 6 Question No 161 to 186
7. Module 7 Question No 187 to 200

Mock Assessment Test Paper 4

1. Which of the following is not the layer of TCP/IP protocol?

   A. Application Layer

   B. Session Layer

   C. Transport Layer

   D. Internetwork layer

   Application Layer, Transport Layer and Network Layer are TCP/IP layers. Session layer is not a TCP/IP protocol layer. Hence b is answer.

2. A concurrent audit technique would include the following:

   A. Integrated test facility

   B. Continuous intermittent simulation

   C. SCARF

   D. All of the above

   All three options are included in the concurrent audit techniques. Hence d is the correct answer

3. In audit planning, auditors assess various audit risk factors, which of the following is NOT an audit risk factor considered during audit planning?

   A. Compliance risk

   B. Sampling risk

   C. Market risk

   D. Environmental risk

   In audit planning the IS auditor will consider sampling risk, market risk related to client's business and environmental risk from a business continuity perspective. Compliance risk is client risk and will be evident only during audit and so it is excluded from planning. Hence Choice a is the correct answer.

4. When would compensating controls be most important?3

   A. There is a lacuna in systems control

   B. Existence of a manual control to cover system lacuna

   C. Controls are found to be slack

   D. Controls over systems are reasonably adequate

   Compensating control is defined as existence of a manual control to compensate a

system lacuna. Options a and c merely suggest that controls are not operating properly. Option d suggests there is no lacuna in system. Option b is correct answer.

5. The auditor's role in systems development should be as a(n):

   A. Independent reviewer

   B. Developer of internal controls

   C. Team member in developing program

   D. Management representative for reporting

   Auditor's involvement in system development can only be as an independent reviewer. Option b & c are suggesting active involvement in system development and hence auditor's independence can be impaired. Option d also suggests control over development process in position as management representative. Option a is the correct answer.

6. Confirmation involves which of the following actions?

   A. With third parties

   B. Recalculation

   C. Statistics

   D. Regression analysis

   Confirmation of balances with third parties is a substantive test. Options b, c & d are involving further analytical procedures on the system itself. Hence option a is correct.

7. When sorting inventory records by location with generalized audit software, which of the following functions of a generalized audit software package is used?

   A. File manipulation

   B. Data analysis

   C. Data dictionary

   D. None of the above

   Option a is the correct answer. Data manipulation techniques enable geographical sorting of inventory records. Option b is data analysis and is not sorting data. Option c is data dictionary which only stores data descriptions.

8. Evaluation of audit evidence includes which of the following?

   A. Assess the quality of internal controls

   B. Assess the reliability of information

   C. Assess operating performance

D. All of the above

Options a, b & c are all techniques for evaluation of audit evidence. Hence d is the correct answer.

9. Which of the following is the first line of defense?

A. Directive controls

B. Detective controls

C. Corrective controls

D. Data recovery controls

In any enterprise, directive controls in the forms of policies and procedures set by the enterprise serve as a first line of defense. Hence choice a is the correct choice.

10. When the services that operate and manage the communications line are provided in addition to the line itself, this is referred to as:

A. VAN

B. VPN

C. PAN

D. WAN

Choice a is the correct answer, when the service provider provides the line along with additional services it is defined as a value added network. Choices b, c, & d are other types of networks.

11. Which statement is false regarding extranets?

A. Security and privacy are serious concerns so the extranets are generally secured behind a firewall.

B. The cost of equipment to establish an extranet may be thousands of dollars at each site and the secure communications lines can be hundreds of dollars each month

C. Extranets is a good source of information dissemination

D. None of the above

Options a and c are true. But Option b about spending thousands of dollars to set an extranet is not true. Hence choice b is the correct choice.

12. Which of the following is a direct benefit of adopting an Interorganizational system?

A. Increased ability to compete

B. Increased operational efficiency

C. Increased customer confidence

D. Decreased operational costs

Building Interorganizational system increases the operational efficiency. Options a and c may also hold true whereas d is not always true and also not an objective for Interorganizational systems. Choice b is most appropriate.

13. Which language can provide file formatting structure and a means for describing data within the file of a Web page?

A. XML

B. HTML

C. DML

D. None of the above

Choice a provides a file formatting structure and a means for describing data within the file of a web page. Choices b c or d are not holding true and hence Option a is the best answer.

14. Which information system is intended to meet the general information needs of managers throughout the firm?

A. Expert system

B. Management information system

C. Robotics

D. Decision support system

Management information system prevail in organizations to provide management with useful information on a periodic basis to enable decision taking. Choices a, c or d also support decision taking, but in the current context, it refers to general information and hence choice b is the correct answer.

15. Which type of video conferencing occurs when people at the receiving sites can talk to people at the transmitting site, while everyone views the same video images?

A. Two-way video and audio

B. One-way video and two-way audio

C. One way video and one way audio

D. Two way video and two way audio

Option b best describes this alternative of hearing on both sides and being able to view a common document which is the subject of discussion. Other options are not true for this situation.

16. The specialist whose duties fall into the areas of planning, implementation, operation, and security is the:

    A. Data administrator

    B. CIO

    C. Database administrator

    D. Data owner

    A DBA is responsible for planning, implementation operation and security of the database. Options a, b and d have varied duties. Choice c is the correct answer.

17. Which systems development skill involves the study and ultimate understanding of a situation for the purpose of formulating a response or solution?

    A. Communication skills

    B. Analytical ability

    C. Mathematical accuracy

    D. Documentation ability

    While Options a, c or d are necessary for formulating a solution analytical skills are compulsory to assess a problem, study the different factors affecting and arrive at a solution. Hence Option b is the correct answer.

18. The challenge faced by developing a knowledge management system that states "that a clear definition of KM must be formulated and used within the organization that fits within the existing IT infrastructure, falls into which logical set?

    A. Standards

    B. Cost benefit risks

    C. Geographical risks

    D. None of the above

    0rganizations strive to standardise the procedures in order to have uniformity in operations. Options b, c or d are not relevant for the situation. Option ‘a’ is the correct answer.

19. Which of the following is NOT a connection strategy used in distributed systems?

    A. Circuit switching

    B. Message switching

    C. Token switching

    D. Packet switching

Options a, b and d are instances of strategies used in distribution systems. Token switching is the odd one that does not match the description. Hence choice c is the correct answer.

20. What is common problem found in distributed system?

A. Process Synchronization

B. Communication synchronization

C. Deadlock problem

D. Power failure

A common problem in distributed systems is the problem of deadlock due to number of concurrent users. Choices a and bare not problems but advantages. Choice d is power failure which is not created due to distributed systems. Hence choice c is the correct answer.

21. Once the changes are written to the log, they are considered to be-.

A. Committed

B. Aborted

C. Completed

D. None of the above

Once changes are written to log they are committed unless system permits unauthorized modification of logs. Choice b and c are not true and d is irrelevant. Hence the correct answer is choice a.

22. When you continuously measure yourself against your peers, you are employing-

A. Benchmarking

B. Peer to peer review

C. Outsourcing

D. None of the above

When you compare yourself with peers, you are doing benchmarking. Hence choice a is the correct answer. A peer to peer review is a formal review of a document or report. Choice c is not correct since outsourcing is not mere comparison but obtaining services from third party vendor.

23. What term refers to the amount of information that can pass through a system during a specified amount of time?

A. Data speed

B. Broadband

C. Throughput

D. System speed

By definition, amount of information passing through the system in a specific period of time is called throughput. Options a, b and d does not match this definition. Hence choice c is the correct answer.

24. When one computer provides services to another computer, the environment is a(n) _____ infrastructure.

A. Independent

B. Client-server environment

C. Dependent

D. Reliant

Option b best describes client-server relationship. Choices a, c and d are merely qualities of a system. Hence choice b is the correct answer.

25. When there is little or no exchange of information within an organization's information systems, we say that the systems are-

A. Independent

B. Autonomous

C. Centralized

D. Decentralized

When two computers do not communicate with each other, they are decentralized and they do not directly share resources. Choice a is not true since they need not be independent but having remote connectivity indirectly. They are neither autonomous nor centralized as in this case they still would be communicating. Hence d is right answer.

26. What terms refers to the structure, and substructures, of an organization's information systems?

A. Subsystems

B. Infrastructure

C. IT configurations

D. None of the above

Choice b is the correct answer as by definition the structure, substructure of an information system is termed as infrastructure.

27. When two or more computers are able to share information, what is this called?

A. Cooperative processing

B. Interoperability

C. Standardized processing

D. Data interchange

Choice b is the correct answer since interoperability signifies capacity of computers to share information.

28. What type of information systems reuses self-contained blocks of code in its systems?

A. Modular systems

B. Component programming

C. Block based coding

D. Service oriented architecture (SOA)

Self-contained blocks of code are reused in Service Oriented Architecture. Choices a, b, c do not fit in the criteria. Hence choice d is the correct answer.

29. Which of the following risks will increase by the installation of a database system?

A. Programming errors

B. Data entry errors

C. Improper file access

D. Loss of parity

Options a, b, & d are not related to database related risks. Choice c speaks of improper file access which is a database related risk especially in the absence of proper access control mechanism. Hence correct answer is c

30. An independent software program that connects two otherwise separate applications to share computing resources across heterogeneous technologies is known as:

A. Middleware.

B. Firmware.

C. Software.

D. Embedded systems

Option b is given by vendor and software refers to any code or program not necessarily a connecting code. Embedded systems are small programs within an application placed there to perform a specific function. A software that connects one application to another is an interface and is referred to as middleware. Hence choice a is the correct answer.

31. In an inventory system on a database management system, one stored record contains part number, part name, part colour, and part weight. These individual items are called-

    A. Stored files

    B. Fields

    C. Bytes

    D. Occurrences

    Individual part, weight, colour, etc are singular fields and a set of related fields form a record. Hence Choice b is the correct answer. A set of related records form a file Hence a, c and d does not fit in the criteria.

32. Which of the following database model is considered most versatile?

    A. The hierarchical model

    B. The tree model

    C. The network model

    D. The relational model

    Option d is the correct answer, the relational model enables modelling of database through relational tables. Options a b and c does not permit complex modelling of database.

33. The relationship between online real-time database systems and batch processing systems is that-

    A. A firm will have only one processing mode because a single computer cannot do both.

    B. A firm will not use batch processing if it has a large computer

    C. A firm may use both processing modes concurrently

    D. A firm will always prefer online real-time processing system because batch processing is slow.

    Options a and b are not true. But it is possible to use both types of processing concurrently. Choice d is not always true. Hence Choice c is the correct choice.

34. Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

    A. Gateway

    B. Protocol converter

    C. Front-end communication processor

D. Concentrator/multiplexor

The function of converting email formats so that they can reach destination are Gateways. When messages travel through the information highway, routers route messages to the nearest Gateway and Gateways enable emails to reach their correct destination. Options b, c and d perform different functions. But they are not relevant to this instance. Hence choice a is the correct answer.

35. Which of the following is a benefit of using "call back" devices?

A. Provide an audit trail.

B. Can be used in a switchboard environment.

C. Permit unlimited user mobility.

D. Allow call forwarding.

Call back devices are used for authentication in case of remote connectivity and the benefit of this mode is that it provides an audit trail of callers being authenticated via call back modem. Options b, c, d do not hold true and hence choice a is correct answer.

36. A hub is that device which connects-

A. Two LANs using different protocols

B. A LAN with a WAN

C. A LAN with a MAN

D. Two segments of a single LAN

Choice d is correct since use of a hub is to join two segments of a single LAN. It does not join LAN with WAN or MAN nor serve to join two LANs with different protocols.

37. In a social media risk management, what is the MOST important asset an IS auditor will focus on?

A. Brand and reputation

B. Compliance to policy

C. Corrective controls in place

D. None of the above

In a risk based audit involving social media, the organization's brand and reputation are of foremost importance. In e-Commerce activities business runs on brand and reputation of the products and company. Choices b and c may be relevant but in the order of importance, Choice a is the correct answer.

38. In the audit of third party contracts, industry standards advocate which of the following controls as mandatory?

    A. Compliance to SSAE 16 standard

    B. Compliance to ISAE 3402

    C. Right to audit clause in the contract

    D. All of the above

    While a SSAE 16 report serves the purpose, it is not mandatory for all organizations and it requires a CPA to sign it. ISAE 3402 is a UK based standard, not applicable to all organizations. But in the absence of any report the third party provides as per the above standards, the basic control with the organization is a right to audit clause in the contract. Auditors of the outsourcing organization has a right to visit the service provider and check out its BCM arrangements and a capacity to provide services continuously even in times of a disaster or outage. Hence Choice c is the correct answer.

39. What are the opportunities for IS auditor in terms of training?

    A. Training IT professionals on controls

    B. Training internal audit staff

    C. Creating security awareness amongst client personnel

    D. All the above

    Training is a very good area for IS professionals in the field of security awareness, controls and making internal audit staff adopt a risk based audit approach. So Choice d is the best choice.

40. Which of the following is NOT a type of Business Analytics?

    A. Descriptive analysis

    B. Retrospective analysis

    C. Predictive analysis

    D. Prescriptive analysis

    Choice a, c, d are types of business analytics by definition. Hence Choice b is the correct answer.

41. Control in design of an information system is used to

    A. inspect the system and check that it is built as per specifications

    B. protect data from accidental or intentional loss

    C. ensure that the system processes data as it was designed to and that the results are reliable

D. ensure privacy of data processed by it

Choice a stresses on system specifications as it was built. Choice b talks of protection against accidental or intentional loss which is not the sole purpose of embedded controls. Choice d talks of preservation of privacy of data which is again not the sole objective. The main objective of controls embedded within a system is to ensure that processing of data takes place as desired and it gives accurate results. Hence Choice c is the correct answer.

42. Controls are necessary in information systems as-

A. Massive amount of data are processed and chances of human errors in data entry is more.

B. Accidental errors can cause loss of money and credibility

C. Protect the system from virus attack

D. Disk may crash causing data loss

Choice a is the correct answer since information systems process large amount of data and errors in data entry are more. Choice b merely indicates consequence of errors and c and d are related to external attacks through virus. But when new systems are set, controls are defined because volume of processing is more and human intervention in the form of data entry cannot be avoided.

43. Audit in the design of information system is used to-

A. inspect the system and check that it is built as per specifications

B. protect data from accidental or intentional loss

C. ensure that the system processes data as it was designed to and that the results are reliable

D. ensure privacy of data processed by it

When an IS auditor audits the design of a new system, he will check that it meets user specifications as defined during the system requirement phase. Choices b c and d would not be considerations in the audit of system design. Hence choice a is the correct answer.

44. An audit trail is established in a system to-

A. detect errors in a system

B. enable auditing of a system

C. localize the source of an error in a system

D. trail a program

An audit trail is a tool to troubleshoot when problems occur. It helps locate or localize

the source of error in a system and help rectify the error. It does not detect error but helps identify source. It is not merely a program trail but a footprint of processing done by system. Hence choice c is the correct answer.

45. The purpose of parallel run is to-

A. to see whether outputs of a newly computerized system matches those of currently running manual or legacy system

B. have redundancy for reliability

C. test an operational information system

D. test a system being newly designed

The purpose of parallel run is to have fall back and redundancy so that if the new system does not operate as desired, the legacy system would still be there as a fall back and also serve a means to benchmark results from both systems. Although choices a, c and d are partially true the exact purpose ifs brought out by Option b which is correct option.

46. Which of the following is MOST LIKELY to be included in general control procedures?

A. Proper authorization procedures

B. Data and program access policies

C. Data processing operations

D. System Development methodologies

General control procedures must include authorization procedures. Options b, c and d are not general controls. Data and program access will be at application level later. Data processing will involve transaction level examination. System development is different department altogether. Hence choice a is the correct answer.

47. The auditor typically has two roles to play in computer environments. First, (s) he may be responsible for evaluating the client's computer system controls in the course of an audit. Second, (s) he may be able to-

A. Use the computer as a tool to perform the audit more efficiently or effectively.

B. Earn additional revenue by selling hardware systems to audit clients.

C. Provide the IRS with computer files of audit clients.

D. Earn additional revenue by selling software systems to audit clients.

The I.S. audit process revolves around evaluation of controls, performing test of controls and going ahead to test detailed transactions. In this process, he can use the computer to audit the computerized processing of transactions. This is done by use of

computer assisted audit techniques that enable the auditor to perform the audit more efficiently and effectively. The other three alternatives are irrelevant and do not fit into the frame of the question

48. Modern computer technology makes it possible to perform paperless audits. For example, in an audit of computer-processed customer accounts receivable balances, an auditor might use a microcomputer to access the accounts receivable balances, an auditor might use a microcomputer to access the accounts receivable directly and copy selected customer records into the microcomputer for audit analysis. Which of the following is an advantage of this type of paperless audit of accounts receivable balances?

    A. It reduces the amount of substantive testing required.

    B. It allows immediate processing of audit data on a spreadsheet working paper.

    C. It increases the amount of technical skill required of the auditor.

    D. It allows direct confirmation of customer account balances.

    Use of CAAT helps in scanning and extracting huge quantity of data. In the above mentioned case, extracting data for analysis reduces the amount of substantive testing required.

49. Detection risk refers to:

    A. Concluding that material errors do not exist, when in fact they do.

    B. Controls that fail to detect an error.

    C. Controls that detect high-risk errors.

    D. Detecting an error but failing to report it.

    Detection risk refers to the risk that an IS auditor may use an inadequate test procedure and conclude that no material error exists when in fact errors do exist. Other options do not relate to detection risk.

50. Senior management has requested that an IS auditor assist the departmental management in the implementation of necessary controls. The IS auditor should:

    A. refuse the assignment since it is not the role of the IS auditor.

    B. inform management of his/her inability to conduct future audits.

    C. perform the assignment and future audits with due professional care.

    D. obtain the approval of user management to perform the implementation and follow-up.

    In this situation the IS auditor should inform management of the impairment of independence in conducting further audits in the auditee area. An IS auditor can perform non-audit assignments where the IS auditor's expertise can be of use to the

management; however, by performing the non-audit assignment, the IS auditor cannot conduct the future audits of the auditee as his/her independence may be compromised. However, the independence of the IS auditor will not be impaired when suggesting/recommending controls to the auditee after the audit.

51. Which of the following should be the FIRST step of an IS audit?

A. Create a flowchart of the decision branches.

B. Gain an understanding of the environment under review.

C. Perform a risk assessment.

D. Develop the audit plan.

An auditor needs to gain an understanding of the processes prior to creating a flowchart. Based on the scope of the audit, the IS auditor should gain an understanding of the environment under review, and then carry out a risk assessment. Finally, on the basis of understanding the environment under review and the risk assessment, the IS auditor should prepare an audit plan.

52. An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable sampling.

B. substantive testing.

C. compliance testing.

D. stop-or-go sampling.

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

53. Overall business risk for a particular threat can be expressed as:

A. A product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

B. The magnitude of the impact should a threat source successfully exploit the vulnerability.

C. The likelihood of a given threat source exploiting a given vulnerability.

D. The collective judgment of the risk assessment team.

Choice A takes into consideration both the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

54. An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.

B. clearly state audit objectives for the delegation of authority for the maintenance and review of internal controls.

C. document the audit procedures designed to achieve the planned audit objectives.

D. outline the overall authority, scope and responsibilities of the audit function.

An audit charter should state management's objectives for, and delegation of authority to, IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

55. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware:

A. of the point at which controls are exercised as data flow through the system.

B. that only preventive and detective controls are relevant.

C. that corrective controls can only be regarded as compensating.

D. that classification allows an IS auditor to determine which controls are missing.

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

56. An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the network.

B. Users can install software on their desktops.

C. Network monitoring is very limited.

D. Many user ids have identical passwords.

Exploitation of a known user id and password requires minimum technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user ids have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of many user IDs having identical passwords can be high (for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

57. An IS auditor's primary purpose of looking for audit trails is to:

A. Improve response time for users.

B. Establish accountability and responsibility for processed transactions.

C. Improve the operational efficiency of the system.

D. Provide useful information to auditors who may wish to track transactions.

Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

58. In an organization where an IT security baseline has been defined, the IS auditor should FIRST ensure:

A. Implementation.

B. Compliance.

C. Documentation.

D. Sufficiency.

The auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps that can be taken later. Hence choice d is appropriate answer.

59. An IS auditor performing a general controls review of IS management practices relating to personnel should pay particular attention to:

A. Mandatory vacation policies and compliance.

B. Staff classifications and fair compensation policies.

C. Staff training.

D. The functions assigned to staff.

When performing a general controls review it is important for an IS auditor to pay attention to the issue of segregation of duties, which is affected by vacation/holiday practices. Mandatory vacation policies and compliance may vary depending on the country and industry. Staff classifications and fair compensation policies may be a morale issue, not a controls issue. Staff training is desirable, but not as critical as an appropriate segregation of duties. An IS auditor can see segregation through review of functions assigned, hence choice d is the right answer.

60. A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. Recovery.

B. Retention.

C. Rebuilding.

D. Reuse.

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic "paper" makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

61. Which of the following would an IS auditor consider to be the MOST important when evaluating an organization’s IS strategy? That it:

A. Has been approved by line management.

B. Does not vary from the IS department’s preliminary budget.

C. Complies with procurement procedures.

D. Supports the business objectives of the organization.

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Answer A is incorrect since line management prepared the plans. Strategic plans to support business objectives and hence choice d is more appropriate.

62. By information system testing we mean

A. testing an information system correctly

B. determining whether a system is performing as per specifications

C. determining whether a system is performing optimally

D. ensuring proper function of a system

System testing is full testing of system as it exists in the computing environment along with all applications. A system testing would involve checking that it performs as per specification. It is not necessary that it means testing is performed correctly as mentioned in Choice a. Also it does not guarantee optimal performance as per choice c. A testing cannot ensure proper functioning of a system as per choice d. Hence choice b is the correct answer.

63. Which of the following is not relevant with cross training?

A. A breakdown in controls due to insufficient understanding and support.

B. More than one individual has been properly trained to perform a specific job or procedure.

C. It decreases dependence on one employee.

D. It would be prudent to have first assessed the risks of any one person knowing all parts of a system and what exposure in control this may cause.

Choice b is the objective of cross training and c and d are also relevant to cross training. But Choice a is the odd one out which does not indicate cross training but merely a breakdown in controls. So Choice a is the correct answer.

64. The risk that an auditor could not find a control weakness when in fact it was present is called

A. Detection risk

B. Control risk

C. Inherent risk

D. Overall audit risk

Choice a is related to business ad Choice b is related to client. Overall audit risk is a product of all risks faced but by definition detection risk is auditor specific and in this situation fails to find control weakness when in fact it was present. This is failure in audit procedure and is known as detection risk.

65. IS auditors must have a thorough understanding of the risk assessment Process. Risk assessment is a-

A. Subjective process

B. Objective process

C. Mathematical process

D. Statistical process

Risk is perceived differently by different people and the method of treating risk also differs. It is person dependent as to who is doing the risk evaluation hence it is subjective in nature. Though objective measures and mathematical and statistical techniques may be used to calculate loss or impact, the ultimate evaluation of risk is a subjective process. Hence Choice a is the correct answer.

66. The responsibility, authority and accountability of the information systems audit functions is appropriately documented in an audit charter and MUST be-

A. Approved by the highest level of management

B. Approved by audit department

C. Approved by user management

D. Changed every year before commencement of IS audits.

Audit Charter is the letter of appointment for an IS auditor and must be signed by the highest authority. An IS audit is a management audit and they set scope, accountability and responsibility. Hence choice a is the correct answer.

67. GEIT aims at directing IT activities to achieve business objectives for meeting needs of-

A. Investors

B. Shareholders

C. Stakeholders

D. Regulators

GEIT works towards value for stakeholders. Hence choice c is the correct answer.

68. Which of the following is a key component of governance?

A. Security policy

B. Employee rights

C. Transparency

D. Risk assessment

A key component of Governance is transparency whereby stakeholders are kept abreast of all developments and it instils trust amongst them. So option c is the correct answer.

69. Business governance assists Board to understand-

A. Key controls

B. Key performance drivers

C. Risk assessment

D. Enterprise functions

Business governance aims in helping Board in understanding key performance drivers. This is critical to the governance process. Hence choice b is the correct answer.

70. Who is responsible for establishing right organizational structures and setting decision-making accountabilities?

A. Senior management

B. Operational management

C. CIO

D. IT Steering Committee

Senior management is responsible for setting authority responsibility to facilitate day to day operations as well as decision-making priorities. Hence Option a is the correct answer.

71. Which is the primary objective of Enterprise Risk Management (ERM)?

A. Right level of controls

B. Availability of information

C. Tight security at low cost

D. Implement IT best practices

Enterprise risk management evaluates business processes and sets a right level of control structure by doing constant gap analysis and benchmarking with industry standards. Choice a is the correct answer.

72. Enterprise governance and enterprise IT governance needs a balance between

A. Compliance and ROI required by shareholders

B. Profit maximization and wealth maximization fixed by Board

C. Conformance goals and performance goals as set by Board

D. IT risks and cost of implementing IT controls as set by IT.

GEIT warrants a balance between IT risks and the cost of implementing controls to contain these risks Choice d is the correct answer

73. Which is the most important function for IT governance to be effective?

A. Monitoring

B. Evaluation

C. Directing

D. Managing

IT governance is governed by direction from the management and hence directing is the most important function All other options depend on right direction. Hence choice c is the right answer

74. Primary objective of implementing policies, principles and framework

A. Communicate stakeholder intent

B. Benchmark performance with competitors

C. Confirm regulatory compliance

D. Implement corporate governance

The primary purpose of policies and procedures is to convey what the management or stakeholder intends to do and based on this the governance process can be directed. Hence choice a is the best answer.

75. IT risk management process helps in-

A. Prioritizing business functions for audit planning

B. Optimizing internal control framework

C. Ensuring residual risk is at an acceptable level

D. Complying with regulatory requirement

IT risk management process helps in conducting proper risk assessments and aiming to mitigate risks so as to reduce the residual risks to an acceptable level. Hence choice c is the correct answer.

76. Which of the following is a major risk factor?

A. Inflationary trends

B. Vendor launches new software

C. BOD elects new Chairman

D. Change in Govt. post elections

Change of political party can be a big impact for the business. Chairman change may not be derogatory. Inflationary trends may or may not affect your business. Vendor launching a new software will not affect your business. Change in Government post elections will impact business directly and hence choice d is the correct answer.

77. The extent to which an organization can accept financial loss is-

A. Risk tolerance

B. Risk appetite

C. Risk management

D. Risk acceptance

By definition risk appetite is the capacity of the organization to accept loss. .Hence choice b is the correct answer.

78. Which of the following is a strategic IT risk?

A. IS audit may not identify critical non-compliance

B. Networks are not available, it affects customers

C. New application does not achieve expected benefits

D. Defer replacement of obsolete hardware.

Options a, b, c are not related to IT Option d is a risk associated with obsolete hardware if not replaced may not perform as desired and cause problems. Hence choice d is the correct answer.

79. Which of the following is the first action after evaluation of inherent risk?

A. Evaluate implemented controls

B. Update risk register

C. Prepare heat map

D. Prioritize evaluated risks

After evaluating inherent risk, it is important to study the effect of existing controls and evaluate how they serve to mitigate the risks. Choices b,c or d are not consequential to evaluation of inherent risk. Choice a is the right answer.

80. Which of the following is the reason to review risk?

A. Changes in risk factors

B. Change in risk appetite

C. Change in budget

D. Change in risk strategy

Once risk is reviewed, it is an annual or pre-set periodic exercise. But if risk factors change there is need to review risk out of turn .Options b, c or d are not indicative of a review of risk.

81. Which of the following is important consideration for an SLA while outsourcing IT operations to cloud service provider?

A. Ownership of information

B. Periodic audit reports

C. Logical access controls

D. Reduction in operations cost

While outsourcing IT operations to cloud service provider the most important consideration would be to maintain ownership of information. It has to be contracted by means of an SLA. Options b, c or d are other considerations but most important is Option a and hence it is the correct answer.

82. Which of the following is primary input for IT resource capacity planning?

A. Annual financial budget

B. IT resource acquisition plan

C. Number of databases in use

D. Expected growth of business

Capacity planning is done based on future business growth and increased need for resources. Although choice a is equally relevant but planning is based on need and hence choice d is the correct answer.

83. In order for a IT strategic plan to be successful, the organization must first ensure plan focuses on-

A. Optimization of cost

B. Is aligned with business strategy

C. Provides direction for IT deployment

D. Consists of long and short term plans.

IT strategic planning should be aligned to business requirement. Then only optimum utilization of resources can take place. Options a, c or d are not relevant to the context. Hence option b is the correct answer.

84. Objective of resource optimization process is to ensure-

A. Resource needs for the enterprise are minimised.

B. Return on IT investments is ensured.

C. Increased monitoring of benefit realization

D. Making IT infrastructure resilient.

Resource optimization is based on benefits realization. Hence choice c is the right answer.

85. Which of the following is best control for building requisite skills and competencies within an organization?

A. Hiring only qualified personnel

B. Outsourcing critical operations

C. Conducting skill enhancement training

D. Defining skill requirements in job description

The best way to build capability is right training of people and enhancement of skills. All other options give temporary solutions. Hence choice c is the correct answer.

86. Which of the following is function of Information Security Manager?

A. Implement firewalls in the organization

B. Perform IT risk assessment

C. Approve Information Security Policy

D. Define rules for implementing ID

Security Manager is responsible for maintaining security in the organization and he does not authorize rules. He can define rules for implementing ID. Hence option d is the right answer.

87. A data administrator is primarily a-

A. Database administrator

B. Data owner

C. Data custodian

D. Data integrator

A data administrator is not owner of data, he is a custodian of the data. Hence choice c is the correct answer.

88. Which of the following is the most important resource of the organization?

A. Policies and procedures

B. IT infrastructure and applications

C. Information and data

D. Culture, ethics, behaviour

In a data centric business organization, data is the most important asset. Information needed to take decisions is also important in smooth running of the business. Hence choice c is the correct answer.

89. Function of IT Steering Committee is-

A. Align IT objectives with business

B. Approve and manage IT projects

C. Supervise IT and business operations

D. Decide IT strategy for the organization.

Function of IT Steering Committee is to align IT with business. Options b, c, d may be true but a is most appropriate, choice a is correct.

90. Prioritizing IT initiatives is based on-

A. Results of risk assessments.

B. Expected benefits realization

C. Recommendations of CIO

D. Rate of obsolescence of IT

Prioritizing IT initiatives is based on expected benefits realization. It is return on investments that is aimed at. Hence choice b is the correct answer.

91. Which of the following has the highest impact?

A. Absence of business continuity plan

B. Absence of security operations centre

C. Absence of monitoring SLA

D. Absence of risk management process

Absence of a business continuity plan has highest impact on business as it would not be able to recover from disaster. Choice a is the most appropriate answer.

92. In the context of effective information security governance, the primary objective of value delivery is to-

A. Optimize security investments in support of business objectives

B. Implement a standard set of security practices

C. Institute a standards based solution

D. Implement a continuous improvement culture99

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commodization of standards based solutions and implementation of a continuous improvement culture considering security as a process not an event. Hence Option a is the correct answer

93. Which of the following features of a SMART CARD makes it flexible to use?

A. the ability to protect stored information

B. the use of a microprocessor and programmable memory

C. the high speeds at which it is able to operate

D. the capability of storing huge amounts of information per unit of area

The smartcard is not faster than any other type of card by any considerable margin. Although it can protect the information it stores, so can other types of cards. The smartcard does not employ a special system of data compression and therefore doesn't store information more efficiently than other cards. The single most significant advantage is the presence of a microprocessor, which makes this device programmable. Memory cards are not useful for 'dynamic situations', where information is changing all the time

94. Which of the following does NOT use a 'Cryptographic Technique' to protect data?

A. the use of digital signatures

B. data encryption

C. the use of stored encrypted password files

D. using asymmetric keys at 'sender' and 'receiver' nodes

Cryptography describes the process where information is configured such that it has to be 'decoded' in order to extract valuable data. Digital signatures use a cryptographic algorithm to obtain a signature at sender and receiver ends. Data encryption is quite obviously a cryptographic method and 'keys' are used to encode and decode information (asymmetric simply means that the two keys are different). The password file does not contain any data, the encryption protects passwords, NOT data. The data is protected by passwords, which do not classify as a cryptographic technique.

95. Which of the following is the MOST important characteristic of the Internet?

A. The 'secure' surroundings within which it is implemented

B. The ability to provide an open, easy-to-use network

C. It eliminates the need for firewalls

D. It is not necessary to use a fast computer to use the Internet.

The internet was never directed to being a secure network. It was simply a means of transferring open information at an efficient rate. So, it does not provide a secure environment and smaller networks who wish to protect sensitive information MUST implement firewalls. There, is a huge amount of information available through the internet and for the process of information extraction to be efficient, the computers at each node must be fast. Answer B best describes the internet.

96. What is the importance of using Protocols on the Internet?

A. to provide a universal data 'platform' for all connections to use

B. so that nobody gets confused

C. to enable the use of cryptographic techniques

D. to prevent the use of viruses

Protocols for the internet are a set of guidelines or rules that all connections and nodes must comply to. It generates a standard method used to transfer information. If all systems were different then the time involved in transforming data would make the system inefficient. Protocols do not prevent viruses, cryptographic techniques can be used in any situation (with or without protocols).

97. Which of the following is not an illustration of a SMART Card?

A. A credit card which can be used to operate a mobile phone

B. An electronic money card e.g Mondex

C. A drivers licence containing current information about bookings etc.

D. An access control card containing a digitised photo.

A smartcard, by definition, is a plastic card which contains a microprocessor and a programmable memory. A credit card operating a mobile phone is a smart card, as it contains a processor operating the phone line and a data store containing credit information. The money card and drivers licence are also smartcards containing read/write information as well as algorithms for specified operations. The access card can simply contain a magnetic strip which stores information to the access allowed. It does not require a microprocessor and is thus, not a smartcard.

98. In which of the following is damage generally invisible, it is difficult to know the extent of damage?

A. Viruses

B. Computer misuse

C. Computer fraud

D. Theft

One of the problems with any logical breach of security is that damage is invisible and its extent is unknown. This is particularly true for viral infections. The virus may be transferred to any floppy disc that comes into contact with an infected PC. The other alternatives do not exhibit the 'invisible' effect that viruses do.

99. Which of the following can be used MOST effectively to prevent a logical breach of security?

A. operating system and other system software

B. computer architectural design

C. distributed systems design

D. network design

All the alternatives stated can be used to protect a network. The most effective of these is the use of operating systems.

100. Why is it that Traditional Methods of authentication are found unsuitable for Computer Networks?

A. They do not use cryptographic techniques

B. They do not permit high speed data flow

C. They use passwords

D. They are incompatible with the internet

The main problem with traditional methods is the fact that cryptographic techniques are not employed. With the modern technological revolution, computer 'hackers' have increased knowledge about internet tracking and using unencrypted passwords has become insufficient for protection.

101. What can a firewall protect against?

A. Viruses

B. Unauthenticated interactive logins from the "outside" world

C. Fire

D. Connecting to and from the "outside" world

Generally firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. This, more than anything, helps prevent vandals from logging into machines on your network. Firewalls can't protect very well against viruses, since there are too many way of encoding binary files from transfer over networks, and too

many different viruses to try to search for them all. If don't want to connect to "outside" world, we don't need the firewall in the first place.

102. What is the purpose of access controls within the organization?

A. To authorise full access to authorised users

B. To limit the actions or operations that a legitimate user can perform

C. To stop unauthorised users accessing resources

D. To protect computers from viral infections

The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security. By using this method, we are protecting the system from both external and internal corruption.

103. Which of the following is NOT a good property of a firewall?

A. only authorised traffic must be allowed to pass through it

B. the firewall itself, should be immune to penetration

C. it should allow for easy modification by authorised users

D. traffic must only be allowed to pass from inside to outside the firewall

The only property which is inaccurately defined is the flow of traffic. It is true that traffic must be able to flow from inside to outside BUT authorised traffic must also be able to pass from outside to inside. The firewall must be the most protected part of the system because, if a hacker gains access to its controls, he automatically has access to all the information. Finally, for obvious reasons, the master user should be able to change attributes of the firewall dynamically.

104. When the firm's purpose for their information infrastructure is to make its data and information available to those who are authorized to use it, the firm is seeking the objective of:

A. Authorization

B. Confidentiality

C. Availability

D. Non repudiation

Availability of information systems is the main purpose of

105. Which of the following is not a component of risk management?

A. Set benchmarks

B. Implement controls

C. Set budgetary constraints

D. Approving new systems development

Setting benchmarks is a management function during strategic planning. It is not a part of risk management. Hence Option a is the correct answer.

106. When changes are made to the firm's data, information, and software, the type of information security risk is:

A. Unauthorized disclosure and theft.

B. Unauthorized modification

C. Unauthorized viewing

D. Unauthorized intrusion

Option b is correct since this type of modification is a breach of integrity. Options a, c and d are different types of offences in relation to data. But Option b is most appropriate answer.

107. Which of the following would BEST ensure Continuity in a WAN across the organization?

A. Built-in alternate routing

B. Completing full system backup daily

C. A repair contract with a service provider

D. A duplicate machine alongside each server

Explanation: Alternate routing ensures that the network will continue if a server is lost or a link is severed since message rerouting could be automatic. System backup will not provide immediate protection. A repair contract is not a better option. Standby servers will not be able to provide continuity if a link is severed. Hence option a is correct answer.

108. For which of the following is an information security policy not developed?

A. Hardware and software control

B. Computer use

C. Authorization to information assets

D. System development

Option a is the correct answer. An information security policy covers options b, c and d.

109. In which of the following is a router used in a firewall?

A. Packet filtering firewall

B. Stateful inspection firewall

C. Single homed firewall

D. Dual homed firewall

A router is used in a packet filtering firewall. It is not so in Options b, c and d Hence a is correct answer.

110. Which of the following technical controls protect stored and transmitted information from unauthorized disclosure?

A. Access control

B. Cryptographic control

C. Physical control

D. Biometric control

Encrypted data is the most secure and is protected against unauthorized viewing and modification. Hence Option b is most appropriate answer.

111. The backup plan that is in use when hot and cold sites are in place is referred to as:

A. Contingency

B. Mobility

C. Redundancy Plan

D. Fall back plan

By definition Option b is the correct answer.

112. Which of the following is independent malicious program that need not any host program?

A. Trap doors

B. Trojan horse

C. Virus

D. Worm

Worms do not be attached to any program. They spread and eat away resources on their own. The other three options replicate automatically.

113. Which of the following malicious program do not replicate automatically?

A. Trojan Horse

B. Virus

C. Worm

D. Zombie

Explanation A Trojan does not replicate but is a malicious program that will run when the program to which it is attached runs. Other options, we witness replication. Hence option a is the correct answer.

114. Which of the following programs secretly take over another Internet-attached computer and then uses that computer to launch an attack?

A. Worm

B. Zombie

C. Virus

D. Trap door

This is the function of a zombie and hence by description Choice b is the correct answer.

115. How are viruses spread?

A. Through Firewalls

B. Downloading infected programs and files from internet.

C. Garbled information.

D. Install anti-virus.

The most common method by which virus propagate is by downloading infected programs through Internet. Firewalls are security devices and installing anti-virus will help prevent viruses from entering your system. Garbling information does not lead to virus infestation. Choice b is the correct answer.

116. How do users prevent and protect themselves against viruses?

A. Do not open e-mail attachments, use an OS that has virus security features, and scan other users' media storage devices before using them on your computer.

B. Missing Files or folders should be deleted.

C. Files with weird and obscene messages should be stored.

D. Delete unwanted SPAM from your computer.

The golden rule is to avoid e-mail attachments that come from unknown sources, take precautions to scan others' media storage devices before using on own computer and have a virus program up and running to protect the machine. Options b, c, d are not relevant in the contest. Choice a is the most appropriate answer.

117. An information system always-

A. Transforms inputs to information

B. Requires hardware to house programs

C. Gives accurate results

D. Is vulnerable to modification

All information system software, utilities and programs need hardware to house it and hence infrastructure and hardware platforms form an integral part of the study in information systems. Hence Choice b is the most appropriate answer.

118. Operating systems software is primarily aimed at

A. Supporting business users in their tasks.

B. Running operations in system

C. Performing network monitoring

D. Serves as a front end processor

Since the main function of the OS is to allow resource sharing and to help user carry out his task, it acts like a driver to help user carry out his daily activities. Choice b of running operations is not true, Choice d is also not true in the context. Choice a is the most appropriate answer.

119. An example of an information to support strategic management is:

A. Business intelligence system

B. Artificial intelligence

C. Decision support systems

D. Management information system

Explanation Business Intelligence Systems help management to analyze, evaluate and help take strategic decisions. Although b, c, d also support decision making a is most appropriate answer.

120. An example of an information that supports operational management is-

A. Business intelligence systems

B. Electronic document management

C. Management information system

D. None of the above

Electronic document management facilitates trading partners to electronically exchange documents and conduct business. Since this is an integral part of operations management, Choice b is the most appropriate answer.

121. Which type of software is focused on supporting communication, collaboration and coordination?

A. Groupware

B. Workflow

C. Middleware

D. Freeware

By definition Groupware supports communication, collaboration and coordination within systems. B, c, d all serve limited purpose. Hence Choice a is the correct answer.

122. The criterion used to assess how user and business needs are met in software is:

A. Functionality

B. User interface

C. Cost

D. Efficiency

No matter what the functionality or what quality the user interface may be, cost to be considered in the beginning itself but efficiency rules large and is used as a criterion to assess whether business needs are being fulfilled by the software application. Hence d is the correct answer.

123. Multipartite viruses attack on

A. files

B. boot sector

C. memory

D. all of the mentioned

By definition all options a, b and c hold good. Hence choice d is the correct answer.

124. Which one of the following is not an attack, but a search for vulnerabilities to attack?

125. denial of service

A. port scanning

B. memory access violation

C. dumpster diving

Port scanning is used in a vulnerability assessment in order to find open ports, it is not an attack by itself. Other options are examples of attack. Choice b is the right answer.

126. File virus attaches itself to the

A. source file

B. object file

C. executable file

D. all of the mentioned

File virus attaches itself to executable file. Other options do not hold good. Choice c is the correct option.

127. When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called

A. denial-of-service attack

B. slow read attack

C. spoofed attack

D. starvation attack

The computer crime that makes a machine or network unavailable to its intended users is called a denial of service attack. Choices b, c or d does not hold good. Choice a is the correct answer.

128. This type of virus is activated when a user runs an application such as a word processor or spreadsheet-

A. Boot sector virus

B. Macro virus

C. Polymorphic virus

D. None of the above

Choice b is the correct answer.

129. A security measure to enable accidentally or deliberately deleted data to be resurrected is:

A. Risk mitigation

B. Backup/restore

C. Off site storage

D. Redundancy

Accidentally or damaged data can be restored through backup restore. Risk mitigation is a risk treatment method and offsite storage is a practice of periodically storage of data off site for business continuity. Redundancy can be maintaining same data in multiple locations to help reconstruct data in case of hardware failure, but the process by which to restore is in Choice b. Hence it is the correct answer.

130. What is the name of the mechanism whereby an unverified entity that seeks access to a resource proposes a label by which they are known to the system?

A. Authentication

B. Authorization

C. Identification

D. Non-repudiation

User ID is the first means of identification and password is assigned to the user which he changes and maintains as per policy. So first is Identification and then password authentication. Choice c is the correct answer.

131. What allows a firewall to react to emergent event and update or create rules to deal with event?

A. Dynamic filtering

B. Static filtering

C. Stateful inspection

D. First generation filtering

Dynamic filtering allows firewalls to react proactively to emergent events and update or create rules to deal with the event. This facility is not available in Option b, c and d. Choice a is most appropriate answer.

132. While evaluating the collective effect of preventive detective and corrective controls, within a process, an IS auditor should be aware of which of the following?

A. Only preventive and detective controls are relevant

B. The point at which the control is exercised as data passes through the system

C. Corrective controls are regarded as compensating

D. Classification allows the auditor to identify which controls are missing

It is important that IS auditor study the data flow and point of origin of a control in order to understand whether system will be able to give accurate results. Option a is not true and Option c is also not true. An auditor does not perform classification to identify missing controls but to test the efficacy of controls. Hence Option b is the correct answer.

133. Which of the following is a network diagnostic tool for monitoring and recording network information?

A. Online monitor

B. Downtime report

C. Help desk report

D. Protocol analyzer

Protocol analyzers are network diagnostic tools that monitor and record network information from packets travelling in the link to which the analyzer is attached. Choice a, online monitors measure telecommunication transmission and determine whether the transmissions are accurate and complete. Downtime reports indicate non availability of systems and help desk reports trace on problems reported by users. Hence by definition, choice d is the correct answer.

134. A context diagram is used

A. As the first step in developing a detailed DFD of a system

B. In systems analysis of very complex systems

C. As an aid to system design

D. As an aid to programmer

Option a is true for context diagram. Choices b, c or d do not hold true. Hence a is correct answer.

135. Which of the following is/are the sources for project requests?

A. Request from Department managers

B. Request from senior executives

C. Request from system Analyst

D. All of the above

All choices a, b and c are sources for requests. Hence choice d is the correct answer.

136. A DFD is normally levelled as-

A. It is a good idea in design

B. It is recommended by many experts

C. it is easy to do it

D. It is easier to read and understand a number of smaller DFDs than one large DFD

Option d is true for DFDs and many times smaller DFDs help understand the flow better. Hence Option d is more appropriate.

137. A project is a process with which of the following characteristics?

A. High volume, high variety

B. Low volume, high variety

C. High volume, low variety

D. Low volume, low variety

A project has low volume and high variety. New projects have high variety and initial volume is low. Choices a, c and d are contrary to definition. Choice b is the right answer.

138. What are the main features of a project?

A. Unique with fixed cost and time constraints

B. Unique with variable costs and time constraints

C. Repeatable with variable costs and time constraints

D. Repeatable with low costs and short timescales.

A project is a unique event with fixed time and cost constraints. Options b, c and d do not hold true. Hence choice a is correct answer.

139. In which of the four stages in a project would you determine the milestones or significant events?

A. Planning

B. Scoping

C. Implementation

D. Evaluation

Milestones would be determined during the Scoping stage of the project. Hence answer is b

140. In which of the four stages in a project would you determine the work activities required?

A. Planning

B. Scoping

C. Implementation

D. Evaluation

The work activities would be determined during the Planning stage.

141. Activities can be drawn in a hierarchical structure called a-

A. WBS (Work breakdown Structure)

B. WAS (Work Allocation Structure)

C. WCS (Work Control Structure)

D. WDS (Work Detail Structure)

Activities can be drawn in a hierarchical structure called a work breakdown structure (WBS). Hence by definition, choice a is the correct answer.

142. Analysing the potential risks in a project is conducting which of the following processes

A. Risk evaluation

B. Risk assessment

C. Risk mitigation

D. Risk acceptance

Analysing the potential risks in a project is called risk assessment.

143. A system to ensure that an organization can return to work after a crisis

A. Crisis management system

B. Business continuity management

C. Incident response system

D. None of the above

A system to ensure that an organization can return to work after a crisis is called business continuity planning.

144. The element of service quality which is defined as 'the knowledge and courtesy of employees and their ability to convey trust and confidence'.

A. Responsiveness

B. Assurance

C. Service level

D. Ownership

Activity is known as Assurance and other options do not fit context. Option b is correct answer.

145. Which of the following should not be used when operators use a communication network control language?

A. Down line loading of a program

B. Altering audit trail

C. Transmitting system warning and status messages

D. Monitoring network control terminal

146. Which of the following is not a MAJOR BENEFIT of application software prototyping?

A. Reduction in development cost

B. Faster development of systems

C. Meeting user requirements

D. Redirect software maintenance efforts

Options a, b, c are known benefits of software. Redirecting software maintenance is not a benefit and hence choice d is the correct answer.

147. Which of the following represents a typical prototype of an interactive application?

A. Screens and process programs.

B. Screens, interactive edits, and sample reports.

C. Interactive edits, process programs, and sample reports.

D. Screens, interactive edits, process programs, and sample reports.

In prototyping key processes are screens, interactive edits and sample reports. It does not have process programs. Hence options a, c and d are not correct. Option b is the correct answer.

148. An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

A. References from other customers

B. Service level agreement (SLA) template

C. Maintenance agreement

D. Conversion plan

In a Request for Proposal an IS auditor will look for references as they will determine the criteria for choice of vendor. SLA is after contract is accorded and maintenance contract also comes later. Conversion plan is not seen in the beginning. So choice a is the correct answer.

149. The Quality Assurance Group is typically responsible for:

A. Ensuring that the output received from system processing is complete.

B. Monitoring the execution of computer processing tasks.

C. Ensuring the programs and program changes and documentation adhere established standards.

D. Designing standards and procedures to protect data against accidental disclosure, modification or destruction.

Quality Assurance function it is to check that system development is according to accepted standards. They are not bothered about processing and they do not take part in design. Hence choice c is the correct answer.

150. Which of the following Computer Aided Software engineering (CASE) products is used for developing detailed designs, such as screens and report layouts?

A. Super CASE.

B. Upper CASE

C. Middle CASE

D. Lower CASE

By definition, Middle Case tools aid in developing designs. Hence choice c is the correct option.

151. A criticism of the data flow approach to program design is

A. It is not a top-down design method.

B. There is no assurance that different programmers with generate the same design for a problem.

C. It leads to inefficient programs.

D. It works best for on-line programs rather than batch programs.

Option b is the correct answer, it is feared that there would be a lack of standard design for a problem. Options a, c or d are not holding good in this context.

152. Which of the following is MOST likely to be the motivation for the auditor using program source code review:

A. Generalized audit software is unavailable

B. The auditor believes the program to be reviewed contains inefficient code

C. The program processors only small quantities of data so there is little code available for review.

D. The auditor is unwilling to treat the program as a black box.

An IS auditor who chooses to carry out a program source code review, shows that the auditor does not want to treat the computer as a black box. Option a is insignificant and option b of assuming that code is inefficient is unrealistic. They do not do source code review because amount of code is small. Hence option d is correct answer.

153. Executable specifications are an extension of which of the following system development approaches?

A. Waterfall model.

B. Incremental development model

C. Evolutionary development model

D. Rapid prototyping model

Executable specifications are a feature of rapid prototyping model which is used for rapid development of systems. It does not hold good for Options a, b or c. Option d is the correct answer.

154. A systems analyst should have access to each of the following except

A. Source code

B. Password identification tables.

C. User procedures

D. Edit criteria.

A system analyst should not have access to password identification tables. This would violate the security provisions. Hence choice b is the correct answer.

155. During the entry phase the system designer

A. Explains to users various alternative designs that can be implemented

B. Attempts to determine what problem is the real motivation for the system development effort

C. Assists users to formulate the strategic design

D. Attempts to unfreeze the organizations

Explanation: During the entry phase, the system designer has to face resistance to change. In this situation he has to prepare the organization for the new system, this is known as unfreezing the organization. Fter the new development is done, the

organization gets refreeze. Option a, b c comes once the organization is geared for change. Hence d is correct option.

156. The primary difference between program testing and system testing is:

A. Program testing is more comprehensive than system testing

B. System testing focuses on testing the interfaces between programs, whereas program testing focuses on individual programs.

C. System testing is concerned with testing all aspects of a system including job designs and reward system designs.

D. Programmers have no involvement in system testing, whereas designers are involved program testing.

Option a is not true. Options c and d does not bring out difference between the two. Option b holds true as system testing tests interfaces and program testing tests individual programs. Hence option b is correct answer.

157. Which of the following characteristics of user-developed systems has been identified in empirical research:

A. Usually have only a single user.

B. Typically obtain data from a centralized database.

C. Often perform important, day-to-day operational functions.

D. All of the above.

User developed systems or end user computing is generally to enable users to perform operational tasks using small self-developed systems. Option a is not true. It is not necessary that data is obtained for a centralized database in user developed systems. Hence option c is the most appropriate option.

158. Pseudocode is needed because:

A. High-level design cannot be expressed in code that is compilable

B. It ensures the “GO TO” statement is not used

C. It is easy to use by unskilled programmers

D. It provides an informal way of expressing a design

Option a is correct because high level design cannot be compilable and pseudocode has to be used. Options b, c or d does not hold true.

159. The information systems requirements plan is derived directly from the:

A. Information systems applications and facilities plan

B. Information systems strategic plan

C. Master plan

D. Organizational strategic plan

Systems requirement plan is not originating from systems application and facilities plan. Option c and d are also not relevant Information systems requirements can come from Information Systems strategic plan not even from organizational strategic plan. Hence choice b is correct answer.

160. Which of the following might be output as a result of using a CASE tool?

A. Programming code

B. Flowcharts and data flow diagrams

C. Prototypes and cost/benefit analysis

D. All of the above

CASE tools are useful in system development and various types of tools are now available for diagramming, analysis, and for data flow diagrams. Hence d is the correct answer.

161. An IS auditor performing a review of the IS department discovers that formal project approval procedures do not exist. In the absence of these procedures, the IS manager has been arbitrarily approving projects that can be completed in a short duration and referring other, more complicated projects to higher levels of management for approval. The IS auditor should recommend as a FIRST course of action that:

A. Users participate in the review and approval process.

B. Formal approval procedures be adopted and documented.

C. Projects be referred to appropriate levels of management for approval.

D. The IS manager's job description be changed to include approval authority.

Option a is not advisable. Since formal procedures do ont exist, first recommendation that an IS auditor should make is that formal approval procedures be documented and adopted. Who should approve is management decision. Hence option d is not true. Correct choice is b.

162. Which one is not an Infrastructure Software?

A. DBMS

B. Operating system

C. Compiler

D. Result oriented system

DBMS, OS, Compiler are all components of infrastructure. But a result oriented system need not be a computer related system. It can be a management system, an HR system etc. So choice d is the correct answer.

163. All modules of the system are integrated and tested as complete system in case of-

A. Bottom-up testing

B. Top-down testing

C. Sandwich testing

D. Big-Bang testing

A Big Bang testing involves exercising the entire system including all modules after integration. Other options do not hold good in this situation. Hence Option d is correct answer.

164. Site of beta testing is-

A. Software company

B. User site

C. Tester site

D. All of the above

Beta testing is done in live environment Hence choice b is the correct answer.

165. Which of the following is NOT a product metric?

A. Productivity

B. Size

C. Reliability

D. Functionality

Size, reliability and functionality are all measures of product metric. Productivity is related to any machine, system or person. Hence choice a is the correct answer.

166. Estimate of size of project is dependent on-

A. Cost

B. Time

C. Schedule

D. None of the above

it is not possible to estimate or measure based on options a, b or c. Hence choice d is the correct answer.

167. Which of the following is NOT a level in the Capability Maturity Model?

A. Repeatable

B. Ad hoc

C. Reusable

D. Organised

By definition choices a, b and d are levels in CMM model. Hence choice c is the correct answer.

168. Spiral model begins with-

A. Design

B. Risk analysis

C. Coding

D. Customer communication

Customer communication is vital for successful design and development. Hence choice d is the correct answer.

169. The main activity of the design phase of the system life cycle is to-

A. Replace system with a new one

B. Develop and test a new system

C. Understand current system

D. Propose alternatives to current system

Main activity in design phase is to suggest alternative models for proposed system. It is not always to replace an old system. Understanding current system and developing a new system will happen later stage. Hence choice d is the correct answer.

170. What is operating system?

A. collection of programs that manages hardware resources

B. system service provider to the application programs

C. link to interface the hardware and application programs

D. all of the mentioned

Options a, b and c are all functions of an OS Hence choice d is the correct answer.

171. To access the services of operating system, the interface is provided by the

A. system calls

B. API

C. library

D. assembly instructions

Option a is the correct answer. By definition, this option holds good. Options b, c or d does not hold good.

172. Which one of the following error will be handle by the operating system?

A. Power failure

B. lack of paper in printer

C. connection failure in the network

D. all of the mentioned

All options, a, b and c support the answer. Hence choice d is correct answer.

173. The number of resources requested by a process :

A. must always be less than the total number of resources available in the system

B. must always be equal to the total number of resources available in the system

C. must not exceed the total number of resources available in the system

D. must exceed the total number of resources available in the system

In order to meet requirements, it is necessary that sufficiency of resources exist and hence requests for resources should not exceed resources available in the system. Hence option c is correct answer.

174. Which of the following is not a method of file access?

A. Sequential access

B. Direct access

C. Random

D. Indexed sequential access

Direct, sequential and indexed sequential are methods of file access. By elimination option c is the correct answer.

175. What is networked virtual memory?

A. Caching

B. Segmentation

C. RAM disk

D. None of these

By definition caching is the networked virtual memory available with some Oss. Options b and c are not relevant. Option a is the correct answer.

176. A process can be terminated due to-

A. Normal exit

B. fatal error

C. killed by another process

D. all of the mentioned

Options a, b or c all are causing a process to be terminated. Hence choice d is the correct answer.

177. What is interprocess communication?

A. Communication within the process

B. communication between two process

C. communications between two threads of same process

D. none of the mentioned

Inter process communication refers to communication between two processes. Options a or c is not relevant in this context. Hence option b is the correct answer.

178. A set of processes is deadlock if-

A. each process is blocked and will remain so forever

B. each process is terminated

C. all processes are trying to kill each other

D. none of the mentioned

A deadlock is created by concurrent users and in this instance process will be blocked. Options b or c do not hold good. Choice a is the correct answer.

179. Which buffer holds the output for a device?

A. spool

B. output

C. status

D. magic

Printer is the output device which carries a spool to allow a queue of files to be printed. Hence option a is the correct answer.

180. What do we call the process of seeking out and studying practices in other organizations that one's own organization desires to duplicate?

A. Baselining

B. Benchmarking

C. Best practices

D. Due diligence

Process of seeking an studying practices in other organizations is known as Benchmarking. Options a, c or d does not describe this situation. Option b is the correct answer.

181. A review of an EDP system reveals the following items. Which of these is a potential internal control weakness?

A. Backup master files are stored in a remote location

B. Users must verbally approve all changes to be made to application programs

C. Computer operators have restricted access to system programs and data files

D. Computer operators are required to take vacations.

Options a, c and d are good practices and desired. But oral approval for changes is a threat as unauthorized changes may occur. Hence Option b is the correct answer.

182. When obtaining an understanding of an entity=s control environment, an auditor should concentrate on the substance of management=s policies and procedures rather than their form because

A. The auditor may believe that the policies and procedures are inappropriate for that particular entity.

B. The board of directors may not be aware of management=s attitude toward the control environment.

C. Management may establish appropriate procedures and policies but not act on them.

D. The policies and procedures may be so weak that no reliance is contemplated by the auditor.

Through observation, an auditor is able to see beyond the written policies and see if people observe them. If he only depends on existence of policies, it may happen that appropriate policies are documented but not acted upon. Hence choice c is most appropriate. Options a, b and d are not relevant in the context.

183. An on-line sales order processing system most likely would have an advantage over a batch sales order processing system by-

A. Detecting errors in the data entry process more easily by the use of data entry programs.

B. Enabling shipment of customer orders to be initiated as soon as the orders are received.

C. Recording more secure backup copies of the database on magnetic tape files.

D. Maintaining more accurate records of customer accounts and finished goods inventories.

The main advantage of an online sales order processing over a batch processing would be avoidance of delay till the batch is received. It leads to faster execution of the order. Hence choice b is the correct answer. Option a is irrelevant and c and d are not true in this context.

184. Which of the following controls would prevent the following situation? A workers paycheck was incorrectly processed as he had transposed letters in his department identification code, having entered AABC@ an invalid code, instead of ACAB

A. Control total

B. Limit test

C. Internal label check

D. Table look up procedure

Option d is the correct answer as a table look up checks for transposition errors. Control test and limit test apply to numeric fields only. Internal labels are used for file identification it will not detect transposition errors. Hence choice d is the correct answer.

185. Programmers should do all except-

A. Test programs for proper performance

B. Evaluate legitimacy of transactions data input

C. Develop flowcharts for new applications

D. Programmers should perform each of the above

It is programmers duty to test programs and develop flowcharts for new applications. But programmers have no know how nor duty to get into the validity of transactions input into the system. Hence option b is the correct answer.

186. Output controls are not designed to assure that data generated by the computer are:

A. Accurate

B. Distributed only to authorized people

C. Complete

D. Used appropriately by employees in making decisions.

Output controls should be accurate and complete and should be distributed to authorized personnel only. But how the reports are used by users in decision making is not output control as it is dependent on users whether they use it appropriately or otherwise. Hence choice d is the correct answer.

187. Rather than maintain an internal IT centre, what can companies use to perform many basic functions such as payroll?

A. External service providers

B. External application service providers

C. Internal control service providers

D. Internal auditors

Many organizations have outsourced their payroll to application service providers who calculate and process monthly salaries for them. An external application service provider provides processing services and is hence differentiated from a normal external service provider who may supply any type of service. Internal auditors are internal to the organization and Option c is not relevant to the context. Option b is the correct answer.

188. What is the activity of keeping the firm and its information resources functioning after a catastrophe?

A. Security management

B. Business continuity management

C. Resource management

D. People management

Activity that keeps the firm going after a disaster is called business continuity management. By definition b is the correct answer.

189. An incremental backup-

A. Copies selected files

B. Copies all files

C. Copies all files since the last full backup

D. Copies all files changed since the last full or incremental backup

Option c is the correct answer, the concept of incremental refers to differential backup that is since the last full backup. Options a, b and d do not hold good in the context.

190. What is the maximum length of time that an organization can tolerate between data backups?

A. Recovery service point (RSP)

B. Recovery point objective (RPO)

C. Optimal recovery time frame (ORT)

D. Recover time objective (RTO)

By definition the maximum data loss that an organization can take in case of outage or between data backups is called the Recovery Point Objective or RPO. Option b is the correct answer. In this context other 3 options are not relevant.

191. Another name for Contingency Planning is-

A. Synergy planning

B. Ad hoc planning

C. Business level planning

D. Scenario planning

Contingencies refer to planning for future events based on imagined different scenarios. Options a, b and c does not indicate any event in future. Option d is the correct answer.

192. What is a definition of an objective?

A. A defined specified outcome to be achieved in the long-term

B. A clear set of goals to be attained given a set number of resources

C. A clearly defined and measurable outcome to be achieved over a specified timeframe

D. set standard of performance agreed by workers and managers.

An objective must be measurable over a timeframe to determine whether or not it has been achieved.

193. Which is not a recognised form of business continuity planning?

A. Building planning

B. IT plan

C. Strategic plan

D. Short term plan

Building planning is not part of a continuity planning but a necessary process of acquiring premises.

194. What is the definition of a scenario in scenario planning?

A. An unpredictable event

B. An imagined sequence of future events

C. A planned for event

D. An unplanned event

Scenarios are about trying to imagine what could happen in the future. It is defined as an imagined sequence of future events. Option b is the correct answer as other options do not refer to future events.

195. What one of the following is NOT a key management skill in planning?

A. Conceptual skills

B. IT & computing skills

C. People skills

D. Analytical skills

IT and computing skills are useful but not necessarily one of the key skills that managers require. Hence Option b is the correct answer.

196. What plan describes the details for recovery when a disaster hits an organization?

A. Disaster diagram

B. Disaster and revival plan

C. Recovery plan

D. Business continuity plan

Details of recovery are described in the disaster recovery plan. Disaster and revival may talk about restoration of business and disaster diagram is not going to show recovery plan. It is part of the business continuity plan but recovery plan lays down specific tasks to be conducted during a disaster. Option c is the correct answer.

197. The primary objective of testing a business continuity plan is-

A. Familiarize employees with plan

B. Ensure all residual risks have been addressed

C. Exercise all possible scenarios

D. Identify limitations of the business continuity plan

Option a is mandatory, Option b is an assumption and sometimes it may not be possible to cover all scenarios. But the main objective of a business continuity plan testing is to

observe its performance and coordination and find out faults of limitations to be documented as 'lessons learnt' Hence Option d is the correct answer.

198. During the design of a business continuity plan the business impact analysis (BIA) identifies critical processes and supporting applications. This will primarily influence the-

A. Responsibility for maintaining the business continuity plan

B. Criteria for selecting a recovery site provider

C. Recovery strategy

D. Responsibilities of key personnel.

Results from the business impact analysis will be reviewed by management on the basis of which BCM strategy will be formulated. Options a, b and d will spring out of strategy and hence c is the correct answer.

199. Activation of an enterprise business continuity plan should be based on predetermined criteria that address the-

A. Duration of the outage

B. Type of outage

C. Probability of outage

D. Cause of outage

The activation and declaration of disaster is directly based on how long the outage is going to last. This will set the severity levels. Options b, c and d will be considered later. But Option a is of primary importance and hence the correct answer.

200. An IS auditor can verify that an organization's BCP is effective by reviewing-

A. Alignment of BCP with industry best practices

B. Results of BCP tests performed by IS and end-user personnel

C. Offsite facility, its contents security and environmental controls

D. Annual financial cost of BCP activities versus expected benefit of implementation of the plan.

The effectiveness of the BCP can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing stated objectives. Choices a, c or d do not provide assurance of effectiveness of the business continuity testing. Hence choice b is the correct answer.

201. A medium sized organization whose IT disaster recovery measures have been in place and regularly tested for years has just developed a formal BCP. A basic

BCP Tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed next, to verify the adequacy of the new BCP

A. Full scale test wih relocation of all departments including IT to the contingency site

B. Walkthrough test of a series of predefined scenarios with all critical personnel involved.

C. IT disaster recovery test with business departments involved in testing the critical applications

D. Functional test of a scenario with limited IT involvement.

After a table top exercise the next step is to perform a functional test which includes the mobilization of staff, to exercise admin and org functions in a recovery. Since the IT part is there and tested for years, it would be more efficient to verify and optimize the BCP before actually involving IT. in a full scale test. The full scale test would be the last step of the verification process before entering into an annual testing schedule. A full scale test in this situation might fail because it would be the first time that the plan is actually exercised and a number of resources (including iT) and time would be wasted. Walkthrough is the most basic type of testing only used to make key staff familiar with the plan and discuss critical plan elements rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT driven. A disaster recovery test would not help in verifying the admin and org parts of a BCP which are not IT related. Hence choice d is correct answer.

Mock Assessment Test Paper 5

1. In a data warehouse, data quality is achieved by:

   A. cleansing.

   B. restructuring.

   C. source data credibility.

   D. transformation.

   Correct Answer: C. source data credibility.

   Explanation: In a data warehouse system, the quality of data depends on the quality of the originating source. Choices A, B and D relate to the composition of a data warehouse and do not affect data quality. Restructuring, transformation and cleansing all relate to reorganization of existing data within the database.

2. Which of the following is the GREATEST risk when implementing a data warehouse?

   A. Increased response time on the production systems

   B. Access controls that are not adequate to prevent data modification

   C. Data duplication

   D. Data that is not updated or current

   Correct Answer: B. Access controls that are not adequate to prevent data modification

   Explanation: Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

3. Which of the following is critical to the selection and acquisition of the correct operating system software?

   A. Competitive bids

   B. User department approval

   C. Hardware configuration analysis

   D. Purchasing department approval

Correct Answer: C. Hardware configuration analysis

Explanation: The purchase of operating system software is dependent on the fact that the software is compatible with the existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

4. Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

   A. Utilization reports

   B. Hardware error reports

   C. System logs

   D. Availability reports

   Correct Answer: D. Availability reports

   Explanation: IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

5. A benefit of quality of service (QoS) is that the:

   A. entire network's availability and performance will be significantly improved.

   B. telecom carrier will provide the company with accurate service-level compliance reports.

   C. participating applications will have guaranteed service levels.

   D. communications link will be supported by security controls to perform secure online transactions.

   Correct Answer: C. participating applications will have guaranteed service levels.

   Explanation: The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved, while the speed of data exchange for specific applications could be faster. Availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

6. For an online transaction processing system, transactions per second is a measure of:

   A. throughput.

   B. response time.

   C. turnaround time.

   D. uptime.

   Correct Answer: A. throughput.

   Explanation: Throughput measures how much work is done by a system over a period of time; it measures the productivity of the system. In an online transaction processing system, transactions per second is a throughput index. Response time is defined as the length of time that elapsed between submission of an input and receipt of the first character of output in an online system. Turnaround time is the length of time that elapsed between submission of a job and receipt of a completed output. It is a measure of timeliness in a batch system. The percentage of time that the system is available for processing is called uptime or a reliability index; thus, this is not the correct answer.

7. Which of the following is MOST important when assessing services provided by an Internet service provider (ISP)?

   A. Performance reports generated by the ISP

   B. The service level agreement (SLA)

   C. Interviews with the provider

   D. Interviews with other clients of the ISP

   Correct Answer: B. The service level agreement (SLA)

   Explanation: A service level agreement provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed service. Choices A, C and D would not be the basis for an independent evaluation of the service.

8. Which of the following would normally be found in application run manuals?

   A. Details of source documents

   B. Error codes and their recovery actions

   C. Program flowcharts and file definitions

   D. Change records for the application source code

   Correct Answer: B. Error codes and their recovery actions

   Explanation: Application run manuals should include actions to be taken by an operator

when an error occurs. Source documents and source code are irrelevant to the operator. Although dataflow diagrams may be useful, detailed program diagrams and file definitions are not.

9. Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

   A. The use of diskless workstations

   B. Periodic checking of hard drives

   C. The use of current antivirus software

   D. Policies that result in instant dismissal if violated

   Correct Answer: B. Periodic checking of hard drives

   Explanation: The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

10. An IS auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late-night shift a month as the senior computer operator. The MOST appropriate course of action for the IS auditor is to:

   A. advise senior management of the risk involved.

   B. agree to work with the security officer on these shifts as a form of preventative control.

   C. develop a computer-assisted audit technique to detect instances of abuses of this arrangement.

   D. review the system log for each of the late-night shifts to determine whether any irregular actions occurred.

   Correct Answer: A. advise senior management of the risk involved.

   Explanation: The IS auditor's first and foremost responsibility is to advise senior management of the risk involved in having the security administrator perform an operation's function. This is a violation of separation of duties. The IS auditor should not get involved in processing.

11. An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

A. the setup is geographically dispersed.

B. the network servers are clustered in a site.

C. a hot site is ready for activation.

D. diverse routing is implemented for the network.

Correct Answer: B. the network servers are clustered in a site.

Explanation: A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backups if a site has been destroyed. A hot site would also be a good alternative for a single-point-of-failure site.

12. To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files

B. Enabled access control software parameters

C. Logs of access control violations

D. System configuration files for control options used

Correct Answer: D. System configuration files for control options used

Explanation: A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

13. A Ping command is used to measure:

A. attenuation.

B. throughput,

C. delay distortion.

D. latency.

Correct Answer: D. latency.

Explanation: Latency, which is measured using a Ping command, represents the delay that a message/packet will have in traveling from source to destination. A decrease in amplitude as a signal propagates through a transmission medium is called attenuation. Throughput, which is the quantity of work per unit of time, is measured in bytes per second. Delay distortion represents delay in transmission because the rate of propagation of a signal along a transmission line varies with the frequency.

14. Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

    A. A system downtime log

    B. Vendors' reliability figures

    C. Regularly scheduled maintenance log

    D. A written preventive maintenance schedule

    Correct Answer: A. A system downtime log

    Explanation: A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

15. Which of the following is the MOST effective means of determining which controls are functioning properly in an operating system?

    A. Consulting with the vendor

    B. Reviewing the vendor installation guide

    C. Consulting with the system programmer

    D. Reviewing the system generation parameters

    Correct Answer: D. Reviewing the system generation parameters

    Explanation: System generation parameters determine how a system runs, the physical configuration and its interaction with the workload.

16. Capacity monitoring software is used to ensure:

    A. maximum use of available capacity.

    B. that future acquisitions meet user needs.

    C. concurrent use by a large number of users.

    D. continuity of efficient operations.

    Correct Answer: D. continuity of efficient operations.

    Explanation: Capacity monitoring software shows the actual usage of online systems vs. their maximum capacity. The aim is to enable software support staff to ensure that efficient operation, in the form of response times, is maintained in the event that use begins to approach the maximum available capacity. Systems should never be allowed to operate at maximum capacity. Monitoring software is intended to prevent this. Although the software reports may be used to support a business case for future acquisitions, it would not provide information on the effect of user requirements and it

would not ensure concurrent usage of the system by users, other than to highlight levels of user access.

17. An independent software program that connects two otherwise separate applications sharing computing resources across heterogeneous technologies is known as:

    A. middleware.

    B. firmware.

    C. application software.

    D. embedded systems.

    Correct Answer: A. middleware.

    Explanation: Middleware is independent software that connects two otherwise separate applications sharing computing resources across heterogeneous technologies. Firmware is software (programs or data) that has been written onto read-only memory (ROM). It is a memory chip with embedded program code that holds its content when power is turned off. Firmware is a combination of software and hardware. Application software are programs that address an organization's processes and functions as opposed to system software, which enables the computer to function.

18. IS management has recently informed the IS auditor of its decision to disable certain referential integrity controls in the payroll system to provide users with a faster report generator. This will MOST likely increase the risk of:

    A. data entry by unauthorized users.

    B. a nonexistent employee being paid.

    C. an employee receiving an unauthorized raise.

    D. duplicate data entry by authorized users.

    Correct Answer: B. a nonexistent employee being paid.

    Explanation: Referential integrity controls prevent the occurrence of unmatched foreign key values. Given that a nonexistent employee does not appear in the employees table, there will never be a corresponding entry in the salary payment's table. The other choices cannot be detected by referential integrity controls.

19. Following a reorganization of a company's legacy database, it was discovered that records were accidentally deleted. Which of the following controls would have MOST effectively detected this occurrence?

    A. Range check

    B. Table lookups

C. Run-to-run totals

D. One-for-one checking

Correct Answer: C. Run-to-run totals

Explanation: Run-to-run totals would have been an effective detective control over processing in this situation. Table lookups and range checks are used for data validation before input, or as close to the point of origination as possible. One-for-one checking is time-consuming and, therefore, less effective.

20. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called:

A. alternative routing.

B. diverse routing.

C. redundancy.

D. circular routing.

Correct Answer: B. diverse routing.

Explanation: Diverse routing is the method of routing traffic through split-cable facilities or duplicate-cable facilities, which can be accomplished with different/duplicate cable sheaths. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics. Redundancy involves providing extra capacity, with an option to use such excess capacity in the event the primary transmission capability is not available. Circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open system interconnection.

21. Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management

B. Topological mappings

C. Application of monitoring tools

D. Proxy server trouble shooting

Correct Answer: A. Configuration management

Explanation: Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally. It also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network

and its connectivity. Application monitoring is not essential and proxy server trouble shooting is used for trouble-shooting purposes.

22. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following must be added to the IS auditor's computer to enable it to communicate with the mainframe system?

    A. Buffer capacity and parallel port

    B. Network controller and buffer capacity

    C. Parallel port and protocol conversion

    D. Protocol conversion and buffer capability

    Correct Answer: D. Protocol conversion and buffer capability

    Explanation: For the IS auditor's microcomputer to communicate with the mainframe, the IS auditor must use a protocol converter to convert the asynchronous and synchronous transmission. Additionally, the message must be spooled to the buffer to compensate for different rates of data flow.

23. The interface that allows access to lower- or higher-level network services is called:

    A. firmware.

    B. middleware.

    C. X.25 interface.

    D. utilities.

    Correct Answer: B. middleware.

    Explanation: Middleware, a class of software employed by client-server applications, provides services, such as identification, authentication, directories and security. It facilitates client-server connections over the network and allows client applications to access and update remote databases and mainframe files. Firmware consists of memory chips with embedded program code that hold their content when the power is turned off. X.25 interface is the interface between data terminal equipment and data circuit terminating equipment for terminals operating in the packet mode on some public data networks. Utilities are system software used to perform system maintenance and routines that are required during normal processing, such as sorting or backup.

24. Which of the following controls will detect MOST effectively the presence of bursts of errors in network transmissions?

    A. Parity check

    B. Echo check

    C. Block sum check

    D. Cyclic redundancy check

    Correct Answer: D. Cyclic redundancy check

    Explanation: The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free. In this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

25. Which of the following types of firewalls provide the GREATEST degree and granularity of control?

    A. Screening router

    B. Packet filter

    C. Application gateway

    D. Circuit gateway

    Correct Answer: C. Application gateway

    Explanation: The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 4) and the ports it is directed to (in this case port 80, layer 4), it also checks every http command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and B) basically work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4 (not from higher levels). A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that, during an

external access, instead of opening a single connection to the internal server, two connections are establishedâ€"one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

26. Which of the following reports is a measure of telecommunication transmissions and determines whether transmissions are completed accurately?

    A. Online monitor reports

    B. Downtime reports

    C. Help desk reports

    D. Response-time reports

    Correct Answer: A. Online monitor reports

    Explanation: Online monitors measure telecommunication transmissions and determine whether transmissions are completed accurately. Downtime reports track the availability of telecommunication lines and circuits. Help desk reports handle problems occurring in the normal course of operations. Response-time reports identify the time it takes for a command entered at a terminal to be answered by the computer.

27. Which of the following is MOST directly affected by network performance monitoring tools?

    A. Integrity

    B. Availability

    C. Completeness

    D. Confidentiality

    Correct Answer: B. Availability

    Explanation: In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

28. Checking for authorized software baselines is an activity addressed within which of the following?

    A. Project management

    B. Configuration management

C. Problem management

D. Risk management

Correct Answer: B. Configuration management

Explanation: Configuration management accounts for all IT components, including software. Project management is about scheduling, resource management and progress tracking of software development. Problem management records and monitors incidents. Risk management involves risk identification, impact analysis, an action plan, etc.

29. Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

A. Firewalls

B. Routers

C. Layer 2 switches

D. VLANs

Correct Answer: A. Firewalls

Explanation: Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

30. To evaluate the referential integrity of a database, an IS auditor should review the:

A. composite keys.

B. indexed fields.

C. physical schema.

D. foreign keys.

Correct Answer: D. foreign keys.

Explanation: A foreign key is a column in a table that references a primary key of another table, thus providing the referential integrity. Composite keys consist of two or

more columns designated together as a table's primary key. Field indexing speeds up searches, but does not ensure referential integrity. Referential integrity is related to the logical schema, not the physical schema.

31. Which of the following operating system mechanisms checks each request by a subject (user process) to access and use an object (e.g., file, device, program) to ensure that the request complies with a security policy?

    A. Address Resolution Protocol

    B. Access control analyzer

    C. Reference monitor

    D. Concurrent monitor

    Correct Answer: C. Reference monitor

    Explanation: A reference monitor is an abstract mechanism that checks each request by a subject (user process) to access and uses an object (e.g., file, device, program) to ensure that the request complies with a security policy. A reference monitor is implemented via a security kernel, which is a hardware/software/firmware mechanism. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address that is recognized in the local network. An access control analyzer is an audit utility for analyzing how well access controls have been implemented and maintained within an access control package. A concurrent monitor is an audit utility that captures select events as application systems are running to facilitate assessing program quality.

32. Which of the following is an operating system access control function?

    A. Logging user activities

    B. Logging data communication access activities

    C. Verifying user authorization at the field level

    D. Changing data files

    Correct Answer: A. Logging user activities

    Explanation: General operating system access control functions include log user activities, log events, etc. Choice B is a network control feature. Choices C and D are database- and/or application-level access control functions.

33. An IS auditor is PRIMARILY concerned about electromagnetic emissions from a cathode ray tube (CRT) because they may:

    A. cause health disorders (such as headaches) and diseases.

    B. be intercepted and information may be obtained from them.

C. cause interference in communications.

D. cause errors in the motherboard.

Correct Answer: B. be intercepted and information may be obtained from them.

Explanation: The greatest risk, although infrequent, due to the expensive technology required is choice B. The expense would be justified only if the value of the information to be obtained was high. CRTs can be intercepted, and information obtained can be from them. This is called a tempest attack, taken from the code name of the first secret project in which such an interception was studied. These weak signals can be radiated and intercepted with the proper equipment or transmitted, for example, via power leads. The signals fade rapidly as distance increases. The first line of defense is to create a physical security zone (PSZ) to keep receivers at a distance. They can cause health disorders, such as headaches and diseases; however, no studies have confirmed that these risks are higher than those posed by the natural radiation found in certain zones (e.g., mountain areas). The intensity of the radiation is so low that, with normal technology, they can not cause interference with communications.

34. Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

A. Filters

B. Switches

C. Routers

D. Firewalls

Correct Answer: B. Switches

Explanation: Switches are at the lowest level of network security and transmit a packet to the device to which it is addressed. This reduces the ability of one device to capture the packets that are meant for another device. Filters allow for some basic isolation of network traffic based on the destination addresses. Routers allow packets to be given or denied access based on the addresses of the sender and receiver and the type of packet. Firewalls are a collection of computer and network equipment used to allow communications to flow out of the organization and restrict communications flowing into the organization.

35. In a database management system (DBMS), the location of data and the method of accessing the data are provided by the:

A. data dictionary.

B. metadata.

C. directory system.

D. data definition language.

Correct Answer: C. directory system.

Explanation: A directory system describes the location of data and the access method. A data dictionary contains an index and description of all the items stored in the database. Metadata are the data elements required to define an enterprisewide data warehouse. The data definition language processor allows the database administrator (DBA) to create/modify a data definition for mapping between external and conceptual schemes.

36. In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

A. Diskless workstations

B. Data encryption techniques

C. Network monitoring devices

D. Authentication systems

Correct Answer: C. Network monitoring devices

Explanation: Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

37. When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

A. they are set to meet security and performance requirements.

B. changes are recorded in an audit trail and periodically reviewed.

C. changes are authorized and supported by appropriate documents.

D. access to parameters in the system is restricted.

Correct Answer: A. they are set to meet security and performance requirements.

Explanation: The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control. Reviewing changes to ensure they are supported by appropriate documents is also a detective control. If parameters

are set incorrectly, the related documentation and the fact that these are authorized does not reduce the impact. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set incorrectly, restricting access will still have an adverse impact.

38. By establishing a network session through an appropriate application, a sender transmits a message by breaking it into packets, but the packets may reach the receiver out of sequence. Which OSI layer addresses the out-of-sequence message through segment sequencing?

A. Network layer

B. Session layer

C. Application layer

D. Transport layer

Correct Answer: . D. Transport layer

Explanation: The function of resequencing packets (segment) received out of order is taken care of by the transport layer. Neither the network, session or application layers address resequencing.

39. Which of the following is a control over component communication failure/errors?

A. Restricting operator access and maintaining audit trails

B. Monitoring and reviewing system engineering activity

C. Providing network redundancy

D. Establishing physical barriers to the data transmitted over the network

Correct Answer: C. Providing network redundancy

Redundancy by building some form of duplication into the network components, such as a link, router or switch, to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echo checks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls

40. An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

A. Electromagnetic interference (EMI)

B. Cross-talk

C. Dispersion

D. Attenuation

Correct Answer: D. Attenuation

Explanation: Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

41. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls

B. A compliance test of program library controls

C. A compliance test of the program compiler controls

D. A substantive test of the program compiler controls

Correct Answer: B. A compliance test of program library controls

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

42. A primary benefit derived from an organization employing control self-assessment (CSA)techniques is that it can:

A. Identify high-risk areas that might need a detailed review later

B. Reduce audit costs

C. Reduce audit time

D. Increase audit accuracy

Correct Answer: C. Reduce audit time

A primary benefit derived from an organization employing control self-assessment

(CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

43. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

A. Integrated test facility (ITF)

B. Continuous and intermittent simulation (CIS)

C. Audit hooks

D. Snapshots

Correct Answer: D. Snapshots

A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

44. An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.

B. impact of any exposures discovered.

C. business processes served by the application.

D. application's optimization.

Correct Answer: B. impact of any exposures discovered.

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

45. Which of the following is a substantive test?

A. Checking a list of exception reports

B. Ensuring approval for parameter changes

C. Using a statistical sample to inventory the tape library

D. Reviewing password history reports

Correct Answer: C. Using a statistical sample to inventory the tape library

A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies

and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

46. An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.

B. clearly state audit objectives for and the delegation of authority to the maintenance and review of internal controls.

C. document the audit procedures designed to achieve the planned audit objectives.

D. outline the overall authority, scope and responsibilities of the audit function.

Correct Answer: D. outline the overall authority, scope and responsibilities of the audit function.

An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

47. Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.

B. Periodic testing does not require separate test processes.

C. It validates application systems and tests the ongoing operation of the system.

D. It eliminates the need to prepare test data.

Correct Answer: B. Periodic testing does not require separate test processes.

An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

48. An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.

B. enables the financial and IS auditors to integrate their audit tests.

C. compares processing output with independently calculated data.

D. provides the IS auditor with a tool to analyze a large range of information.

Correct Answer: C. compares processing output with independently calculated data.

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

49. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware:

A. of the point at which controls are exercised as data flow through the system.

B. that only preventive and detective controls are relevant.

C. that corrective controls can only be regarded as compensating.

D. that classification allows an IS auditor to determine which controls are missing.

Correct Answer: A. of the point at which controls are exercised as data flow through the system.

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

50. An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.

B. investigating various communication channels.

C. understanding the responsibilities and authority of individuals.

D. investigating the network connected to different employees.

Correct Answer: C. understanding the responsibilities and authority of individuals.

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

51. Which of the following BEST describes an integrated test facility?

A. A technique that enables the IS auditor to test a computer application for the purpose of verifying correct processing

B. The utilization of hardware and/or software to review and test the functioning of a computer system

C. A method of using special programming options to permit the printout of the path through a computer program taken to process a specific transaction

D. A procedure for tagging and extending transactions and master records that are used by an IS auditor for tests

Correct Answer: A. A technique that enables the IS auditor to test a computer application for the purpose of verifying correct processing

Answer A best describes an integrated test facility, which is a specialized computer-assisted audit process that allows an IS auditor to test an application on a continuous basis. Answer B is an example of a systems control audit review file; answers C and D are examples of snapshots.

52. An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.

B. interview programmers about the procedures currently being followed.

C. compare utilization records to operations schedules.

D. review data file access records to test the librarian function.

Correct Answer: B. interview programmers about the procedures currently being followed.

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

53. Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling

B. Variable sampling

C. Stratified mean per unit

D. Difference estimation

Correct Answer: A. Attribute sampling

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

54. Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.

B. Access controls establish accountability for e-mail activity.

C. Data classification regulates what information should be communicated via e-mail.

D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Correct Answer: A. Multiple cycles of backup files remain available.

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

55. Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management

B. Review of the organization chart

C. Observation and interviews

D. Testing of user access rights

Correct Answer: C. Observation and interviews

By observing the IS staff performing their tasks, the IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees.

Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

56. An IS auditor has evaluated the controls for the integrity of the data in a financial application. Which of the following findings would be the MOST significant?

A. The application owner was unaware of several changes applied to the application by the IT department.

B. The application data are backed up only once a week.

C. The application development documentation is incomplete.

D. Information processing facilities are not protected by appropriate fire detection systems.

Correct Answer: A. The application owner was unaware of several changes applied to the application by the IT department.

Choice A is the most significant finding as it directly affects the integrity of the application's data and is evidence of an inadequate change control process and incorrect access rights to the processing environment. Although backing up the application data only once a week is a finding, it does not affect the integrity of the data in the system. Incomplete application development documentation does not affect integrity of the data. The lack of appropriate fire detection systems does not affect the integrity of the data but may affect the storage of the data.

57. Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

B. the magnitude of the impact should a threat source successfully exploit the vulnerability.

C. the likelihood of a given threat source exploiting a given vulnerability.

D. the collective judgment of the risk assessment team.

Correct Answer: A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

58. An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

A. variable sampling.

B. substantive testing.

C. compliance testing.

D. stop-or-go sampling.

Correct Answer: C. compliance testing.

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

59. A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review later.

B. allows IS auditors to independently assess risk.

C. can be used as a replacement for traditional audits.

D. allows management to relinquish responsibility for control.

Correct Answer: A. can identify high-risk areas that might need a detailed review later.

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Answer B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Answer C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Answer D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

60. Data flow diagrams are used by IS auditors to:

A. order data hierarchically.

B. highlight high-level data definitions.

C. graphically summarize data paths and storage.

D. portray step-by-step details of data generation.

Correct Answer: C. graphically summarize data paths and storage.

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

61. The use of statistical sampling procedures helps minimize:

A. sampling risk.

B. detection risk.

C. inherent risk.

D. control risk.

Correct Answer: B. detection risk.

Detection risk is the risk that the IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when in fact they do. Using statistical sampling, an IS auditor can quantify how closely the sample should represent the population and quantify the probability of error. Sampling risk is the risk that incorrect assumptions will be made about the characteristics of a population from which a sample is selected. Assuming there are no related compensating controls, inherent risk is the risk that an error exists, which could be material or significant when combined with other errors found during the audit. Statistical sampling will not minimize this. Control risk is the risk that a material error exists, which will not be prevented or detected on a timely basis by the system of internal controls. This cannot be minimized using statistical sampling.

62. What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

A. Business risk

B. Detection risk

C. Residual risk

D. Inherent risk

Correct Answer: B. Detection risk

Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

63. The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

A. Inherent

B. Detection

C. Control

D. Business

Correct Answer: B. Detection

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks usually are not affected by the IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by the IS auditor.

64. Which one of the following could an IS auditor use to validate the effectiveness of edit and validation routines?

A. Domain integrity test

B. Relational integrity test

C. Referential integrity test

D. Parity checks

Correct Answer: A. Domain integrity test

Domain integrity testing is aimed at verifying that the data conform to definitions, i.e., the data items are all in the correct domains. The major objective of this exercise is to verify that the edit and validation routines are working satisfactorily. Relational integrity tests are performed at the record level and usually involve calculating and verifying various calculated fields, such as control totals. Referential integrity tests involve ensuring that all references to a primary key from another file actually exist in their original file. A parity check is a bit added to each character prior to transmission. The parity bit is a function of the bits making up the character. The recipient performs the same function on the received character and compares the result to the transmitted parity bit. If it is different, an error is assumed.

65. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.

B. Determine the risks/threats to the data center site.

C. Review business continuity procedures.

D. Test for evidence of physical access at suspect locations.

Correct Answer: B. Determine the risks/threats to the data center site.

During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

66. The PRIMARY purpose of audit trails is to:

A. improve response time for users.

B. establish accountability and responsibility for processed transactions.

C. improve the operational efficiency of the system.

D. provide useful information to auditors who may wish to track transactions.

Correct Answer: B. establish accountability and responsibility for processed transactions.

Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

67. Which of the following would BEST provide assurance of the integrity of new staff?

A. Background screening

B. References

C. Bonding

D. Qualifications listed on a resume

Correct Answer: A. Background screening

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

68. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

A. enterprise data model.

B. IT balanced scorecard (BSC).

C. IT organizational structure.

D. historical financial statements.

Correct Answer: B. IT balanced scorecard (BSC).

A Balanced Scorecard defines what management means by "performance" and measures whether management is achieving desired results. The Balanced Scorecard translates Mission and Vision Statements into a comprehensive set of objectives and performance measures that can be quantified and appraised. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, IS Auditor should review IT Balanced Scorecard.

69. The advantage of a bottom-up approach to the development of organizational policies is that the policies:

A. are developed for the organization as a whole.

B. are more likely to be derived as a result of a risk assessment.

C. will not conflict with overall corporate policy.

D. ensure consistency across the organization.

Correct Answer: B. are more likely to be derived as a result of a risk assessment.

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

70. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer? Each correct answer represents a complete solution. Choose all that apply.

A. Facilitating the sharing of security risk-related information among authorizing officials

B. Preserving high-level communications and working group relationships in an organization

C. Establishing effective continuous monitoring program for the organization

D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

Correct Answer: A. Facilitating the sharing of security risk-related information among authorizing officials

A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization. Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

71. A data administrator is responsible for:

A. maintaining database system software.

B. defining data elements, data names and their relationship.

C. developing physical database structures.

D. developing data dictionary system software.

Correct Answer: B. defining data elements, data names and their relationship.

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

72. Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.

B. define key performance indicators.

C. provide business value to IT projects.

D. control IT expenses.

Correct Answer: B. define key performance indicators.

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

73. A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilities.

B. reporting to the end-user manager.

C. having programming responsibilities.

D. being responsible for LAN security administration.

Correct Answer: C. having programming responsibilities.

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

74. The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.

B. performance of a comprehensive security control review by the IS auditor.

C. adoption of a corporate information security policy statement.

D. purchase of security access control software.

Correct Answer: C. adoption of a corporate information security policy statement.

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

75. Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response

B. Correction

C. Detection

D. Monitoring

Correct Answer: A. Response

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

76. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.

B. a lack of a methodology for systems development.

C. the technology not aligning with the organization's objectives.

D. an absence of control over technology contracts.

Correct Answer: C. the technology not aligning with the organization's objectives.

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

77. When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy

B. Defining the corporate security policy

C. Implementing the corporate security policy

D. Defining security procedures and guidelines

Correct Answer: A. Accountability for the corporate security policy

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

78. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services

B. Participating in systems design with the provider

C. Managing compliance with the contract for the outsourced services

D. Negotiating contractual agreement with the provider

Correct Answer: C. Managing compliance with the contract for the outsourced services

Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

79. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information

B. information security is not critical to all functions.

C. IS audit should provide security training to the employees.

D. the audit finding will cause management to provide continuous training to staff.

Correct Answer: A. this lack of knowledge may lead to unintentional disclosure of sensitive information

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

80. Although BCP and DRP are often implemented and tested by middle management and end users,the ultimate responsibility and accountability for the plans remain with executivemanagement, such as the _____. (fill-in-the-blank)

A. Security administrator

B. Systems auditor

C. Board of directors

D. Financial auditor

Correct Answer: C. Board of directors

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

81. IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedures.

B. best IT security control practices relevant to a specific entity.

C. techniques for securing information.

D. security policy.

Correct Answer: A. desired result or purpose of implementing specific control procedures.

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

82. Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors.

B. Gather performance data.

C. Establish performance baselines.

D. Optimize performance.

Correct Answer: D. Optimize performance.

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability, and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

83. Which of the following would provide a mechanism whereby IS management can determine if the activities of the organization have deviated from the planned or expected levels?

A. Quality management

B. IS assessment methods

C. Management principles

D. Industry standards/benchmarking

Correct Answer: B. IS assessment methods

Assessment methods provide a mechanism, whereby IS management can determine if the activities of the organization have deviated from planned or expected levels. These methods include IS budgets, capacity and growth planning, industry standards/ benchmarking, financial management practices, and goal accomplishment. Quality management is the means by which the IS department processes are controlled, measured and improved. Management principles focus on areas such as people, change, processes and security. Industry standards/benchmarking provide a means of determining the level of performance provided by similar information processing facility environments

84. Which of the following is the MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Correct Answer: A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules are also required along with the user's education on the importance of security.

85. The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.

B. security and control policies support business and IT objectives.

C. there is a published organizational chart with functional descriptions.

D. duties are appropriately segregated.

Correct Answer: B. security and control policies support business and IT objectives.

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

86. Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Correct Answer: A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

87. Which of the following would be a compensating control to mitigate risks resulting from an inadequate segregation of duties?

A. Sequence check

B. Check digit

C. Source documentation retention

D. Batch control reconciliations

Correct Answer: D. Batch control reconciliations

Batch control reconciliations are an example of compensating controls. Other examples of compensating controls are transaction logs, reasonableness tests, independent reviews and audit trails, such as console logs, library logs and job accounting date. Sequence checks and check digits are data validation edits, and source documentation retention is an example of a data file control.

88. Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements

B. Promoting ethical understanding

C. Security awareness programs

D. Effective performance incentives

Correct Answer: C. Security awareness programs

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

89. To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

A. O/S and hardware refresh frequencies

B. Gain-sharing performance bonuses

C. Penalties for noncompliance

D. Charges tied to variable cost metrics

Correct Answer: B. Gain-sharing performance bonuses

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

90. A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recovery.

B. retention.

C. rebuilding.

D. reuse.

Correct Answer: B. retention.

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic "paper" makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves.

Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

91. When are benchmarking partners identified within the benchmarking process?

A. In the design stage

B. In the testing stage

C. In the research stage

D. In the development stage

Correct Answer: C. In the research stage

Benchmarking partners are identified in the research stage of the benchmarking process.

92. In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized

B. Managed

C. Defined

D. Repeatable

Correct Answer: B. Managed

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be "managed and measurable."

93. Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.

B. Data can be amended without authorization.

C. Unauthorized report copies can be printed.

D. Output can be lost in the event of system failure.

Correct Answer: C. Unauthorized report copies can be printed.

Explanation: Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure

94. Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.

B. data will not be deleted before that date.

C. backup copies are not retained after that date.

D. datasets having the same name are differentiated.

Correct Answer: B. data will not be deleted before that date.

Explanation: A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and, therefore, may well be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

95. Which of the following can be used to verify output results and control totals by matching them against the input data and control totals?

A. Batch header forms

B. Batch balancing

C. Data conversion error corrections

D. Access controls over print spools

Correct Answer: B. Batch balancing

Explanation: Batch balancing is used to verify output results and control totals by matching them against the input data and control totals. Batch header forms control data preparation; data conversion error corrections correct errors that occur due to duplication of transactions and inaccurate data entry; and access controls over print spools prevent reports from being accidentally deleted from print spools or directed to a different printer.

96. Which of the following would an IS auditor expect to find in a console log?

A. Names of system users

B. Shift supervisor identification

C. System errors

D. Data edit errors

Correct Answer: C. System errors

Explanation: System errors are the only ones that one would expect to find in the console log.

97. A network diagnostic tool that monitors and records network information is a(n):

A. online monitor.

B. downtime report.

C. help desk report.

D. protocol analyzer.

Correct Answer: B. downtime report.

Explanation: Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

98. Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server

B. Simultaneously duplicating the system log on a write-once disk

C. Write-protecting the directory containing the system log

D. Storing the backup of the system log offsite

Correct Answer: B. Simultaneously duplicating the system log on a write-once disk

Explanation: A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

99. During an audit of the tape management system at a data center, an IS auditor discovered that parameters are set to bypass or ignore the labels written on tape header records. The IS auditor also determined that effective staging and job setup procedures were in place. In this situation, the IS auditor should conclude that the:

A. tape headers should be manually logged and checked by the operators.

B. staging and job setup procedures are not appropriate compensating controls.

C. staging and job setup procedures compensate for the tape label control weakness.

D. tape management system parameters must be set to check all labels.

Correct Answer: C. staging and job setup procedures compensate for the tape label control weakness.

Explanation: Compensating controls are an important part of a control structure. They are considered adequate if they help to achieve the control objective and are cost-effective. In this situation, the IS auditor is most likely to conclude that staging and job setup procedures compensate for the tape label control weakness.

100. IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

B. The service provider does not have incident handling procedures.

C. Recently a corrupted database could not be recovered because of library management problems.

D. Incident logs are not being reviewed.

Correct Answer: A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

Explanation: The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

101. Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location

B. Setting a boot password

C. Hardening the server configuration

D. Implementing activity logging

Correct Answer: C. Hardening the server configuration

Explanation: Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenarioâ€"it is a detective control (not a preventive one) and the attacker who already gained privileged access can modify logs or disable them.

102. An IS auditor detected that several PCs connected to the Internet have a low security level that is allowing for the free recording of cookies. This creates a risk because cookies locally store:

A. information about the Internet site.

B. information about the user.

C. information for the Internet connection.

D. Internet pages.

Correct Answer: B. information about the user.

Explanation: The cookie file resides on the client machine. It contains data passed from web sites, so that web sites can communicate with this file when the same client returns. The web site only has access to that part of the cookie file that represents the interaction with that particular web site. Cookie files have caused some issues with respect to privacy. The four choices all relate to a cookie, but the fact that the cookie stores information about the user is the risk.

103. Which of the following is the MOST probable cause for a mail server being used to send spam?

A. Installing an open relay server

B. Enabling Post Office Protocol (POP3)

C. Using Simple Mail Transfer Protocol (SMTP)

D. Activating user accounting

Correct Answer: A. Installing an open relay server

Explanation: An open relay (or open proxy) allows unauthorized people to route their spam through someone else's mail server. POP3 and SMTP are commonly used mail protocols. Activating user accounting does not relate to using a server to send spam.

104. Which of the following is the MOST probable cause for a mail server being used to send spam?

A. Installing an open relay server

B. Enabling Post Office Protocol (POP3)

C. Using Simple Mail Transfer Protocol (SMTP)

D. Activating user accounting

Correct Answer: A. Installing an open relay server

Explanation: An open relay (or open proxy) allows unauthorized people to route their spam through someone else's mail server. POP3 and SMTP are commonly used mail protocols. Activating user accounting does not relate to using a server to send spam.

105. The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

A. contents are highly volatile.

B. data cannot be backed up.

C. data can be copied.

D. device may not be compatible with other peripherals.

Correct Answer: C. data can be copied.

Explanation: Unless properly controlled, flash memory provides an avenue anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

106. The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.

B. increased redundancy.

C. unauthorized accesses.

D. application malfunctions.

Correct Answer: B. increased redundancy.

Explanation: Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy (Redundancy which is usually considered positive when it is a question of resource

availability is negative in a database environment, since it demands additional, otherwise unnecessary, data handling efforts.) Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

107. Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and non business materials.

B. maximize employee performance.

C. safeguard the organization's image.

D. assist the organization in preventing legal issues

Correct Answer: A. protect the organization from viruses and nonbusiness materials.

Explanation: The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved); however, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

108. Which of the following is the GREATEST risk related to the monitoring of audit logs?

A. Logs are not backed up periodically.

B. Routine events are recorded.

C. Procedures for enabling logs are not documented.

D. Unauthorized system actions are recorded but not investigated.

Correct Answer: D. Unauthorized system actions are recorded but not investigated.

Explanation: If unauthorized system actions are not investigated, the log is useless. Not backing up logs periodically is a risk, but not as critical as the need to investigate questionable actions. Recording routine events can make it more difficult to recognize unauthorized actions, but the critical events are still recorded. Procedures for enabling and reviewing logs should be documented, but documentation does not ensure investigation.

109. An organization wants to enforce data integrity principles and achieve faster performance/execution in a database application. Which of the following design principles should be applied?

A. User (customized) triggers

B. Data validation at the front end

C. Data validation at the back end

D. Referential integrity

Correct Answer: D. Referential integrity

Explanation: Referential integrity should be implemented at the time of the design of the database to provide a faster execution mechanism. All other options are implemented at the application coding stage.

110. To share data in a multivendor network environment, it is essential to implement program-to-program communication. With respect to program-to-program communication features, that can be implemented in this environment, which of the following makes implementation and maintenance difficult?

A. User isolation

B. Controlled remote access

C. Transparent remote access

D. The network environments

Correct Answer: D. The network environments

Explanation: Depending on the complexity of the network environment, implementation of program-to-program communication features becomes progressively more difficult. It is possible to implement program-to-program communication to isolate a user in the multivendor network. Program-to-program communication can be implemented to control and monitor the files that a user can transfer between systems, and the remote program-to-program communication will be transparent to the end user. All of these are security features.

111. An IS auditor is reviewing the database administration (DBA) function to ascertain whether adequate provision has been made for controlling data. The IS auditor should determine that the:

A. function reports to data processing operations.

B. responsibilities of the function are well defined.

C. database administrator is a competent systems programmer.

D. audit software has the capability of efficiently accessing the database.

Correct Answer: B. responsibilities of the function are well defined.

Explanation: The IS auditor should determine that the responsibilities of the DBA

function are not only well defined but also assure that the DBA reports directly to the IS manager or executive to provide independence, authority and responsibility. The DBA should not report to either data processing operations or systems development management. The DBA need not be a competent systems programmer. Choice D is not as important as choice A.

112. Which of the following is a control over database administration activities?

A. A database checkpoint to restart processing after a system failure

B. Database compression to reduce unused space

C. Supervisory review of access logs

D. Backup and recovery procedures to ensure database availability

Correct Answer: C. Supervisory review of access logs

Explanation: To ensure management approval of database administration activities and to exercise control over the use of database tools, there should be a supervisory review of access logs. Database administration activities include among others, database checkpoints, database compression techniques, and data backup and recovery procedures established and implemented to ensure database availability.

113. To maximize the performance of a large database in a parallel processing environment, which of the following is used for separating indexes?

A. Disk partitioning

B. Mirroring

C. Hashing

D. Duplexing

Correct Answer: C. Hashing

Explanation: An essential part of designing a database for parallel processing is the partitioning scheme. Because large databases are indexed, independent indexes must also be partitioned to maximize performance. Hashing is a method used for index partitioning. It associates data to disks based on a hash key. Disk partitioning creates logical drives on the single disk for better management of the contents. Disk mirroring uses two identical disks. All operations on the two disks are performed so that each disk is a mirror image of the other. This provides redundancy in case of failure of one of the disks. Disk duplexing makes use of more than one disk with two separate controllers providing redundancy in case of a disk failure or a controller card failure.

114. Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity

B. Domain integrity

C. Relational integrity

D. Referential integrity

Correct Answer: D. Referential integrity

Explanation: Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables. If this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

115. The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.

B. prevent integrity problems, when two processes attempt to update the same data at the same time.

C. prevent inadvertent or unauthorized disclosure of data in the database.

D. ensure the accuracy, completeness and consistency of data.

Correct Answer: B. prevent integrity problems, when two processes attempt to update the same data at the same time.

Explanation: Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users and controls, such as passwords, prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

116. A referential integrity constraint consists of:

A. ensuring the integrity of transaction processing.

B. ensuring that data are updated through triggers.

C. ensuring controlled user updates to the database.

D. rules for designing tables and queries.

Correct Answer: B. ensuring that data are updated through triggers.

Explanation: Referential integrity constraints ensure that a change in a primary key of one table is automatically updated in the matching foreign keys of other tables. This is done using triggers.

117. Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures

B. Table link/reference checks

C. Query/table access time checks

D. Rollback and roll forward database features

Correct Answer: B. Table link/reference checks

Explanation: Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database) and thus provides the greatest assurance of database integrity. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

118. The database administrator has decided to disable certain normalization controls in the database management system (DBMS) software to provide users with increased query performance. This will MOST likely increase the risk of:

A. loss of audit trails.

B. redundancy of data.

C. loss of data integrity.

D. unauthorized access to data.

Correct Answer: B. redundancy of data.

Explanation: Normalization is the removal of redundant data elements from the database structure. Disabling features of normalization in relational databases will increase the likelihood of data redundancy. Audit trails are a feature of DBMS software that can be lost by not enabling them. These are not connected to normalization controls. The integrity of data is not directly affected by disabling normalization controls. Access to data is set through defining user rights and controlling access to information, and is not affected by normalization controls.

119. In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries

B. Additional staff to provide separation of duties

C. Procedures that verify that only approved program changes are implemented

D. Access controls to prevent the operator from making program modifications

Correct Answer: C. Procedures that verify that only approved program changes are implemented

Explanation: While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited, as suggested in choice B, this practice is not always possible in small organizations. The IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

120. Vendors have released patches fixing security flaws in their software. Which of the following should the IS auditor recommend in this situation?

A. Assess the impact of patches prior to installation.

B. Ask the vendors for a new software version with all fixes included.

C. Install the security patch immediately.

D. Decline to deal with these vendors in the future.

Correct Answer: A. Assess the impact of patches prior to installation.

Explanation: The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions with all fixes included are not always available and a full installation could be time-consuming. Declining to deal with vendors does not take care of the flaw.

121. A programmer, using firecall IDs, as provided in the manufacture's manual, gained access to the production environment and made an unauthorized change. Which of the following could have prevented this from happening?

A. Deactivation

B. Monitoring

C. Authorization

D. Resetting

Correct Answer: D. Resetting

Explanation: The vendor supplied firecall IDs should be reset at the time of implementing the system and new IDs generated. Deactivation may cause the disruption of a critical production job. Without resetting the vendor provided firecall IDs, monitoring and authorization of such IDs are not effective controls.

122. One of the purposes of library control software is to allow:

A. programmers access to production source and object libraries.

B. batch program updating.

C. operators to update the control library with the production version before testing is completed.

D. read-only access to source code.

Correct Answer: D. read-only access to source code.

Explanation: An important purpose of library control software is to allow read-only access to source code. Choices A, B and C are activities which library control software should help to prevent or prohibit.

123. An organization is moving its application maintenance in-house from an outside source. Which of the following should be the main concern of an IS auditor?

A. Regression testing

B. Job scheduling

C. User manuals

D. Change control procedures

Correct Answer: D. Change control procedures

Explanation: It is essential for the maintenance and control of software that change control procedures be in place. Regression testing is completed after changes are made to the software, and since the software is already being used, the job schedule must be in place and may be reviewed later. This change does not affect user manuals and any associated risks.

124. Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports

B. Library control software restricting changes to source code

C. Restricted access to source code and object code

D. Date and time-stamp reviews of source and object code

Correct Answer: D. Date and time-stamp reviews of source and object code

Explanation: Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

125. An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.

B. Make changes to the database after granting access to a normal user account

C. Use the DBA user account to make changes, log the changes and review the change log the following day.

D. Use the normal user account to make changes, log the changes and review the change log the following day.

Correct Answer: C. Use the DBA user account to make changes, log the changes and review the change log the following day.

Explanation: The use of a database administrator (DBA) user account is (should be) normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

126. Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

A. Review software migration records and verify approvals.

B. Identify changes that have occurred and verify approvals.

C. Review change control documentation and verify approvals.

D. Ensure that only appropriate staff can migrate changes into production.

Correct Answer: B. Identify changes that have occurred and verify approvals.

Explanation: The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

127. After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

A. Differential reporting

B. False-positive reporting

C. False-negative reporting

D. Less-detail reporting

Correct Answer: C. False-negative reporting

Explanation: False-negative reporting on weaknesses means the control weaknesses in the network are not identified and, hence, may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

128. The FIRST step in managing the risk of a cyberattack is to:

A. assess the vulnerability impact.

B. evaluate the likelihood of threats.

C. identify critical information assets.

D. estimate potential damage.

Correct Answer: C. identify critical information assets.

Explanation: The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

129. Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits a vulnerability in a protocol?

A. Install the vendor's security fix for the vulnerability.

B. Block the protocol traffic in the perimeter firewall.

C. Block the protocol traffic between internal network segments.

D. Stop the service until an appropriate security fix is installed.

Correct Answer: D. Stop the service until an appropriate security fix is installed.

Explanation: Stopping the service and installing the security fix is the safest way to prevent the worm from spreading. If the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits every software that utilizes it from working between segments

130. Which of the following is the BEST control to detect internal attacks on IT resources?

A. Checking of activity logs

B. Reviewing firewall logs

C. Implementing a security policy

D. Implementing appropriate segregation of duties

Correct Answer: A. Checking of activity logs

Explanation: Verification of individual activity logs will detect the misuse of IT resources. Depending on the configuration, firewall logs can help in detecting attacks passing through the firewall. Implementation of a security policy and segregation of duties are deterrent controls that might prevent the misuse of IT resources.

131. A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

A. Most employees use laptops.

B. A packet filtering firewall is used.

C. The IP address space is smaller than the number of PCs.

D. Access to a network port is not restricted.

Correct Answer: D. Access to a network port is not restricted.

Explanation: Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

132. An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned, if a hacker:

A. compromises the Wireless Application Protocol (WAP) gateway.

B. installs a sniffing program in front of the server.

C. steals a customer's PDA.

D. listens to the wireless transmission.

Correct Answer: A. compromises the Wireless Application Protocol (WAP) gateway.

Explanation: In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

133. Analysis of which of the following would MOST likely enable the IS auditor to determine if an unapproved program attempted to access sensitive data?

A. Abnormal job termination reports

B. Operator problem reports

C. System logs

D. Operator work schedules

Correct Answer: C. System logs

Explanation: System logs are automated reports that identify most of the activities performed on the computer. Many programs that analyze the system log to report on specifically defined items have been developed. Abnormal job termination reports identify application jobs that were terminated before successful completion. Operator problem reports are used by operators to log computer operations problems and their solutions. Operator work schedules are maintained by IS management to assist in human resource planning.

134. A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies

B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing

C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format

D. Reengineering the existing processing and redesigning the existing system

Correct Answer: C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format

Explanation: EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls) EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

135. A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

A. Unit testing

B. Integration testing

C. Design walk-throughs

D. Configuration management

Correct Answer: B. Integration testing

Explanation: A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight); units are tested by the programmer and then transferred to the acceptance test area; this often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

136. A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

A. Comparing source code

B. Reviewing system log files

C. Comparing object code

D. Reviewing executable and source code integrity

Correct Answer: B. Reviewing system log files

Explanation: Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

137. An employee is responsible for updating daily the interest rates in a finance application, including interest rate exceptions for preferred customers. Which of the following is the BEST control to ensure that all rate exceptions are approved?

A. A supervisor must enter his/her password before a rate exception is validated.

B. Rates outside the normal range require prior management approval.

C. The system beeps an alarm when rate exceptions are entered.

D. All interest rates must be logged and verified every 30 days.

Correct Answer: B. Rates outside the normal range require prior management approval.

Explanation: Prior approval of management for rates outside the normal range would be a proper control. Entering the password of a supervisor does not ensure authorization. A system alarm upon entry of a rate exception is only a warning. Logging of exceptions is a detective control.

138. An IS auditor is conducting a review of an application system after users have completed acceptance testing. What should be the IS auditorâ€™s major concern?

A. Determining whether test objectives were documented

B. Assessing whether users documented expected test results

C. Reviewing whether test problem logs were completed

D. Determining if there are unresolved issues

Correct Answer: D. Determining if there are unresolved issues

Explanation: In assessing the overall success or failure of the acceptance test, the IS auditor should determine whether the test plans were documented and whether actual

results were compared with expected results as well as review the test problem log to confirm resolution of identified test issues. The IS auditor should then determine the impact of the unresolved issues on system functionality and usability.

139. By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

A. reliable products are guaranteed.

B. programmers' efficiency is improved.

C. security requirements are designed.

D. predictable software processes are followed.

Correct Answer: D. predictable software processes are followed.

Explanation: By evaluating the organization's development projects against the CMM, the IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

140. Ideally, stress testing should be carried out in a:

A. test environment using test data.

B. production environment using live workloads.

C. test environment using live workloads.

D. production environment using test data.

Correct Answer: C. test environment using live workloads.

Explanation: Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

141. In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handler.

B. EDI translator.

C. application interface.

D. EDI interface.

Correct Answer: A. communications handler.

Explanation: A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs). An EDI translator translates data between the standard format and a trading partner's proprietary format. An application interface moves electronic transactions to or from the application system and performs data mapping. An EDI interface manipulates and routes data between the application system and the communications handler.

142. In an electronic fund transfer (EFT) system, which of the following controls would be useful in detecting a duplication of messages?

A. Message authentication code

B. Digital signature

C. Authorization sequence number

D. Segregation of authorization

Correct Answer: C. Authorization sequence number

Explanation: All of these controls are necessary in an EFT system; however, the authorization sequence number is the control that will detect the duplication of a message. A message authentication code detects unauthorized modifications, a digital signature ensures non-repudiation, and the segregation of the creation of the message and the authorization will avoid dummy messages.

143. Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.

B. transaction journal.

C. automated suspense file listing.

D. user error report.

Correct Answer: B. transaction journal.

Explanation: The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, and the user error report would only list input that resulted in an edit error.

144. Peer reviews to detect software errors during a program development activity are called:

A. emulation techniques.

B. structured walk-throughs.

C. modular program techniques.

D. top-down program construction.

Correct Answer: B. structured walk-throughs.

Explanation: A structured walk-through is a management tool for improving productivity. Structured walk-throughs can detect an incorrect or improper interpretation of the program specifications. This, in turn, improves the quality of system testing and acceptance of it. The other choices are methods or tools in the overall systems development process.

145. The MAJOR concern for an IS auditor reviewing a CASE environment should be that the use of CASE does not automatically:

A. result in a correct capture of requirements.

B. ensure that desirable application controls have been implemented.

C. produce ergonomic and user-friendly interfaces.

D. generate efficient code.

Correct Answer: A. result in a correct capture of requirements.

Explanation: The principal concern should be to ensure an alignment of the application with business needs and user requirements. While the CASE being used may provide tools to cover this crucial initial phase, a cooperative user-analyst interaction is always needed. Choice B should be the next concern. If the system meets business needs and user requirements, it should also incorporate all desirable controls. Controls have to be specified since CASE can only automatically incorporate certain, rather low-level, controls (such as type of input data, e.g., date, expected). CASE will not (choice C) automatically generate ergonomic and user-friendly interfaces, but it should provide tools for easy (and automatically documented) tuning. CASE applications (choice D) generally come short of optimizing the use of hardware and software resources, precisely because they are designed to optimize other elements, such as developers' effort or documentation.

146. The request for proposal (RFP) for the acquisition of an application system would MOST likely be approved by the:

A. project steering committee.

B. project sponsor.

C. project manager.

D. user project team.

Correct Answer: A. project steering committee.

Explanation: A project steering committee usually consists of a senior representative from each function that will be affected by the new system and would be the most appropriate group to approve the RFP. The project sponsor provides funding for the project. The project manager and user project team are responsible for drafting the RFP.

147. The use of a GANTT chart can:

A. aid in scheduling project tasks.

B. determine project checkpoints.

C. ensure documentation standards.

D. direct the post-implementation review.

Correct Answer: A. aid in scheduling project tasks.

Explanation: A GANTT chart is used in project control. It may aid in the identification of needed checkpoints, but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

148. Which of the following is a characteristic of timebox management? It:

A. is not suitable for prototyping or rapid application development (RAD).

B. eliminates the need for a quality process.

C. prevents cost overruns and delivery delays.

D. separates system and user acceptance testing.

Correct Answer: C. prevents cost overruns and delivery delays.

Explanation: Time box management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

149. Which of the following is an implementation risk within the process of decision support systems?

A. Management control

B. Semi-structured dimensions

C. Inability to specify purpose and usage patterns

D. Changes in decision processes

Correct Answer: C. Inability to specify purpose and usage patterns

Explanation: The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

150. Which of the following is the FIRST step in a business process reengineering (BPR) project?

A. Defining the areas to be reviewed

B. Developing a project plan

C. Understanding the process under review

D. Reengineering and streamlining the process under review

Correct Answer: A. Defining the areas to be reviewed

Explanation: On the basis of the evaluation of the entire business process, correctly defining the areas to be reviewed is the first step in a BPR project. On the basis of the definition of the areas to be reviewed, the project plan is developed. Understanding the process under review is important, but the subject of the review must be defined first. Thereafter, the process can be reengineered, streamlined, implemented and monitored for continuous improvement.

151. Which of the following is used to ensure that batch data is completely and accurately transferred between two systems?

A. Control total

B. Check digit

C. Check sum

D. Control account

Correct Answer: A. Control total

Explanation: A control total is frequently used as an easily recalculated control. The number of invoices in a batch or the value of invoices in a batch are examples of control totals. They provide a simple way of following an audit trail from a general ledger summary item to an individual transaction, and back. A check digit is a method of verifying the accuracy of a single data item, such as a credit card number. Although a check sum is an excellent control over batch completeness and accuracy, it is not easily recalculated and, therefore, is not as commonly used in financial systems as a control total. Check sums are frequently used in data transfer as part of encryption protocols. Control accounts are used in financial systems to ensure that components that exchange summary information, such as a sales register and a general ledger, can be reconciled.

152. Which of the following should be included in a feasibility study for a project to implement an EDI process?

A. The encryption algorithm format

B. The detailed internal control procedures

C. The necessary communication protocols

D. The proposed trusted third-party agreement

Correct Answer: C. The necessary communication protocols

Explanation: Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may be significant cost implications, if new hardware and software are involved, and risk implications, if the technology is new to the organization.

153. A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house-developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.

B. A quality plan is not part of the contracted deliverables.

C. Not all business functions will be available on initial implementation.

D. Prototyping is being used to confirm that the system meets business requirements.

Correct Answer: B. A quality plan is not part of the contracted deliverables.

Explanation: A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

154. A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders

B. Logging all customer orders in the ERP system

C. Using hash totals in the order transmitting process

D. Approving (production supervisor) orders prior to production

Correct Answer: A. Verifying production to customer orders

Explanation: Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time-consuming, manual process that does not guarantee proper control.

155. A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification

B. One-for-one checking

C. Manual recalculations

D. Functional acknowledgements

Correct Answer: D. Functional acknowledgements

Explanation: Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

156. A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be the IS auditor's main concern about the new process?

A. Are key controls in place to protect assets and information resources?

B. Does it address the corporate customer requirements?

C. Does the system meet the performance goals (time and resources)?

D. Have owners been identified who will be responsible for the process?

Correct Answer: A. Are key controls in place to protect assets and information resources?

Explanation: The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D

are objectives that the BPR process should achieve, but they are not the auditor's primary concern.

157. A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

A. payroll reports should be compared to input forms.

B. gross payroll should be recalculated manually.

C. checks (cheques) should be compared to input forms.

D. checks (cheques) should be reconciled with output reports.

Correct Answer: A. payroll reports should be compared to input forms.

Explanation: The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

158. A data validation edit that matches input data to an occurrence rate is a:

A. limit check.

B. reasonableness check.

C. range check.

D. validity check.

Correct Answer: B. reasonableness check.

Explanation: A reasonableness check is an edit check, wherein input data are matched to predetermined reasonable limits or occurrence rates. Limit checks verify that data do not exceed a predetermined amount. Range checks verify that data are within a predetermined range of values. Validity checks test for data validity in accordance with predetermined criteria.

159. A data warehouse is:

A. object-oriented.

B. subject-oriented.

C. departmental specific.

D. a volatile database

Correct Answer: B. subject-oriented.

Explanation: Data warehouses are subject-oriented. The data warehouse is meant to help make decisions when the function(s) to be affected by the decision transgresses across departments within an organization. They are nonvolatile. Object orientation and volatility are irrelevant to a data warehouse system.

160. A debugging tool, which reports on the sequence of steps executed by a program, is called a(n):

A. output analyzer.

B. memory dump.

C. compiler.

D. logic path monitor.

Correct Answer: D. logic path monitor.

Explanation: Logic path monitors report on the sequence of steps executed by a program. This provides the programmer with clues to logic errors, if any, in the program. An output analyzer checks the results of a program for accuracy by comparing the expected results with the actual results. A memory dump provides a picture of the content of a computer's internal memory at any point in time, often when the program is aborted, thus providing information on inconsistencies in data or parameter values. Though compilers have some potential to provide feedback to a programmer, they are not generally considered a debugging tool.

161. A decision support system (DSS):

A. is aimed at solving highly structured problems.

B. combines the use of models with nontraditional data access and retrieval functions.

C. emphasizes flexibility in the decision-making approach of users.

D. supports only structured decision-making tasks.

Correct Answer: C. emphasizes flexibility in the decision-making approach of users.

Explanation: DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less-structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi-structured decision-making tasks.

162. Which of the following is a check (control) for completeness?

A. Check digits

B. Parity bits

C. One-for-one checking

D. Prerecorded input

Correct Answer: B. Parity bits

Explanation: Parity bits are used to check for completeness of data transmissions. Choice A is incorrect because check digits are a control check for accuracy. Choice C is incorrect because, in one-for-one checking, individual documents are matched to a detailed listing of documents processed by the computer, but do not ensure that all documents have been received for processing. Choice D (prerecorded input) is a data file control for which selected information fields are preprinted on blank input forms to reduce the chance of input errors.

163. Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit

B. Existence check

C. Completeness check

D. Reasonableness check

Correct Answer: C. Completeness check

Explanation: A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

164. Which of the following types of controls is designed to provide the ability to verify data and record values through the stages of application processing?

A. Range checks

B. Run-to-run totals

C. Limit checks on calculated amounts

D. Exception reports

Correct Answer: B. Run-to-run totals

Explanation: Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer were accepted and then applied to the updating process.

165. The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.

B. central processing site during the running of the application system.

C. remote processing site after transmission of the data to the central processing site.

D. remote processing site prior to transmission of the data to the central processing site.

Correct Answer: D. remote processing site prior to transmission of the data to the central processing site.

Explanation: It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

166. To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparation.

B. in transit to the computer.

C. between related computer runs.

D. during the return of the data to the user department.

Correct Answer: A. during data preparation.

Explanation: During data preparation is the best answer, because it establishes control at the earliest point.

167. Functional acknowledgements are used:

A. as an audit trail for EDI transactions.

B. to functionally describe the IS department.

C. to document user roles and responsibilities.

D. as a functional description of application software.

Correct Answer: A. as an audit trail for EDI transactions.

Explanation: Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of

functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

168. The impact of EDI on internal controls will be:

A. that fewer opportunities for review and authorization will exist.

B. an inherent authentication.

C. a proper distribution of EDI transactions while in the possession of third parties.

D. that IPF management will have increased responsibilities over data center controls.

Correct Answer: A. that fewer opportunities for review and authorization will exist.

Explanation: EDI promotes a more efficient paperless environment, but at the same time, less human intervention makes it more difficult for reviewing and authorizing. Choice B is incorrect; since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and does not include any distinguishing human element or signature. Choice C is incorrect because this is a security risk associated with EDI. Choice D is incorrect because there are relatively few, if any, additional data center controls associated with the implementation of EDI applications. Instead, more control will need to be exercised by the user's application system to replace manual controls, such as site reviews of documents. More emphasis will need to be placed on control over data transmission (network management controls).

169. Sales orders are automatically numbered sequentially at each of a retailer's multiple outlets. Small orders are processed directly at the outlets, with large orders sent to a central production facility. The MOST appropriate control to ensure that all orders transmitted to production are received and processed would be to:

A. send and reconcile transaction counts and totals.

B. have data transmitted back to the local site for comparison.

C. compare data communications protocols with parity checking.

D. track and account for the numerical sequence of sales orders at the production facility.

Correct Answer: A. send and reconcile transaction counts and totals.

Explanation: Sending and reconciling transaction totals not only ensure that the orders were received, but also processed by the central production location. Transmission

back to the local site confirms that the central location received it, but not that they have actually processed it. Tracking and accounting for the numerical sequence only confirms what orders are on hand, and not whether they actually have been completed. The use of parity checking would only confirm that the order was not changed during transmission.

170. Which of the following ensures completeness and accuracy of accumulated data?

A. Processing control procedures

B. Data file control procedures

C. Output controls

D. Application controls

Correct Answer: A. Processing control procedures

Explanation: Processing controls ensure the completeness and accuracy of accumulated data, for example, editing and run-to-run totals. Data file control procedures ensure that only authorized processing occurs to stored data, for example, transaction logs. Output controls ensure that data delivered to users will be presented, formatted and delivered in a consistent and secure manner, for example, using report distribution. "Application controls" is a general term comprising all kinds of controls used in an application.

171. A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness check.

B. parity check.

C. redundancy check.

D. check digits.

Correct Answer: C. redundancy check.

Explanation: A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

172. Which of the following integrity tests examines the accuracy, completeness, consistency and authorization of data?

A. Data

B. Relational

C. Domain

D. Referential

Correct Answer: A. Data

Explanation: Data integrity testing examines the accuracy, completeness, consistency and authorization of data. Relational integrity testing detects modification to sensitive data by the use of control totals. Domain integrity testing verifies that data conforms to specifications. Referential integrity testing ensures that data exists in its parent or original file before it exists in the child or another file.

173. Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check

B. Check digit

C. Validity check

D. Duplicate check

Correct Answer: B. Check digit

Explanation: A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered, e.g., an incorrect, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

174. Which of the following data validation edits could be used by a bank, to ensure the correctness of bank account numbers assigned to customers, thereby helping to avoid transposition and transcription errors?

A. Sequence check

B. Validity check

C. Check digit

D. Existence check

Correct Answer: C. Check digit

Explanation: A check digit is a mathematically calculated value that is added to data to ensure that the original data have not been altered. This helps in avoiding transposition

and transcription errors. Thus, a check digit can be added to an account number to check for accuracy. Sequence checks ensure that a number follows sequentially and any out of sequence or duplicate control numbers are rejected or noted on an exception report. Validity checks and existence checks match data against predetermined criteria to ensure accuracy.

175. During an application audit, the IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. Implement data backup and recovery procedures.

B. Define standards and closely monitor for compliance.

C. Ensure that only authorized personnel can update the database.

D. Establish controls to handle concurrent access problems.

Correct Answer: A. Implement data backup and recovery procedures.

Explanation: Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, and monitoring for compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is a preventive control.

176. An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.

B. Implement before-and-after image reporting.

C. Use tracing and tagging.

D. Implement integrity constraints in the database.

Correct Answer: D. Implement integrity constraints in the database.

Explanation: Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

177. When assessing the portability of a database application, the IS auditor should verify that:

A. a structured query language (SQL) is used.

B. information import and export procedures exist with other systems.

C. indexes are used.

D. all entities have a significant name and identified primary and foreign keys.

Correct Answer: A. a structured query language (SQL) is used.

Explanation: The use of an SQL is a key element for database portability. Import and export of information with other systems is an objective of a database interfaces review. The use of an index is an objective of a database access review, and the fact that all entities have a significant name and identified primary and foreign keys is an objective of a database design review.

178. In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.

B. consistency.

C. atomicity.

D. durability.

Correct Answer: C. atomicity.

Explanation: The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions, and hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

179. Which of the following would help to ensure the portability of an application connected to a database? The:

A. verification of database import and export procedures.

B. usage of a structured query language (SQL).

C. analysis of stored procedures/triggers.

D. synchronization of the entity-relation model with the database physical schema.

Correct Answer: B. usage of a structured query language (SQL).

Explanation: The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

180. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

A. Encrypting the hash of the payment instruction with the public key of the financial institution

B. Affixing a time stamp to the instruction and using it to check for duplicate payments

C. Encrypting the hash of the payment instruction with the private key of the instructor

D. Affixing a time stamp to the hash of the instruction before having it digitally signed by the instructor

Correct Answer: B. Affixing a time stamp to the instruction and using it to check for duplicate payments

Explanation: Affixing a time stamp to the instruction and using it to check for duplicate payments makes the instruction unique. The financial institution can check that the instruction was not intercepted and replayed, and thus, it could prevent crediting the account three times. Encrypting the hash of the payment instruction with the public key of the financial institution does not protect replay, it only protects confidentiality and integrity of the instruction. Encrypting the hash of the payment instruction with the private key of the instructor ensures integrity of the instruction and nonrepudiation of the issued instruction. The process of creating a message digest requires applying a cryptographic hashing algorithm to the entire message. The receiver, upon decrypting the message digest, will recompute the hash using the same hashing algorithm and compare the result with what was sent. Hence, affixing a time stamp into the hash of the instruction before being digitally signed by the instructor would violate the integrity requirements of a digital signature.

181. An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

A. Analyze the need for the structural change.

B. Recommend restoration to the originally designed structure.

C. Recommend the implementation of a change control process.

D. Determine if the modifications were properly approved.

Correct Answer: D. Determine if the modifications were properly approved.

Explanation: The IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the auditor find that the structural modification had not been approved.

182. An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

A. Consistency

B. Isolation

C. Durability

D. Atomicity

Correct Answer: D. Atomicity

Explanation: Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends. Isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

183. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

Correct Answer: C. preparing simulated transactions for processing and comparing the results to predetermined results.

Explanation: Preparing simulated transactions for processing and comparing the results to pre determined results is the best method for proving accuracy of a tax calculation.

Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

184. An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized software.

B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.

C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.

D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Correct Answer: C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.

Explanation: The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. The IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

185. Which of the following is the GREATEST challenge in using test data?

A. Ensuring the program version tested is the same as the production program

B. Creating test data that covers all possible valid and invalid conditions

C. Minimizing the impact of additional transactions on the application being tested

D. Processing the test data under an auditor's supervision

Correct Answer: B. Creating test data that covers all possible valid and invalid conditions

Explanation: The effectiveness of test data is determined by the comprehensiveness of the coverage of all the key controls to be tested. If the test data does not cover all valid and invalid conditions, there is a risk that relevant control weakness may remain undetected. Changes in the program, for the period covered under audit, may have been done to remove bugs or for additional functionalities. However, as the test data approach involves testing of data for the audit period, changes in the program tested may have minimal impact. Applications with current technology are usually not impacted

by additional transactions. Test data are developed by the auditor; however, processing does not have to be under an auditor's supervision, since the input data will be verified by the outputs.

186. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs.

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

Correct Answer: C. preparing simulated transactions for processing and comparing the results to predetermined results.

Explanation: Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

187. Which of the following would BEST support 24/7 availability?

A. Daily backup

B. Offsite storage

C. Mirroring

D. Periodic testing

Correct Answer: C. Mirroring

Explanation: Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

188. The PRIMARY purpose of implementing Redundent Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.

B. provide user authentication.

C. ensure availability of data.

D. ensure the confidentiality of data.

Correct Answer: C. ensure availability of data.

Explanation: RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk. If disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

189. Which of the following is the MOST important criterion for the selection of a loation for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.

B. given the same level of protection as that of the computer data center.

C. outsourced to a reliable third party.

D. equipped with surveillance capabilities.

Correct Answer: A. physically separated from the data center and not subject to the same risks.

Explanation: It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

190. If a database is restored using before-image dumps, where should the process be started following an interruption?

A. Before the last transaction

B. After the last transaction

C. As the first transaction after the latest checkpoint

D. As the last transaction before the latest checkpoint

Correct Answer: A. Before the last transaction

Explanation: If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

191. In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

A. Maintaining system software parameters

B. Ensuring periodic dumps of transaction logs

C. Ensuring grandfather-father-son file backups

D. Maintaining important data at an offsite location

Correct Answer: B. Ensuring periodic dumps of transaction logs

Explanation: Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

192. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

A. The previous day's backup file and the current transaction tape

B. The previous day's transaction file and the current transaction tape

C. The current transaction tape and the current hard copy transaction log

D. The current hard copy transaction log and the previous day's transaction file

Correct Answer: A. The previous day's backup file and the current transaction tape

Explanation: The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

193. An offsite information processing facility:

A. should have the same amount of physical access restrictions as the primary processing site.

B. should be easily identified from the outside so that, in the event of an emergency, it can be easily found.

C. should be located in proximity to the originating site, so it can quickly be made operational.

D. need not have the same level of environmental monitoring as the originating site.

Correct Answer: A. should have the same amount of physical access restrictions as the primary processing site.

Explanation: An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site, and the offsite facility should possess the same level of environmental monitoring and control as the originating site.

194. An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.

B. regular hardware maintenance is performed.

C. offsite storage of transaction and master files exists.

D. backup processing facilities are fully tested.

Correct Answer: C. offsite storage of transaction and master files exists.

Explanation: Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

195. Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

A. Reviewing program code

B. Reviewing operations documentation

C. Turning off the UPS, then the power

D. Reviewing program documentation

Correct Answer: B. Reviewing operations documentation

Explanation: Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

196. A company performs full backup of data and programs on a regular basis. The primary purpose of this practice is to:

A. maintain data integrity in the applications.

B. restore application processing after a disruption.

C. prevent unauthorized changes to programs and data.

D. ensure recovery of data processing in case of a disaster.

Correct Answer: B. restore application processing after a disruption.

Explanation: Backup procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Backup procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures are a necessary part of the recovery process following a disaster, they are not sufficient in themselves.

197. Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.

B. Paper documents are also stored in the offsite vault.

C. Data files that are stored in the vault are synchronized.

D. The offsite vault is located in a separate facility.

Correct Answer: C. Data files that are stored in the vault are synchronized.

Explanation: Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because the IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

198. Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.

B. validation checks.

C. input controls.

D. database commits and rollbacks.

Correct Answer: D. database commits and rollbacks.

Explanation: Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

199. When developing a backup strategy, the FIRST step is to:

A. identify the data.

B. select the storage location.

C. specify the storage media.

D. define the retention period.

Correct Answer: A. identify the data.

Explanation: Archiving data and backups is essential for the continuity of business. Selection of the data to be backed up is the first step in the process. Once the data have been identified, an appropriate retention period, storage media and location can be selected.

200. To provide protection for media backup stored at an offsite location, the storage site should be:

A. located on a different floor of the building.

B. easily accessible by everyone.

C. clearly labeled for emergency access.

D. protected from unauthorized access.

Correct Answer: D. protected from unauthorized access.

Explanation: The offsite storage site should always be protected against unauthorized accesses and at least have the same security requirements as the primary site. Choice A is incorrect because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choice B and C represent access risks.

Mock Assessment Test Paper 6

1. An organization is reviewing its contract with a cloud computing provider. For which of the following reasons would the organization want to remove a lock-in clause from the contract?

   A. Availability

   B. Portability

   C. Agility

   D. Scalability

   Answer: B

   Explanation: When drawing up a contract with a cloud service provider, the ideal practice is to remove the customer lock-in clause. It may be important for the client to secure portability of their system assets, i.e., the right to transfer from one vendor to another.

2. The _____ model represents transactions between end users facilitated by a third party.

   A. B2B

   B. B2C

   C. B2E

   D. C2C

   Answer: D

3. A computer manufacturing company selling computers directly to customers is known as_____.

   A. C2C

   B. B2C

   C. C2B

   D. B2B

   Answer: B

4. _____ is a form of electronic commerce that focuses on handling activities that take place within an organization.

   A. B2C

   B. C2C

C. B2B

D. B2E

Answer: D

5. In a LAN environment, which of the following minimizes the risk of data corruption during transmission?

A. Using end-to-end encryption for data communication

B. Using separate conduits for electrical and data cables

C. Using check sums for checking the corruption of data

D. Connecting the terminals using a star topology

Answer: B

Explanation: Using separate conduits for data cables and electrical cables, minimizes the risk of data corruption due to an induced magnetic field created by electrical current. Data encryption minimizes the risk of data leakage in case of wiretapping; however, it cannot prevent corruption. A check sum will help detect the data corruption during communication, but will not prevent it. Using a star topology will increase the speed of communication, but will not detect the corruption.

6. Which of the following is an operating system access control function?

A. Logging user activities

B. Logging data communication access activities

C. Verifying user authorization at the field level

D. Changing data files

Answer: A

Explanation: General operating system access control functions include log user activities, log events, etc. Choice B is a network control feature. Choices C and D are database- and/or application-level access control functions.

7. A LAN can be best described as:

A. which connects computers of various types, terminals, printers and other devices within a limited proximity

B. which allows users to meet and share ideas

C. Tape library containing backed up tapes

D. TCP-IP

Answer: A

8. For Information security to be effective and complete:

   A. only Network security needs to be implemented

   B. ISO/OSI reference model should be implemented

   C. Security policy should be prepared but should not be shared with the users

   D. Users of all types and all levels should be made adequately aware of their roles and responsibilities.

   Answer: D

   Explanation: A & B are part of information security. C is irrelevant.

9. Which of the following types of transmission media provide the BEST security against unauthorized access?

   A. Copper wire

   B. Twisted pair

   C. Fibre-optic cables

   D. Coaxial cables

   Answer: C

   Explanation: Fibre-optic cables have proven to be more secure than the other media. Twisted pair and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

10. Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

    A. Sensitive data can be read by operators.

    B. Data can be amended without authorization.

    C. Unauthorized report copies can be printed.

    D. Output can be lost in the event of system failure.

    Answer: C

    Explanation: Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

11. Which of the following would enable an enterprise to provide its business partners access to its intranet (i.e., extranet) across the Internet?

A. Virtual private network

B. Client-server

C. Dial-in access

D. Network service provider

Answer: A

Explanation: Apart from being low cost, VPN rely on tunnelling techniques as a principal method of transport which allow the Internet-Protocol (IP) to carry a variety of different protocols (eg., SNA, IPX, NETBEUI). A client-server (choice B) does not address extending the network to business partners (i.e., client-server refers to a group of computers within an organization connected by a communications network where the client is the requesting machine and the server is the supplying machine). Choice C refers to remote users accessing a secured environment. It is the means, not the method, of providing access to a network. A network service provider (choice D) may provide services to a shared private network by providing Internet services, but it does not extend to an organization's intranet.

12. Which of the following device/technique is used in a data communications system to fully use the capacity of a high-speed data communication line?

A. Multiplexing

B. Bridge

C. Coaxial Cable

D. Star Topology

Answer: A

13. A Digital Certificate verifies the

A. Private key of the subject

B. Public key of the subject

C. Integrity of the subject

D. Strength of the Encryption Algorithm

Answer: B

Explanation: A Digital Certificate is a digital file used to cryptographically bind an entity's Public Key to specific attributes relating to its identity. The entity may be a person, organisation, web entity or software application. Like a driving license or passport binds a photograph to personal information about its holder, a Digital Certificate binds a Public Key to information about its owner.

14. For subtraction, if a SUB statement is used instead of 10110111, the programmer is using _____ language.

    A. fourth-generation language (4GL)

    B. Assembly Language

    C. High-Level Language

    D. Machine Language

    Answer: B

15. The main components of the Central Processing Unit (CPU) of a computer are:

    A. Semiconductors, printers and memory

    B. Arithmetic-logic unit, control Unit and primary memory

    C. Random access memory, read only memory and tape drive

    D. Primary storage, input-output devices and hub

    Answer: B

16. A packet filter router:

    A. Checks the header of each incoming packet to determine whether it matches any of the packet filtering rules.

    B. Decrypts the data

    C. Is used as an application server

    D. is a bastion host server

    Answer: A

17. Application, Presentation and session layers in OSI model are mapped to

    A. Application layer in TCP/IP model

    B. Transport layer in TCP/IP model

    C. Internet layer in TCP/IP model

    D. Network Interface Layer in TCP/IP model

    Answer: A

18. Brick-and-mortar companies have both physical and virtual stores.

    A. True

    B. False

    Answer: B

19. A compiler translates the source code of a program to machine language:

    A. True

    B. False

    Answer: B

20. _____ refers to sharing information, developing and maintaining business relationships, and using telecommunications networks to conduct business.

    A. E-Business

    B. CRM

    C. B2C

    D. SEO

    Answer: A

21. One of the following is not an example of computer software:

    A. Operating system

    B. Word processing package

    C. Application software

    D. Modem

    Answer: D

22. Name the hardware that transforms the computer's digital information into signals that can be sent over ordinary telephone lines is called

    A. Router

    B. IMAP

    C. POP

    D. Modem

    Answer: D

23. Three basic tenets of Information Security are:

    A. Encryption, Authentication, Backups

    B. Confidentiality, Integrity, Availability

    C. Topology, addressing, DMZ

    D. Access control lists, application controls, Network controls

    Answer: B

24. User Datagram Protocol (UDP)

    A. is a unreliable connectionless protocol

    B. is a reliable connectionless protocol

    C. is used at application layer

    D. Does handshaking

    Answer: A

    Explanation: Unlike TCP, UDP is a lighter-weight protocol that lacks connection orientation, order of delivery and guaranteed delivery. UDP consequently has less computing and network overhead, which makes it ideal for some protocols that are less sensitive to occasional packet loss. Sometimes UDP is called “Unreliable Data Protocol” a memory aid that is a reference to the protocol’s lack of guaranteed delivery.

25. ARP is:

    A. Resolution Protocol

    B. Media Access protocol

    C. Address Resolution protocol

    D. User Datagram Protocol

    Answer: C

26. An IP address is divided into

    A. Network ID and Host ID

    B. Seven layers

    C. Four layers

    D. Sub net mask

    Answer: A

27. Asynchronous transmission happens when

    A. Two devices with dissimilar speeds communicate

    B. Two devices with similar speeds communication

    C. OSI layers are used

    D. BUS topology is used

    Answer: A

28. In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

A. Foreign key

B. Primary key

C. Secondary key

D. Public key

Answer: A

Explanation: In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from acustomer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

29. A ring topology can be best described as:

A. All computers connected to a central hub

B. Each computer is connected to its neighbour and each link passes communications through its neighbour to the destination computer

C. All computers are connected to a backbone cable

D. All computers are connected to each other

Answer: B

30. A digital certificate is issued by:

A. Registration Authority

B. CERT

C. Digital certification Authority

D. Certificate Authority

Answer: D

31. Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

A. A remote access server

B. A proxy server

C. A personal firewall

D. A password-generating token

Answer: C

Explanation: A personal firewall is the best way to protect against hacking, because it can be defined with rules that describe the type of user or connection that is or is not permitted. A remote access server can be mapped or scanned from the Internet, creating security exposures. Proxy servers can provide protection based on the IP address and ports; however, an individual would need to have in-depth knowledge to do this, and applications can use different ports for the different sections of their program. A password-generating token may help to encrypt the session but does not protect a computer against hacking.

32. Digital signatures help in ensuring

A. Authentication, maintaining integrity, non-repudiation

B. Access to internet

C. Routing

D. Application security

Answer: A

33. When two devices communicate, the term described for data and control information to be transmitted and interpreted is:

A. Router

B. Synchronous communication

C. Cable

D. Communication protocol

Answer: D

34. Factors that degrade a signal are

A. Bus topology

B. TCP-IP

C. Attenuation, Delay Distortion, noise

D. Multiplexing

Answer: C

Explanation: Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems.

35. To protect a Local Area Network from external attacks which of the following is used:

    A. Passwords

    B. Fiber Optic cables

    C. Ring Topology

    D. Firewalls

    Answer: D

36. A digital signature does not contain:

    A. Certificate Serial Number

    B. Issuer's name

    C. Subject's name

    D. Private key of the subject

    Answer: D

37. What should be done to the Hard disk to prevent access to the data residing on it?

    A. Rewrite the hard disk with random 0s & 1s

    B. Low-level format the disk

    C. Demagnetize the disk

    D. Physically destroy the disk

    Answer: D

38. In IP address 122.35.0.56, which is the host id:

    A. 122

    B. 35

    C. 35.0.56

    D. 56

    Answer: C

39. In a full duplex mode of data transmission:

    A. Data is always transmitted in one direction only

    B. Data is transmitted in both direction but in only one direction at a time

    C. Data is transmitted in both directions simultaneously

D. USB is an example of full – duplex

Answer: C

40. In the OSI layers – Network layer is at number:

A. 1

B. 3

C. 7

D. 5

Answer: B

41. The susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls.

A. Inherent Risk

B. Control Risk

C. Detection Risk

D. Correction Risk

Answer: A

42. The analysis of Past-due account reports is an example of

A. Preventive controls

B. Detective controls

C. Corrective controls

D. Compensating controls

Answer: C

43. The Internal Audit functions are examples of

A. Preventive controls

B. Detective controls

C. Corrective controls

D. Compensating controls

Answer: B

44. The process of paying someone else to assume the risk is

A. Risk transference

B. Risk mitigation

C. Risk acceptance

D. Inherent risk

Answer: A

45. Evidence gathering to evaluate the integrity of individual transactions, data or other information is typical of which of the following?

A. Substantive testing

B. Compliance testing

C. Detection testing

D. Control testing

Answer: A

Evidence gathering to evaluate the integrity of individual transactions, data or other information is called substantive testing whereas evidence gathering for the purpose of testing an organization's compliance with control procedures is called compliance testing. Detection and control tests are irrelevant.

46. What is the first action an IS auditor should take after identifying a weakness in a control?

A. Suggest a corrective action

B. Take the finding directly to the steering committee

C. Try and find a compensating control for the identified weakness

D. Take note of it for inclusion in the final audit report

Answer: C

A control objective will not normally be achieved by considering one control adequate. The IS auditor will rather perform a variety of testing procedures and evaluate how these relate to one another. An IS auditor should always review for compensating controls prior to reporting a control weakness.

47. When planning an IS audit, which of the following factors is least likely to be relevant to the scope of the engagement?

A. The concerns of management for ensuring that controls are sufficient and working properly

B. The amount of controls currently in place

C. The type of business, management culture, and risk tolerance

D. The complexity of the technology used by the business in performing the business functions

Answer: B

The correct answer is B. How many controls are in place has little bearing on what the scope of the audit should be. Scope is a definition of what should be covered in the audit. What management is concerned about (A), what the management risk environment is (C), and how complex the technical environment is (D) could all have an impact of what the scope of a particular audit might be but not the sheer number of controls.

48. Due care can best be described as

A. A level of diligence that a prudent and competent person would exercise under a given set of circumstances

B. A level of best effort provided by applying professional judgment

C. A guarantee that no wrong conclusions are made during the course of the audit work

D. Someone with a lesser skill level that provides a similar level of detail or quality of work

Answer: A

The correct answer is A. Due care is a level of diligence applied to work performed. It is a reasonably competent third-party test. It does not ensure that no wrong conclusions are made (C) and is not related on a skill level (D) but a competence and prudence level. It is not a level of best effort (B). It is a benchmark to compare efforts against that which would have been done in similar circumstances by a prudent and competent person.

49. In a risk-based audit approach, an IS auditor must consider the inherent risk and

A. How to eliminate the risk through an application of controls

B. Whether the risk is material, regardless of management's tolerance for risk

C. The balance of the loss potential and the cost to implement controls

D. Residual risk being higher than the insurance coverage purchased

Answer: C

The correct answer is C. You do not want to eliminate risk (A), you want to only manage and control it. Management's tolerance of the risk is part of the definition of what is material so whether the risk is material (B) is not a correct answer. Insurance coverage is not necessarily the only control to consider for mitigating residual risk (D). The correct balance of cost to control any potential losses is a very important part of the risk mitigation considerations.

50. Which statement best describes the difference between a detective control and a corrective control?

A. Neither control stops errors from occurring. One control type is applied sooner than the other.

B. One control is used to keep errors from resulting in loss, and the other is used to warn of danger.

C. One is used as a reasonableness check, and the other is used to make management aware that an error has occurred.

D. One control is used to identify that an error has occurred and the other fixes the problems before a loss occurs.

Answer: D

The correct answer is D. While both are after the fact (A), the order of application is not really relevant. While corrective controls keep errors from resulting in loss (B), detective controls do not warn, deterrent controls do. While reasonableness checks can be a detective control, it also is used to make errors known (C).

51. One of the most important reasons for having the audit organization report to the audit committee of the board is because

A. Their budgets are more easily managed separate from the other budgets of the organization

B. The departments resources cannot easily be redirected and used for other projects

C. The internal audit function is to assist all parts of the organization and no one reporting manager should get priority on this help and support

D. The audit organization must be independent from influence from reporting structures that do not enable them to communicate directly with the audit committee

Answer: D

The correct answer is D. Independence from influence and for reporting purposes is the primary reason to have reporting lines outside of the corporate reporting structure.

52. Which of the following is not a method to identify risks?

A. Identify the risks, then determine the likelihood of occurrence and cost of a loss.

B. Identify the threats, their associated vulnerabilities, and the cost of losses.

C. Identify the vulnerabilities and effort to correct, based on the industry's best practices.

D. Seek managements risk tolerance and determine what threats exist that exceed that tolerance.

Answer: C

The correct answer is C. The industry's best practices must be tempered by management tolerance for risk and their direction. The elimination of risks is not your goal. Risk is only relevant to management's needs.

53. Which of the following is not a reason to be concerned about auditor independence?

A. The auditor starts dating the change control librarian.

B. The auditor invests in the business spin-off of the company.

C. The auditor used to manage the same business process at a different company.

D. The auditor is working as consultant for the implementation portion of the project being audited.

Answer: C

The correct answer is C. The fact that this was their job at another company may actually be an advantage for the audit team. The other items listed could lead to a compromise of the auditor's independence and should be investigated.

54. An audit charter serves the following primary purpose:

A. To describe the audit process used by the auditors

B. To document the mission and business plan of the audit department

C. To explain the code of ethics used by the auditor

D. To provide a clear mandate to perform the audit function in terms of authority and responsibilities

Answer: D

The correct answer is D. The charter's main purpose is to define the auditor's roles and responsibilities. It should evidence a clear mandate and authority for the auditors to perform their work. Unlike a mission statement (B) or a process document (A), it describes the bounds of authority. The code of ethics (C) is a non-relevant answer to this exercise.

55. Control objectives are defined in an audit program to

A. Give the auditor a view of the big picture of what the key control issue are based on the risk and management input

B. Enable the auditor to scope the audit to only those issues identified in the control objective

C. Keep the management from changing the scope of the audit

D. Define what testing steps need to be performed in the program

Answer: A

The correct answer is A. The scope is not defined exclusively by the auditor (C) and does not necessarily define testing the related tasks (D). Answer B is somewhat correct; however, Answer A is the best answer.

56. Some audit managements choose to use the element of surprise to

A. To check if the complacency has been built in and to see if there are procedures that can be used as a backup

B. Ensure that staffing is sufficient to manage an audit and daily processing simultaneously

C. Ensure that supervision is appropriate during surprise inspections

D. Ensure that policies and procedures coincide with the actual practices in place

Answer: A

The correct answer is A. Some of the other answers are nonsensical, but the real reason for using the element of surprise is to ensure that the policies and procedures documents line up with actual practices.

57. When identifying the potential for irregularities, the auditor should consider

A. If a vacation policy exists that requires fixed periods of vacation to be mandatory

B. How much money is devoted to the payroll

C. Whether the best practices are deployed in the IS environment

D. What kind of firewall is installed at the Internet

Answer: A

The correct answer is A. While the others have varying relevance to audit testing, they do not indicate possible irregularities by themselves. A vacation policy that does not require staff to be away from work for a fixed period of time - usually one to two full weeks - enables employees to maintain fraudulent schemes without requiring a trained back up employee to step in and perform the process for at least some period of time during the year.

58. When an audit finding is considered material, it means that

A. In terms of all possible risk and management risk tolerance, this finding is significant.

B. It has actual substance in terms of hard assets.

C. It is important to the audit in terms of the audit objectives and findings related to them.

D. Management cares about this kind of finding so it needs to be reported regardless of the risk.

Answer: A

The correct answer is A. Materiality is a relative, professional judgment call that must take into context management's aggregate tolerance of risk, how this finding stacks up to all of the findings, and the potential cumulative effect of this error.

59. In order to meet the requirements of audit, evidence sampling must be

A. Of a 95 percent or higher confidence level, based on repeated pulls of similar sample sizes

B. Sufficient, reliable, relevant, and useful, and supported by the appropriate analysis

C. Within two standard deviations of the mean for the entire population of the data

D. A random selection of the population in which every item has an equal chance of being selected

Answer: B

The correct answer is B. Sampling satisfies the evidence requirements that the data is sufficient, reliable, relevant, useful, and supported by the appropriate analysis. A random population section (D) is the definition of a random sample. Answers A and C do not make sense.

60. Audit evidence can take many forms. When determining the types required for an audit, the auditor must consider

A. CAATs, flowcharts, and narratives

B. Interviews, observations, and re-performance testing

C. The best evidence available that is consistent with the importance of the audit objectives

D. Inspection, confirmation, and substantive testing

Answer: C

The correct answer is C. The rest of the answers list types of audit evidence that could be considered, but the auditor must consider the best evidence available and determine what method for gathering and reviewing it as a second step in the audit planning process.

61. The primary thing to consider when planning for the use of CAATs in an audit program is

A. Whether the sampling error will be at an unacceptable level

B. Whether you can trust the programmer who developed the tools of the CAATs

C. Whether the source and object codes of the programs of the CAATs match

D. The extent of the invasive access necessary to the production environment

Answer: D

The correct answer is D. There is no sampling error with CAATs, which is one of their strengths (A), you will need to be aware of other participants in the process but that should be under your control (B), and understanding whether the source and object code match is an issue with what you are testing not to itself (C). The best answer is that you should be concerned with the potential impact of your testing on live data.

62. The most important aspect of drawing conclusions in an audit report is to

A. Prove your initial assumptions were correct.

B. Identify control weakness based on test work performed.

C. Obtain the goals of the audit objectives and to form an opinion on the sufficiency of the control environment.

D. Determine why the client is at risk at the end of each step.

Answer: C

The correct answer is C. Answer A is not value-added to the client; neither is D unless there is a weakness identified first. Answer B is an okay answer, however, Answer C is the best possible choice.

63. Some things to consider when determining what reportable findings should be are

A. How many findings there are and how long the report would be if all findings were included

B. The materiality of the findings in relevance to the audit objectives and management's tolerance for risk

C. How the recommendations will affect the process and future audit work

D. Whether the test samples were sufficient to support the conclusions

Answer: B

The correct answer is B. Materiality, audit objectives, and management's direction are the key items to consider. Answer D needs resolving long before the findings are

reviewed for reportability; Answer A, how many, or Answer C, the effect of the recommendations, is not an issue with whether they should be reported or not.

64. The primary objective of performing a root cause analysis is to

A. Ask why three times.

B. Perform an analysis that justifies the recommendations.

C. Determine the costs and benefits of the proposed recommendations.

D. Ensure that you are not trying to address symptoms rather than the real problem that needs to be solved.

Answer: D

The correct answer is D. Answers B and C are not correct because they are related to recommendations and not to the root cause. Answer A is a technique used in root cause analysis. The best answer is D

65. The primary reason for reviewing audit work is to

A. Ensure that the conclusions, testing, and results were performed with due professional care.

B. Ensure that the findings are sufficient to warrant the final report rating.

C. Ensure that all of the work is completed and checked by a supervisor.

D. Ensure that all of the audits are consistent in style and technique.

Answer: A

The correct answer is A. The other answers are all important but the primary reason is one of ensuring due professional care by checking the work with a reasonably competent third-party review.

66. Which criteria would an IS auditor consider to be the most important aspect of an organization's IS strategy?

A. It includes a mission statement.

B. It identifies a mechanism for charging for its services.

C. It includes a Web-based e-commerce strategy.

D. It supports the business objectives.

Answer: D

The correct answer is D. While a mission statement (A) is certainly a common component of a strategy documentation, and charging mechanisms (B) can be included as a reference, the most important item to consider is the alignment of the strategy with

the business needs and objectives. Web strategies (C) may or may not be relevant to the business at hand.

67. The development of an IS security policy is ultimately the responsibility of the:

A. IS department.

B. Security committee.

C. Security administrator.

D. Board of directors.

Answer: D

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

68. Involvement of senior management is MOST important in the development of:

A. Strategic plans.

B. IS policies.

C. IS procedures.

D. Standards and guidelines.

Answer: A.

Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

69. The output of the risk management process is an input for making:

A. business plans.

B. audit charters.

C. security policy decisions.

D. software design decisions.

Answer: C

Explanation: The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

70. The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction policy.

B. security policy.

C. archive policy.

D. audit policy.

Answer: C

Explanation: With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

71. An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirements.

B. if proposed system functionality is adequate.

C. the stability of existing software.

D. the complexity of installed technology.

Answer: A.

Explanation: The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

72. An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environment.

B. the business plan.

C. the present IT budget.

D. current technology trends.

Answer: B

Explanation: The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, the IS auditor would first need to familiarize him/herself with the business plan.

73. As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirements.

B. baseline security following best practices.

C. institutionalized and commoditized solutions.

D. an understanding of risk exposure.

Answer: A

Explanation: Information security governance, when properly implemented, should provide four basic outcomes. They are strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

74. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

A. compute the amortization of the related assets.

B. calculate a return on investment (ROI).

C. apply a qualitative approach.

D. spend the time needed to define exactly the loss amount.

Answer: C

Explanation: The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor (e.g., one is a very low impact to the business and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

75. The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial results.

B. customer satisfaction.

C. internal process efficiency.

D. innovation capacity.

Answer: A

Explanation: Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

76. Establishing the level of acceptable risk is the responsibility of:

A. quality assurance management.

B. senior business management.

C. the chief information officer.

D. the chief security officer.

Answer: B

Explanation: Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

77. Which of the following is the MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation: Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules are also required along with the user's education on the importance of security.

78. To ensure an organization is complying with privacy requirements, the IS auditor should FIRST review:

A. the IT infrastructure.

B. the organization's policies, standards and procedures.

C. legal and regulatory requirements.

D. the adherence to organizational policies, standards and procedures.

Answer: C

Explanation: To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, the IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

79. Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider

B. Participating in systems design with the provider

C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

Answer: D

Explanation: In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a by-product of monitoring

the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

80. Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.

B. define key performance indicators.

C. provide business value to IT projects.

D. control IT expenses.

Answer: B

Explanation: A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

81. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.

B. a lack of a methodology for systems development.

C. the technology not aligning with the organization's objectives.

D. an absence of control over technology contracts.

Answer: C

Explanation: A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

82. Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.

B. Specific user accountability cannot be established.

C. Unauthorized users may have access to originate, modify or delete data.

D. Audit recommendations may not be implemented.

Answer: C.

Explanation: Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access

to specific users, there is a better chance that business objectives will be properly supported.

83. Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business plan.

B. audit plan.

C. security plan.

D. investment plan.

Answer: A

Explanation: To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans arenot part of the IT plan, and the security plan should be at a corporate level.

84. Which of the following is a function of an IS steering committee?

A. Monitoring vendor-controlled change control and testing

B. Ensuring a separation of duties within the information's processing environment

C. Approving and monitoring major projects, the status of IS plans and budgets

D. Liaising between the IS department and the end users

Answer: C

Explanation: The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

85. Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response

B. Correction

C. Detection

D. Monitoring

Answer: A.

Explanation: A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

86. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services

B. Participating in systems design with the provider

C. Managing compliance with the contract for the outsourced services

D. Negotiating contractual agreement with the provider

Answer: C

Explanation: Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

87. When reviewing IS strategies, the IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

A. has all the personnel and equipment it needs.

B. plans are consistent with management strategy.

C. uses its equipment and personnel efficiently and effectively.

D. has sufficient excess capacity to respond to changing directions.

Answer: B

Explanation: Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

88. Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors.

B. Gather performance data.

C. Establish performance baselines.

D. Optimize performance.

Answer: D

Explanation: An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability, and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

89. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivity.

B. reduce the opportunity for an employee to commit an improper or illegal act.

C. provide proper cross-training for another employee.

D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Answer: B

Explanation: Required vacations/holidays of a week or more duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions. This reduces the opportunity to commit improper or illegal acts, and during this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

90. In reviewing the IS short-range (tactical) plan, the IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.

B. there is a clear definition of the IS mission and vision.

C. there is a strategic information technology planning methodology in place.

D. the plan correlates business objectives to IS goals and objectives.

Answer: A

Explanation: The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

91. Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package.

B. Perform an evaluation of information technology needs.

C. Implement a new project planning system within the next 12 months.

D. Become the supplier of choice for the product offered.

Answer: D

Explanation: Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs.

Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

92. Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT projects.

B. using the firm's past actual loss experience to determine current exposure.

C. reviewing published loss statistics from comparable organizations.

D. reviewing IT control weaknesses identified in audit reports.

Answer: A

Explanation: To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Hence, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited and there may not be a sufficient assessment of strategic IT risks.

93. Network Penetration testing is also called as:

A. Ethical Hacking

B. Handshaking

C. Cracking a User password

D. Social Engineering

Answer: A

94. One of the following is not a physical access control technique

A. Bolting door locks

B. Combination of cipher locks

C. Biometric Door locks

D. Public Key Infrastructure

Answer: D

95. An audit review of physical and environmental security of a CRITICAL area, like data centre, will not cover the following:

A. Authorization, authentication and access controls in the operating systems and application systems.

B. Availability of identification sign boards for approach to the critical areas

C. Physical access controls to the critical areas

D. Environmental controls like adequacy of UPS, temperature and humidity controls, fire and smoke detection system

Answer: A

96. One of the following is not a password attack:

A. Password guessing

B. Brute force

C. Dictionary attack

D. Password Encryption

Answer: D

97. To exercise controls over physical access to facilities following technique is not used:

A Identification badges

B. Manual logging

C. Security guards

D. Hardening of operating systems

Answer: D

98. One of the main advantage of employing biometric access controls is:

A. It helps to restrict the access by authorized persons only

B. Sharing password is restricted

C. Passwords can be encrypted

D. Audit trails can be enabled

Answer: A

99. User ID and password is a:

A. Encryption control

B. Logical access control

C. Backup control

D. Environmental control

Answer: B

100. A Biometrics authentication like finger print or voice recognition needs to be calibrated so that:

A. False positives and false negatives are low and the results are as accurate as possible

B. Encrypt the credentials

C. Create audit trails

D. Corrective control

Answer: A

101. Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs

B. Dynamic passwords

C. Key verification

D. Biometrics

Answer: D

Explanation: Biometrics can be used to provide excellent physical access control.

102. During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

A. enrollment.

B. identification.

C. verification.

D. storage.

Answer: A

Explanation: The users of a biometrics device must first be enrolled in the device. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.

103. A penetration test performed as part of evaluating network security:

A. provides assurance that all vulnerabilities are discovered.

B. should be performed without warning the organization's management.

C. exploits the existing vulnerabilities to gain unauthorized access.

D. would not damage the information assets when performed at network perimeters.

Answer: C

Explanation: Penetration tests are an effective method of identifying real-time risks to an information processing environment. They attempt to break into a live site in order to gain unauthorized access to a system. They do have the potential for damaging information assets or misusing information because they mimic an experienced hacker attacking a live system. On the other hand, penetration tests do not provide assurance that all vulnerabilities are discovered because they are based on a limited number of procedures. Management should provide consent for the test to avoid false alarms to IT personnel or to law enforcement bodies.

104. Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

A. Targeted testing

B. External testing

C. internal testing

D. Double-blind testing

Answer: D

Explanation: In a double-blind test, the administrator and security staff are not aware of the test, which will result in an assessment of the incident handling and response capability in an organization. In targeted, external, and internal testing, the system administrator and security staff are aware of the tests since they are informed before the start of the tests.

105. An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

A. The tools used to conduct the test

B. Certifications held by the IS auditor

C. Permission from the data owner of the server

D. An intrusion detection system (IDS) is enabled

Answer: C

Explanation: The data owner should be informed of the risks associated with a penetration test, what types of tests are to be conducted and other relevant details. All other choices are not as important as the data owner's responsibility for the security of the data assets.

106. An IS auditor doing penetration testing during an audit of internet connections would:

A. evaluate configurations.

B. examine security settings.

C. ensure virus-scanning software is in use.

D. use tools and techniques available to a hacker.

Answer: D

Explanation: Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of

107. The MOST important success factor in planning a penetration test is:

A. the documentation of the planned testing procedure.

B. scheduling and deciding on the timed length of the test.

C. the involvement of the management of the client organization.

D. the qualifications and experience of staff involved in the test.

Answer: C

Explanation: The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

108. Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners

B. Surge protective devices

C. Alternative power supplies

D. Interruptible power supplies

Answer: A

Explanation: Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment. Surge protection devices protect against high-voltage bursts. Alternative power supplies are intended for computer equipment running for longer periods and are normally coupled with other devices such as an uninterruptible power supply (UPS) to compensate for the power loss until the alternate power supply becomes available. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

109. During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

A. Look for compensating controls.

B. Review financial transactions logs.

C. Review the scope of the audit.

D. Ask the administrator to disable these accounts.

Answer: A

Explanation: The best logical access control practice is to create user IDs for each individual to define accountability. This is possible only by establishing a one-to-one relationship between IDs and individuals. However, if the user IDs are created based on role designations, an IS auditor should first understand the reasons and then evaluate the effectiveness and efficiency of compensating controls. Reviewing transactions logs is not relevant to an audit of logical access control nor is reviewing the scope of the audit relevant. Asking the administrator to disable the shared accounts should not be recommended by an IS auditor before understanding the reasons and evaluating the compensating controls. It is not an IS auditor's responsibility to ask for disabling accounts during an audit.

110. An organization has been recently downsized, in light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:

A. all system access is authorized and appropriate for an individual's role and responsibilities.

B. management has authorized appropriate access for all newly-hired individuals.

C. only the system administrator has authority to grant or modify access to individuals.

D. access authorization forms are used to grant or modify access to individuals.

Answer: A

Explanation: The downsizing of an organization implies a large number of personnel actions over a relatively short period of time. Employees can be assigned new duties while retaining some or all of their former duties. Numerous employees may be laid off. The auditor should be concerned that an appropriate segregation of duties is maintained, that access is limited to what is required for an employee's role and responsibilities, and that access is revoked for those that are no longer employed by the organization. Choices B, C and D are all potential concerns of an IS auditor, but in light of the particular risks associated with a downsizing, should not be the primary concern.

111. Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic

B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic

C. Having no physical signs on the outside of a computer center building

D. Using two firewalls in parallel to check different types of incoming traffic

Answer: B

Explanation: Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

112. Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy

B. Access control lists

C. Password management

D. System configuration files

Answer: A

Explanation: The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are tools for implementing the access controls.

113. The PRIMARY objective of a logical access control review is to:

A. review access controls provided through software.

B. ensure access is granted per the organization's authorities.

C. walk through and assess the access provided in the IT environment.

D. provide assurance that computer hardware is adequately protected against abuse.

Answer: B

Explanation: The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

114. During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.

B. user access management is time consuming.

C. passwords are easily guessed.

D. user accountability may not be established.

Answer: D

Explanation: The use of a single user ID by more than one individual precludes knowing who in fact used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

115. Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model

B. Access is granted on a least-privilege basis, per the organization's data owners

C. Implementing the Take-Grant access control model

D. Classifying data according to the subject's requirements

Answer: B

Explanation: Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

116. What are often the primary safeguards for systems software and data?

A. Administrative access controls

B. Logical access controls

C. Physical access controls

D. Detective access controls

Answer: B

Explanation: Logical access controls are often the primary safeguards for systems software and data.

117. Which of the following physical access controls effectively reduces the risk of piggybacking?

A. Biometric door locks

B. Combination door locks

C. Dead man doors

D. Bolting door locks

Answer: C

Explanation: Dead man doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding area. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric key pad or dial to gain entry. They do not prevent or reduce the risk of piggybacking since unauthorized individuals may still gain access to the processing center. Bolting door locks require the traditional metal key to gain entry. Unauthorized individuals could still gain access to the processing center along with an authorized individual.

118. In the context of physical access control, what is known as the process of verifying user identities?

A. Authentication

B. Authorization

C. Accounting

D. Encryption

Answer: A.

Explanation: Authentication is the process of verifying a user's claimed identity. It is based on at least one of these three factors: Something you know, Something you have, or Something you are.

119. Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based

B. Signature-based

C. Neural network

D. Host-based

Answer: A

Explanation: A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

120. What is the BEST approach to mitigate the risk of a phishing attack?

A. Implement an intrusion detection system (IDS)

B. Assess web site security

C. Strong authentication

D. User education

Answer: D

Explanation: Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious internet communications and not to trust them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

121. The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

A. Antivirus software

B. Hardening the servers

C. Screening routers

D. Honey pots

Answer: D

Explanation:
Honey pots can collect data on precursors of attacks. Since they serve no business function, honey pots are hosts that have no authorized users other than the honey pot administrators. All activity directed at them is considered suspicious. Attackers will scan and attack honey pots , giving administrators data on new trends and attack tools, particularly malicious code. However, honey pots are a supplement to, not a replacement for, properly securing networks, systems and applications. If honey pots are to be used by an organization, qualified incident handlers and intrusion detection analysts should manage them. The other choices do not provide indications of potential attacks.

122. Which of the following potentially blocks hacking attempts?

A. Intrusion detection system

B. Honey pot system

C. Intrusion prevention system

D. Network security scanner

Answer: C

Explanation: An intrusion prevention system (IPS) is deployed as an in-line device that can detect and block hacking attempts. An intrusion detection system (IDS) normally is deployed in sniffing mode and can detect intrusion attempts, but cannot effectively stop them. A honey pot solution traps the intruders to explore a simulated target. A network security scanner scans for the vulnerabilities, but it will not stop the intrusion.

123. An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

A. IDS sensors are placed outside of the firewall.

B. a behavior-based IDS is causing many false alarms.

C. a signature-based IDS is weak against new types of attacks.

D. the IDS is used to detect encrypted traffic.

Answer: D

Explanation: An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks. These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature-based IDS, because it can only recognize attacks that have been previously identified.

124. When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

A. Number of nonthreatening events identified as threatening

B. Attacks not being identified by the system

C. Reports/logs being produced by an automated tool

D. Legitimate traffic being blocked by the system

Answer: B

Explanation: Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often, IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem. An IDS does not block any traffic.

125. To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:

A. Firewall and the organization's network.

B. Internet and the firewall.

C. Internet and the web server.

D. Web server and the firewall.

Answer: A

Explanation: Attack attempts that could not be recognized by the firewall will be detected if a network-based intrusion detection system is placed between the firewall

and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

126. E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network. The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.

B. create an entry in the log.

C. close firewall-2.

D. close firewall-1.

Answer: C

Explanation: Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been be caused by an attack from a hacker. Closing firewa!l-2 is the first thing that should be done, thus preventing damage to the internal network. After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

127. Which of the following is a feature of an intrusion detection system (IDS)?

A. Gathering evidence on attack attempts

B. Identifying weaknesses in the policy definition

C. Blocking access to particular sites on the Internet

D. Preventing certain users from accessing specific servers

Answer: A

Explanation: An IDS can gather evidence on intrusive activity such as an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, while choice B requires a manual review, and therefore is outside the functionality of an IDS.

128. Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

A. Analyzer

B. Administration console

C. User interface

D. Sensor

Answer: D

Explanation: Sensors are responsible for collecting data . Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

129. Which of the following would MOST effectively reduce social engineering incidents?

A. Security awareness training

B. increased physical security measures

C. E-mail monitoring policy

D. intrusion detection systems

Answer: A

Explanation: Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e-mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

130. Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

A. Intrusion detection systems

B. Data mining techniques

C. Firewalls

D. Packet filtering routers

Answer: B

Explanation: Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

131. The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

A. Utilization of an intrusion detection system to report incidents

B. Mandating the use of passwords to access all software

C. Installing an efficient user log system to track the actions of each user

D. Training provided on a regular basis to all current and new employees.

Answer: D

Explanation: Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

132. An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

A. The corporate network is using an intrusion prevention system (IPS)

B. This part of the network is isolated from the corporate network

C. A single sign-on has been implemented in the corporate network

D. Antivirus software is in place to protect the corporate network

Answer: B

Explanation: If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An I PS would detect possible attacks, but only after they have occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

133. When auditing the requirements phase of a software acquisition, the IS auditor should:

A. assess the feasibility of the project timetable.

B. assess the vendor's proposed quality processes.

C. ensure that the best software package is acquired.

D. review the completeness of the specifications.

Answer: D

Explanation: The purpose of the requirements phase is to specify the functionality of the proposed system; therefore the IS auditor would concentrate on the completeness of the specifications. The decision to purchase a package from a vendor would come after the requirements have been completed. Therefore choices B and C are incorrect. Choice A is incorrect because a project timetable normally would not be found in a requirements document.

134. Which of the following is critical to the selection and acquisition of the correct operating System software?

A. Competitive bids

B. User department approval

C. Hardware configuration analysis

D. Purchasing department approval

Answer: C

Explanation: The purchase of operating system software is dependent on the fact that the software is compatible with the existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

135. Assumptions while planning an IS project involve a high degree of risk because they are:

A. based on known constraints.

B. based on objective past data.

C. a result of a lack of information.

D. often made by unqualified people.

Answer: C

Explanation: Assumptions are made when adequate information is not available. When an IS project manager makes an assumption, there is a high degree of risk because the lack of proper information can cause unexpected loss to an IS project. Assumptions are not based on "known" constraints. When constraints are known in advance, a project manager can plan according to those constraints rather than assuming the constraints will not affect the project. Having objective data about past IS projects will not lead to making assumptions, but rather helps the IS project manager in planning the project. Hence, if objective past data are available and the project manager makes use of them,

the risk to the project is less. Regardless of whether they are made by qualified people or unqualified people, assumptions are risky.

136. When implementing an acquired system in a client-server environment, which of the following tests would confirm that the modifications in the Windows registry do not adversely impact the desktop environment?

A. Sociability testing

B. Parallel testing

C. White box testing

D. Validation testing

Answer: A

Explanation: When implementing an acquired system in an client-server environment, sociability testing would confirm that the system can operate in the target environment without adversely impacting other systems. Parallel testing is the process of feeding test data to the old and new systems and comparing the results. White box testing is based on a close examination of procedural details, and validation testing tests the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

137. The IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could the IS auditor use to estimate the size of the development effort?

A. Program evaluation review technique (PERT)

B. Counting source lines of code (SLOC)

C. Function point analysis

D. White box testing

Answer: C

Explanation: Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behaviour of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

138. A System Development Life Cycle can be best described as

A. A process used by programmers to document compliance

B. A methodology used to guide the process of software creation project management

C. A system design methodology that includes all the steps in problem definition, solution identification, testing, implementation, and maintenance of the solution

D. A process used to manage change control and approval cycles in a development environment

Answer: C

Explanation: The correct answer is C. SDLC methodologies are described by all of the answers provided for this question to some extent. They can guide in change control and approval cycles (D) and the project management of software development. It also can be helpful when analyzing capital- versus expense-related tasks related to development projects, but Answer C best describes the SDLC components and use as a design methodology.

139. During the problem analysis and solution design phases of an SDLC methodology, which of the following steps would you be most concerned with finding?

A. Current state analysis and documentation processes

B. Entity relationship diagramming and process flow definitions

C. Pilot testing of planned solutions

D. Gathering of functional requirements from business sponsors

Answer: C

Explanation: The correct answer is C. The other three answers are all part of a well-executed SDLC methodology used to design a system or software. However, the initial problem analysis and design phases of a development cycle are not the appropriate place for the testing of solutions, especially by piloting them with end users.

140. An organization's software-development projects are planned according to formal software Development Life Cycle (SDLC) processes. In which of the following phases would the software-development project's baselines and scope be established?

A. Feasibility

B. Requirements definition

C. Design

D. Development

Answer: C

Explanation: Although all answers are valid SDLC phases, procedures to prevent scope creep are base lined in the design phase of the systems-development life cycle (SDLC) model.

141. Which of the following processes are performed during the design phase of the systems-development life cycle (SDLC) model?

A. Develop test plans.

B. Baseline procedures to prevent scope creep.

C. Define the need that requires resolution, and map to the major requirements of the solution.

D. Program and test the new system. The tests verify and validate what has been developed.

Answer: B

Explanation: Procedures to prevent scope creep are base-lined in the design phase of the systems-development life cycle (SDLC) model.

142. The application test plans are developed in which of the following systems development life cycle (SDLC) phases?

A. Design

B. Testing

C. Requirement

D. Development

Answer: A

Explanation: Developing test plans for the various levels of testing is one of the key activities during the application development design phase. The test plans are used in the actual software testing.

143. Change control procedures to prevent scope creep during an application development project should be defined during:

A. design.

B. feasibility.

C. implementation.

D. requirements definition.

Answer: A

Explanation: The change control procedures are generally common for applications

within one organization; however, the application-specific change control procedures are to be defined during the design phase of SDLC and should be based on the modules in the software. The other choices are incorrect. It is too early to define change control procedures during the feasibility phase, and it would also be too late during the implementation phase and after the implementation of software.

144. When a systems development life cycle (SDLC) methodology is inadequate, the MOST serious immediate risk is that the new system will:

A. be completed late.

B. exceed the cost estimates.

C. not meet business and user needs.

D. be incompatible with existing systems.

Answer: C

Explanation: Although all of the answers are risks of an inadequate SDLC methodology, the first and most devastating is that the new system will not need business and user needs and requirements.

145. In which of the following phases of the system development life cycle (SDLC) is it the MOST important for the IS auditor to participate?

A. Design

B. Testing

C. Programming

D. Implementation

Answer: A

Explanation: Controls should be considered in the design phase and included in the system. The cost of building controls into a system will be minimized if they are included in the initial design.

146. When selecting software, which of the following business and technical issues is the MOST important to be considered?

A. Vendor reputation

B. Requirements of the organization

C. Cost factors

D. Installed base

Answer: B

Explanation: Establishing the requirements of the organization is a task that should be

completed early in the process. Cost factors are a part of the analysis in the evaluation of software alternatives. A vendor's reputation and the installed base become important only after the requirements are met.

147. Functionality is a characteristic associated with evaluating the quality of software products throughout their lifecycle, and is BEST described as the set of attributes that bear on the:

A. existence of a set of functions and their specified properties.

B. ability of the software to be transferred from one environment to another.

C. capability of software to maintain its level of performance under stated conditions.

D. relationship between the performance of the software and the amount of resources used.

Answer: A

Explanation: Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability, choice C refers to reliability and choice D refers to efficiency.

148. When assessing the potential scope of an application-development project, which of the following provides the most reliable estimate of the size of an information system?

A. Critical path analysis

B. Function point analysis

C. Program evaluation review technique

D. Rapid application development

Answer: B

Explanation: A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project. PERT is used in both the planning and control of projects for network management. RAD is a methodology that enables organizations to develop strategically important systems more quickly and to reduce development costs. Critical path analysis is a process for finding the shortest project duration by optimizing utilization of project resources.

149. What is a reliable technique for estimating the scope and cost of a software-development project?

A. Function point analysis (FPA)

B. Feature point analysis (FPA)

C. GANTT

D. PERT

Answer: A

Explanation: A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

150. Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)

B. GANTT

C. Rapid Application Development (RAD)

D. PERT

Answer: D

Explanation: PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

151. Who is ultimately responsible for providing requirement specifications to the software-development team?

A. The project sponsor

B. The project members

C. The project leader

D. The project steering committee

Answer: A

Explanation: The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

152. Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

A. Failing to perform user acceptance testing

B. Lack of user training for the new system

C. Lack of software documentation and run manuals

D. Insufficient unit, module, and systems testing

Answer: A

Explanation: Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

153. An IS auditor, performing a review of an application's controls, discovers a weakness in system software, which could materially impact the application. The IS auditor should:

A. Disregard these control weaknesses as a system software review is beyond the scope of this review.

B. Conduct a detailed system software review and report the control weaknesses.

C. Include in the report a statement that the audit was limited to a review of the application's controls.

D. Review the system software controls as relevant and recommend a detailed system software review.

Answer: D

Explanation: The IS auditor is not expected to ignore control weaknesses just because they are outside the scope of a current review. Further, the conduct of a detailed systems software review may hamper the audits schedule and the IS auditor may not be technically competent to do such a review at this time. If there are control weaknesses which have been discovered by the IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived. Hence, the appropriate option would be to review the systems software as relevant to the review and recommend a detailed systems software for which additional resources may be recommended.

154. The use of a GANTT chart can:

A. aid in scheduling project tasks.

B. determine project checkpoints.

C. ensure documentation standards.

D. direct the post-implementation review.

Answer: A

Explanation: A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

155. What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

A. Rapid application development (RAD)

B. GANTT

C. PERT

D. Decision trees

Answer: A

Explanation: Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

156. Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

A. PERT

B. Rapid application development (RAD)

C. Function point analysis (FPA)

D. GANTT

Answer: B

Explanation: Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

157. Which of the following methodologies is appropriate for planning and control activities and resources in a system project?

A. Critical path methodology (CPM)

B. Program evaluation review technique (PERT)

C. Gantt charts

D. Function point analysis

Answer: B

158. An organization planning to purchase a software package asks the IS auditor for a risk assessment. Which of the following is the MAJOR risk?

A. Unavailability of the source code

B. Lack of a vendor-quality certification

C. Absence of vendor/client references

D. Little vendor experience with the package

Answer: A

Explanation: If the vendor goes out of business, not having the source code available would make it impossible to update the (software) package. Lack of a vendor-quality certification, absence of vendor/client references and little vendor experience with the package are important issues but not critical.

159. During unit testing, the test strategy applied is:

A. black box.

B. white box.

C. bottom-up.

D. top-down.

Answer: B

Explanation: White box testing examines the internal structure of a module. A programmer should perform this test for each module prior to integrating the module with others. Black box testing focuses on the functional requirements and does not consider the control structure of the module. Choices C and D are not correct because these tests require that several modules have already been assembled and tested.

160. Good quality software is BEST achieved:

A. through thorough testing.

B. by finding and quickly correcting programming errors.

C. by determining the amount of testing using the available time and budget.

D. by applying well-defined processes and structured reviews throughout the project.

Answer: D.

Explanation: Testing can point to quality deficiencies, however, it cannot by itself fix them. Corrective action at this point in the project is expensive. While it is necessary to detect and correct program errors, the bigger return comes from detecting defects as they occur in upstream phases, such as requirements and design. Choice C is representative of the most common mistake when applying quality management to a software project. It is seen as overhead, instead early removal of defects has a substantial payback. Rework is actually the largest cost driver on most software projects. Choice D represents the core of achieving quality, that is, following a well-defined, consistent process and effectively reviewing key deliverables.

161. A decision support system (DSS):

A. is aimed at solving highly structured problems.

B. combines the use of models with non-traditional data access and retrieval functions.

C. emphasizes flexibility in the decision-making approach of users.

D. supports only structured decision-making tasks.

Answer: C

Explanation: DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi structured decision making tasks.

162. Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.

B. Periodic testing does not require separate test processes.

C. It validates application systems and tests the ongoing operation of the system.

D. The need to prepare test data is eliminated.

Answer: B

Explanation: An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

163. Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

A. Embedded audit module

B. Integrated test facility

C. Snapshots

D. Audit hooks

Answer: D

Explanation: The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially- written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audit trail is required.

164. Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software

B. Generalized audit software

C. Productivity audit software

D. Manual review

Answer: B

Explanation: Generalized audit software can be used to search for address field duplications.

165. During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

A. test data to validate data input.

B. test data to determine system sort capabilities.

C. generalized audit software to search for address field duplications.

D. generalized audit software to search for account field duplications.

Answer: C

Explanation: Since the name is not the same (due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation.

166. In a review of a software acquisition process, the IS auditor will typically not review the following:

A. Whether the decision to acquire the software flows from the feasibility study.

B. Whether the RFP (Request for Proposal) is adequately detailed for transaction volume, data base size, turn around time and response time requirements and vendor responsibilities are clearly specified in the RFP.

C. Whether Program change history exists.

D. Whether sufficient documentation is available to justify the selection of the final vendor/product

Answer: C

167. Auditing around the computer is also called

A. White Box Approach

B. Black Box Approach

C. Yellow Box Approach

D. Red Box Approach

Answer: B

168. Input controls in Application systems are:

A. To prevent unauthorized access to application and application data

B. To prevent unauthorized physical access to the Data centre

C. To ensure accuracy and completeness of data and instruction input into an application system,

D. For User Acceptance Testing

Answer: C

169. An IS auditor should use statistical sampling and not judgment (non-statistical) sampling, when:

A. the probability of error must be objectively quantified.

B. the auditor wishes to avoid sampling risk.

C. generalized audit software is unavailable.

D. the tolerable error rate cannot be determined.

Answer: A

Explanation: statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples.

170. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

Answer: C

Explanation: Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

171. What is used as a control to detect loss, corruption, or duplication of data?

A. Redundancy check

B. Reasonableness check

C. Hash totals

D. Accuracy check

Answer: C

Explanation: Hash totals are used as a control to detect loss, corruption, or duplication of data.

172. Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

A. Redundancy check

B. Completeness check

C. Accuracy check

D. Parity check

Answer: A

Explanation: A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of data.

173. Parity bits are a control used to validate:

A. Data authentication

B. Data completeness

C. Data source

D. Data accuracy

Answer: B

174. Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit

B. Existence check

C. Completeness check

D. Reasonableness check

Answer: D

Explanation: A completeness check is used to determine if a field contains data and

not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

175. What is an edit check to determine whether a field contains valid data?

A. Completeness check

B. Accuracy check

C. Redundancy check

D. Reasonableness check

Answer: A

Explanation: A completeness check is an edit check to determine whether a field contains valid data.

176. What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

A. Accuracy check

B. Completeness check

C. Reasonableness check

D. Redundancy check

Answer: C

Explanation: A reasonableness check is a data validation edit control that matches input data to an occurrence rate.

177. Which of the following is a data validation edit and control?

A. Hash totals

B. Reasonableness checks

C. Online access controls

D. Before and after image reporting

Answer: B

178. Which of the following is an implementation risk within the process of decision support systems?

A. Management control

B. Semi-structured dimensions

C. inability to specify purpose and usage patterns

D. Changes in decision processes

Answer: C, others are not a risk

179. When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

A. Before transaction completion

B. Immediately after an EFT is initiated

C. During run-to-run total testing

D. Before an EFT is initiated

Answer: D

180. When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question regarding the legal jurisdiction.

B. Having a provider abroad will cause excessive costs in future audits.

C. The auditing process will be difficult because of the distance.

D. There could be different auditing norms.

Answer: A

181. When using an integrated test facility (ITF), an IS auditor should ensure that:

A. production data are used for testing.

B. test data are isolated from production data.

C. a test data generator is used.

D. master files are updated with the test data.

Answer: B

182. An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

A. True

B. False

Answer: B

Explanation: An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

183. Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True

B. False

Answer: A

184. An IS auditor is assigned to perform a post-implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.

B. designed an embedded audit module exclusively for auditing the application system.

C. participated as a member of the application system project team, but did not have operational responsibilities.

D. provided consulting advice concerning application system best practices.

Answer: A

Explanation: implementing a control measure and then checking it is conflict of interest.

185. At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretion.

B. attempt to resolve the error.

C. recommend that problem resolution be escalated.

D. ignore the error, as it is not possible to get objective evidence for the software error.

Answer: C

Explanation: When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

186. What is the MOST effective method of preventing unauthorized use of data files?

A. Automated file entry

B. Tape librarian

C. Access control software

D. Locked library

Answer: C

Explanation: Access control software is an active control designed to prevent unauthorized access to data.

187. Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

A. Minimum operating requirements

B. Acceptable data loss

C. Mean time between failures

D. Acceptable time for recovery

Answer: B

Explanation: Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept. Mean time between failures and minimum operating requirements help in defining recovery strategies.

188. Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

A. Backup time would steadily increase

B. Backup operational cost would significantly increase

C. Storage operational cost would significantly increase

D. Server recovery work may not meet the recovery time objective (RTO)

Answer: D

Explanation: In case of a crash, recovering a server with an extensive amount of data could require a significant amount of time. If the recovery cannot meet the recovery time objective (RTO), there will be a discrepancy in IT strategies. It's important to ensure that server restoration can meet the RTO. Incremental backup would only take the backup of the daily differential, thus a steady increase in backup time is not always true. The backup and storage costs issues are not as significant as not meeting the RTO.

189. In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

A. Disaster tolerance is high.

B. Recovery time objective is high.

C. Recovery point objective is low.

D. Recovery point objective is high.

Answer: C

Explanation: A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data . If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of the disaster tolerance. The lower the RTO, the lower the disaster tolerance. Therefore, choice C is the correct answer.

190. An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

A. a data loss of up to 1 minute, but the processing must be continuous.

B. a 1-minute processing interruption but cannot tolerate any data loss.

C. a processing interruption of 1 minute or more.

D. both a data loss and a processing interruption longer than 1 minute.

Answer: A

Explanation: The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

191. Regarding a disaster recovery plan, the role of an IS auditor should include:

A. identifying critical applications.

B. determining the external service providers involved in a recovery test.

C. observing the tests of the disaster recovery plan.

D. determining the criteria for establishing a recovery time objective (RTO).

Answer: C

Explanation: The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

192. A lower recovery time objective (RTO) results in:

A. higher disaster tolerance.

B. higher cost.

C. wider interruption windows.

D. more permissive data loss.

Answer: B

Explanation: A recovery time objective (RTO) is based on the acceptable downtime in case of a disruption of operations. The lower the RTO, the higher the cost of recovery strategies. The lower the disaster tolerance, the narrower the interruption windows, and the lesser the permissive data loss.

193. If the recovery time objective (RTO) increases:

A. the disaster tolerance increases.

B. the cost of recovery increases.

C. a cold site cannot be used.

D. the data backup frequency increases.

Answer: A

Explanation: The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

194. \Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

A. Minimum operating requirements

B. Acceptable data loss

C. Mean time between failures

D. Acceptable time for recovery

Answer: B

Explanation: Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept. Mean time between failures and minimum operating requirements help in defining recovery strategies.

195. If the recovery time objective (RTO) increases:

A. the disaster tolerance increases.

B. the cost of recovery increases.

C. a cold site cannot be used.

D. the data backup frequency increases.

Answer: A

Explanation: The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

196. A Disaster can be BEST defined as:

A. A planned interruption of normal business process

B. Catastrophe

C. Local Incidence

D. An Unplanned interruption of normal business process

Answer: D

197. To address an organization's disaster recovery requirements, backup intervals should not exceed the:

A. service level objective (SLO).

B. recovery time objective (RTO).

C. recovery point objective (RPO).

D. maximum acceptable outage (MAO).

Answer: C

Explanation: The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

198. Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

A. Resuming critical processes

B. Recovering sensitive processes

C. Restoring the site

D. Relocating operations to an alternative site

Answer: A

Explanation: The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failure (MTBF). Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time and those that are not marked as high priority. Repairing and restoring the site to original status and resuming the business operations are time consuming operations and are not the highest priority. Relocating operations to an alternative site, either temporarily or permanently depending on the interruption, is a time consuming process; moreover, relocation may not be required.

199. The PRIMARY purpose of a business impact analysis (BIA) is to:

A. provide a plan for resuming operations after a disaster.

B. identify the events that could impact the continuity of an organization's operations.

C. publicize the commitment of the organization to physical and logical security.

D. provide the framework for an effective disaster recovery plan.

Answer: B

Explanation: A business impact analysis (BIA) is one of the key steps in the development of a business continuity plan (BCP). A BIA will identify the diverse events that could impact the continuity of the operations of an organization.

200. Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

A. The disaster levels are based on scopes of damaged functions, but not on duration.

B. The difference between low-level disaster and software incidents is not clear.

C. The overall BCP is documented, but detailed recovery steps are not specified.

D. The responsibility for declaring a disaster is not identified.

Answer: D

Explanation: If nobody declares the disaster, the response and recovery plan would not be invoked, making all other concerns mute. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to have someone invoke the plan. The difference between incidents and low-level disasters is always unclear and frequently revolves around the amount of time required to correct the damage. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery, if in fact someone has invoked the plan.

Mock Assessment Test Paper 7

1. In a data warehouse, data quality is achieved by:

   A. cleansing.

   B. restructuring.

   C. source data credibility.

   D. transformation.

   Answer: C. source data credibility.

   Explanation: In a data warehouse system, the quality of data depends on the quality of the originating source. Choices A, B and D relate to the composition of a data warehouse and do not affect data quality. Restructuring, transformation and cleansing all relate to reorganization of existing data within the database.

2. Which of the following is the GREATEST risk when implementing a data warehouse?

   A. Increased response time on the production systems

   B. Access controls that are not adequate to prevent data modification

   C. Data duplication

   D. Data that is not updated or current

   Answer: B. Access controls that are not adequate to prevent data modification

   Explanation: Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

3. Which of the following is critical to the selection and acquisition of the operating system software?

   A. Competitive bids

   B. User department approval

   C. Hardware configuration analysis

   D. Purchasing department approval

   Answer: C. Hardware configuration analysis

   Explanation: The purchase of operating system software is dependent on the fact that

the software is compatible with the existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

4. Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

   A. Utilization reports

   B. Hardware error reports

   C. System logs

   D. Availability reports

   Answer: D. Availability reports

   Explanation: IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating ive action. System logs are a recording of the system's activities.

5. A benefit of quality of service (QoS) is that the:

   A. entire network's availability and performance will be significantly improved.

   B. telecom carrier will provide the company with accurate service-level compliance reports.

   C. participating applications will have guaranteed service levels.

   D. communications link will be supported by security controls to perform secure online transactions.

   Answer: C. participating applications will have guaranteed service levels.

   Explanation: The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved, while the speed of data exchange for specific applications could be faster. Availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

6. For an online transaction processing system, transactions per second is a measure of:

A. throughput.

B. response time.

C. turnaround time.

D. uptime.

Answer: A. throughput.

Explanation: Throughput measures how much work is done by a system over a period of time; it measures the productivity of the system. In an online transaction processing system, transactions per second is a throughput index. Response time is defined as the length of time that elapsed between submission of an input and receipt of the first character of output in an online system. Turnaround time is the length of time that elapsed between submission of a job and receipt of a completed output. It is a measure of timeliness in a batch system. The percentage of time that the system is available for processing is called uptime or a reliability index; thus, this is not the Answer.

7. Which of the following is MOST important when assessing services provided by an Internet service provider (ISP)?

A. Performance reports generated by the ISP

B. The service level agreement (SLA)

C. Interviews with the provider

D. Interviews with other clients of the ISP

Answer: B. The service level agreement (SLA)

Explanation: A service level agreement provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed service. Choices A, C and D would not be the basis for an independent evaluation of the service.

8. Which of the following would normally be found in application run manuals?

A. Details of source documents

B. Error codes and their recovery actions

C. Program flowcharts and file definitions

D. Change records for the application source code

Answer: B. Error codes and their recovery actions

Explanation: Application run manuals should include actions to be taken by an operator when an error occurs. Source documents and source code are irrelevant to the operator. Although dataflow diagrams may be useful, detailed program diagrams and file definitions are not.

9. Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

   A. The use of diskless workstations

   B. Periodic checking of hard drives

   C. The use of current antivirus software

   D. Policies that result in instant dismissal if violated

   Answer: B. Periodic checking of hard drives

   Explanation: The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

10. An IS auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late-night shift a month as the senior computer operator. The MOST appropriate course of action for the IS auditor is to:

   A. advise senior management of the risk involved.

   B. agree to work with the security officer on these shifts as a form of preventative control.

   C. develop a computer-assisted audit technique to detect instances of abuses of this arrangement.

   D. review the system log for each of the late-night shifts to determine whether any irregular actions occurred.

   Answer: A. advise senior management of the risk involved.

   Explanation: The IS auditor's first and foremost responsibility is to advise senior management of the risk involved in having the security administrator perform an operation's function. This is a violation of separation of duties. The IS auditor should not get involved in processing.

11. An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

   A. the setup is geographically dispersed.

   B. the network servers are clustered in a site.

C. a hot site is ready for activation.

D. diverse routing is implemented for the network.

Answer: B. the network servers are clustered in a site.

Explanation: A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backups if a site has been destroyed. A hot site would also be a good alternative for a single-point-of-failure site.

12. To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files

B. Enabled access control software parameters

C. Logs of access control violations

D. System configuration files for control options used

Answer: D. System configuration files for control options used

Explanation: A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

13. A Ping command is used to measure:

A. attenuation.

B. throughput,

C. delay distortion.

D. latency.

Answer: D. latency.

Explanation: Latency, which is measured using a Ping command, represents the delay that a message/packet will have in traveling from source to destination. A decrease in amplitude as a signal propagates through a transmission medium is called attenuation. Throughput, which is the quantity of work per unit of time, is measured in bytes per second. Delay distortion represents delay in transmission because the rate of propagation of a signal along a transmission line varies with the frequency.

14. Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

A. A system downtime log

B. Vendors' reliability figures

C. Regularly scheduled maintenance log

D. A written preventive maintenance schedule

Answer: A. A system downtime log

Explanation: A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

15. Which of the following is the MOST effective means of determining which controls are functioning properly in an operating system?

A. Consulting with the vendor

B. Reviewing the vendor installation guide

C. Consulting with the system programmer

D. Reviewing the system generation parameters

Answer: D. Reviewing the system generation parameters

Explanation: System generation parameters determine how a system runs, the physical configuration and its interaction with the workload.

16. Capacity monitoring software is used to ensure:

A. maximum use of available capacity.

B. that future acquisitions meet user needs.

C. concurrent use by a large number of users.

D. continuity of efficient operations.

Answer: D. continuity of efficient operations.

Explanation: Capacity monitoring software shows the actual usage of online systems vs. their maximum capacity. The aim is to enable software support staff to ensure that efficient operation, in the form of response times, is maintained in the event that use begins to approach the maximum available capacity. Systems should never be allowed to operate at maximum capacity. Monitoring software is intended to prevent this. Although the software reports may be used to support a business case for future acquisitions, it would not provide information on the effect of user requirements and it would not ensure concurrent usage of the system by users, other than to highlight levels of user access.

17. An independent software program that connects two otherwise separate applications sharing computing resources across heterogeneous technologies is known as:

A. middleware.

B. firmware.

C. application software.

D. embedded systems.

Answer: A. middleware.

Explanation: Middleware is independent software that connects two otherwise separate applications sharing computing resources across heterogeneous technologies. Firmware is software (programs or data) that has been written onto read-only memory (ROM). It is a memory chip with embedded program code that holds its content when power is turned off. Firmware is a combination of software and hardware. Application software are programs that address an organization's processes and functions as opposed to system software, which enables the computer to function.

18. IS management has recently informed the IS auditor of its decision to disable certain referential integrity controls in the payroll system to provide users with a faster report generator. This will MOST likely increase the risk of:

A. data entry by unauthorized users.

B. a nonexistent employee being paid.

C. an employee receiving an unauthorized raise.

D. duplicate data entry by authorized users.

Answer: B. a nonexistent employee being paid.

Explanation: Referential integrity controls prevent the occurrence of unmatched foreign key values. Given that a nonexistent employee does not appear in the employees table, there will never be a corresponding entry in the salary payment's table. The other choices cannot be detected by referential integrity controls.

19. Following a reorganization of a company's legacy database, it was discovered that records were accidentally deleted. Which of the following controls would have MOST effectively detected this occurrence?

A. Range check

B. Table lookups

C. Run-to-run totals

D. One-for-one checking

Answer: C. Run-to-run totals

Explanation: Run-to-run totals would have been an effective detective control over processing in this situation. Table lookups and range checks are used for data

validation before input, or as close to the point of origination as possible. One-for-one checking is time-consuming and, therefore, less effective.

20. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called:

    A. alternative routing.

    B. diverse routing.

    C. redundancy.

    D. circular routing.

    Answer: B. diverse routing.

    Explanation: Diverse routing is the method of routing traffic through split-cable facilities or duplicate-cable facilities, which can be accomplished with different/duplicate cable sheaths. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics. Redundancy involves providing extra capacity, with an option to use such excess capacity in the event the primary transmission capability is not available. Circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open system interconnection.

21. Which of the following is widely accepted as one of the critical components in networking management?

    A. Configuration management

    B. Topological mappings

    C. Application of monitoring tools

    D. Proxy server trouble shooting

    Answer: A. Configuration management

    Explanation: Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally. It also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server trouble shooting is used for trouble-shooting purposes.

22. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following

must be added to the IS auditor's computer to enable it to communicate with the mainframe system?

A. Buffer capacity and parallel port

B. Network controller and buffer capacity

C. Parallel port and protocol conversion

D. Protocol conversion and buffer capability

Answer: D. Protocol conversion and buffer capability

Explanation: For the IS auditor's microcomputer to communicate with the mainframe, the IS auditor must use a protocol converter to convert the asynchronous and synchronous transmission. Additionally, the message must be spooled to the buffer to compensate for different rates of data flow.

23. The interface that allows access to lower- or higher-level network services is called:

A. firmware.

B. middleware.

C. X.25 interface.

D. utilities.

Answer: B. middleware.

Explanation: Middleware, a class of software employed by client-server applications, provides services, such as identification, authentication, directories and security. It facilitates client-server connections over the network and allows client applications to access and update remote databases and mainframe files. Firmware consists of memory chips with embedded program code that hold their content when the power is turned off. X.25 interface is the interface between data terminal equipment and data circuit terminating equipment for terminals operating in the packet mode on some public data networks. Utilities are system software used to perform system maintenance and routines that are required during normal processing, such as sorting or backup.

24. Which of the following controls will detect MOST effectively the presence of bursts of errors in network transmissions?

A. Parity check

B. Echo check

C. Block sum check

D. Cyclic redundancy check

Answer: D. Cyclic redundancy check

Explanation: The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free. In this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

25. Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router

B. Packet filter

C. Application gateway

D. Circuit gateway

Answer: C. Application gateway

Explanation: The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 4) and the ports it is directed to (in this case port 80, layer 4), it also checks every http command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and B) basically work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4 (not from higher levels). A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that, during an external access, instead of opening a single connection to the internal server, two connections are establishedâ€"one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

26. Which of the following reports is a measure of telecommunication transmissions and determines whether transmissions are completed accurately?

A. Online monitor reports

B. Downtime reports

C. Help desk reports

D. Response-time reports

Answer: A. Online monitor reports

Explanation: Online monitors measure telecommunication transmissions and determine whether transmissions are completed accurately. Downtime reports track the availability of telecommunication lines and circuits. Help desk reports handle problems occurring in the normal course of operations. Response-time reports identify the time it takes for a command entered at a terminal to be answered by the computer.

27. Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity

B. Availability

C. Completeness

D. Confidentiality

Answer: B. Availability

Explanation: In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

28. Checking for authorized software baselines is an activity addressed within which of the following?

A. Project management

B. Configuration management

C. Problem management

D. Risk management

Answer: B. Configuration management

Explanation: Configuration management accounts for all IT components, including software. Project management is about scheduling, resource management and progress tracking of software development. Problem management records and monitors incidents. Risk management involves risk identification, impact analysis, an action plan, etc.

29. Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

    A. Firewalls

    B. Routers

    C. Layer 2 switches

    D. VLANs

    Answer: A. Firewalls

    Explanation: Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

30. To evaluate the referential integrity of a database, an IS auditor should review the:

    A. composite keys.

    B. indexed fields.

    C. physical schema.

    D. foreign keys.

    Answer: D. foreign keys.

    Explanation: A foreign key is a column in a table that references a primary key of another table, thus providing the referential integrity. Composite keys consist of two or more columns designated together as a table's primary key. Field indexing speeds up searches, but does not ensure referential integrity. Referential integrity is related to the logical schema, not the physical schema.

31. Which of the following operating system mechanisms checks each request by a subject (user process) to access and use an object (e.g., file, device, program) to ensure that the request complies with a security policy?

    A. Address Resolution Protocol

    B. Access control analyzer

C. Reference monitor

D. Concurrent monitor

Answer: C. Reference monitor

Explanation: A reference monitor is an abstract mechanism that checks each request by a subject (user process) to access and uses an object (e.g., file, device, program) to ensure that the request complies with a security policy. A reference monitor is implemented via a security kernel, which is a hardware/software/firmware mechanism. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address that is recognized in the local network. An access control analyzer is an audit utility for analyzing how well access controls have been implemented and maintained within an access control package. A concurrent monitor is an audit utility that captures select events as application systems are running to facilitate assessing program quality.

32. Which of the following is an operating system access control function?

A. Logging user activities

B. Logging data communication access activities

C. Verifying user authorization at the field level

D. Changing data files

Answer: A. Logging user activities

Explanation: General operating system access control functions include log user activities, log events, etc. Choice B is a network control feature. Choices C and D are database- and/or application-level access control functions.

33. An IS auditor is PRIMARILY concerned about electromagnetic emissions from a cathode ray tube (CRT) because they may:

A. cause health disorders (such as headaches) and diseases.

B. be intercepted and information may be obtained from them.

C. cause interference in communications.

D. cause errors in the motherboard.

Answer: B. be intercepted and information may be obtained from them.

Explanation: The greatest risk, although infrequent, due to the expensive technology required is choice B. The expense would be justified only if the value of the information to be obtained was high. CRTs can be intercepted, and information obtained can be from them. This is called a tempest attack, taken from the code name of the first secret project in which such an interception was studied. These weak signals can be radiated

and intercepted with the proper equipment or transmitted, for example, via power leads. The signals fade rapidly as distance increases. The first line of defense is to create a physical security zone (PSZ) to keep receivers at a distance. They can cause health disorders, such as headaches and diseases; however, no studies have confirmed that these risks are higher than those posed by the natural radiation found in certain zones (e.g., mountain areas). The intensity of the radiation is so low that, with normal technology, they can not cause interference with communications.

34. Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

A. Filters

B. Switches

C. Routers

D. Firewalls

Answer: B. Switches

Explanation: Switches are at the lowest level of network security and transmit a packet to the device to which it is addressed. This reduces the ability of one device to capture the packets that are meant for another device. Filters allow for some basic isolation of network traffic based on the destination addresses. Routers allow packets to be given or denied access based on the addresses of the sender and receiver and the type of packet. Firewalls are a collection of computer and network equipment used to allow communications to flow out of the organization and restrict communications flowing into the organization.

35. In a database management system (DBMS), the location of data and the method of accessing the data are provided by the:

A. data dictionary.

B. metadata.

C. directory system.

D. data definition language.

Answer: C. directory system.

Explanation: A directory system describes the location of data and the access method. A data dictionary contains an index and description of all the items stored in the database. Metadata are the data elements required to define an enterprisewide data warehouse. The data definition language processor allows the database administrator (DBA) to create/modify a data definition for mapping between external and conceptual schemes.

36. In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

A. Diskless workstations

B. Data encryption techniques

C. Network monitoring devices

D. Authentication systems

Answer: C. Network monitoring devices

Explanation: Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

37. When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

A. they are set to meet security and performance requirements.

B. changes are recorded in an audit trail and periodically reviewed.

C. changes are authorized and supported by appropriate documents.

D. access to parameters in the system is restricted.

Answer: A. they are set to meet security and performance requirements.

Explanation: The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control. Reviewing changes to ensure they are supported by appropriate documents is also a detective control. If parameters are set inly, the related documentation and the fact that these are authorized does not reduce the impact. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set inly, restricting access will still have an adverse impact.

38. By establishing a network session through an appropriate application, a sender transmits a message by breaking it into packets, but the packets may reach the receiver out of sequence. Which OSI layer addresses the out-of-sequence message through segment sequencing?

A. Network layer

B. Session layer

C. Application layer

D. Transport layer

Answer: . D. Transport layer

Explanation: The function of resequencing packets (segment) received out of order is taken care of by the transport layer. Neither the network, session or application layers address resequencing.

39. Which of the following is a control over component communication failure/ errors?

A. Restricting operator access and maintaining audit trails

B. Monitoring and reviewing system engineering activity

C. Providing network redundancy

D. Establishing physical barriers to the data transmitted over the network

Answer: C. Providing network redundancy

Explanation: Redundancy by building some form of duplication into the network components, such as a link, router or switch, to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echo checks to detect line errors, parity checks, error ion codes and sequence checks. Choices A, B and D are communication network controls

40. An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

A. Electromagnetic interference (EMI)

B. Cross-talk

C. Dispersion

D. Attenuation

Answer: D. Attenuation

Explanation: Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

41. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

    A. A substantive test of program library controls

    B. A compliance test of program library controls

    C. A compliance test of the program compiler controls

    D. A substantive test of the program compiler controls

    Answer: B. A compliance test of program library controls

    Explanation: A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

42. A primary benefit derived from an organization employing control self-assessment (CSA)techniques is that it can:

    A. Identify high-risk areas that might need a detailed review later

    B. Reduce audit costs

    C. Reduce audit time

    D. Increase audit accuracy

    Answer: C. Reduce audit time

    Explanation: A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

43. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

    A. Integrated test facility (ITF)

    B. Continuous and intermittent simulation (CIS)

    C. Audit hooks

    D. Snapshots

    Answer: D. Snapshots

Explanation: A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

44. An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.

B. impact of any exposures discovered.

C. business processes served by the application.

D. application's optimization.

Answer: B. impact of any exposures discovered.

Explanation: An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

45. Which of the following is a substantive test?

A. Checking a list of exception reports

B. Ensuring approval for parameter changes

C. Using a statistical sample to inventory the tape library

D. Reviewing password history reports

Answer: C. Using a statistical sample to inventory the tape library

Explanation: A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated ly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

46. An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.

B. clearly state audit objectives for and the delegation of authority to the maintenance and review of internal controls.

C. document the audit procedures designed to achieve the planned audit objectives.

D. outline the overall authority, scope and responsibilities of the audit function.

Answer: D. outline the overall authority, scope and responsibilities of the audit function.

Explanation: An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

47. Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.

B. Periodic testing does not require separate test processes.

C. It validates application systems and tests the ongoing operation of the system.

D. It eliminates the need to prepare test data.

Answer: B. Periodic testing does not require separate test processes.

Explanation: An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

48. An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.

B. enables the financial and IS auditors to integrate their audit tests.

C. compares processing output with independently calculated data.

D. provides the IS auditor with a tool to analyze a large range of information.

Answer: C. compares processing output with independently calculated data.

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

49. When evaluating the collective effect of preventive, detective or ive controls within a process, an IS auditor should be aware:

A. of the point at which controls are exercised as data flow through the system.

B. that only preventive and detective controls are relevant.

C. that ive controls can only be regarded as compensating.

D. that classification allows an IS auditor to determine which controls are missing.

Answer: A. of the point at which controls are exercised as data flow through the system.

Explanation: An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is in since ive controls may also be relevant. Choice C is in since ive controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is in and irrelevant since the existence and function of controls is important, not the classification.

50. An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.

B. investigating various communication channels.

C. understanding the responsibilities and authority of individuals.

D. investigating the network connected to different employees.

Answer: C. understanding the responsibilities and authority of individuals.

Explanation: An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

51. Which of the following BEST describes an integrated test facility?

A. A technique that enables the IS auditor to test a computer application for the purpose of verifying processing

B. The utilization of hardware and/or software to review and test the functioning of a computer system

C. A method of using special programming options to permit the printout of the path through a computer program taken to process a specific transaction

D. A procedure for tagging and extending transactions and master records that are used by an IS auditor for tests

Answer: A. A technique that enables the IS auditor to test a computer application for the purpose of verifying processing

Explanation: Answer A best describes an integrated test facility, which is a specialized computer-assisted audit process that allows an IS auditor to test an application on a continuous basis. Answer B is an example of a systems control audit review file; Answers C and D are examples of snapshots.

52. An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.

B. interview programmers about the procedures currently being followed.

C. compare utilization records to operations schedules.

D. review data file access records to test the librarian function.

Answer: B. interview programmers about the procedures currently being followed.

Explanation: Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

53. Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling

B. Variable sampling

C. Stratified mean per unit

D. Difference estimation

Answer: A. Attribute sampling

Explanation: Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

54. Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.

B. Access controls establish accountability for e-mail activity.

C. Data classification regulates what information should be communicated via e-mail.

D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Answer: A. Multiple cycles of backup files remain available.

Explanation: Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

55. Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management

B. Review of the organization chart

C. Observation and interviews

D. Testing of user access rights

Answer: C. Observation and interviews

Explanation: By observing the IS staff performing their tasks, the IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

56. An IS auditor has evaluated the controls for the integrity of the data in a financial application. Which of the following findings would be the MOST significant?

A. The application owner was unaware of several changes applied to the application by the IT department.

B. The application data are backed up only once a week.

C. The application development documentation is incomplete.

D. Information processing facilities are not protected by appropriate fire detection systems.

Answer: A. The application owner was unaware of several changes applied to the application by the IT department.

Explanation: Choice A is the most significant finding as it directly affects the integrity of

the application's data and is evidence of an inadequate change control process and in access rights to the processing environment. Although backing up the application data only once a week is a finding, it does not affect the integrity of the data in the system. Incomplete application development documentation does not affect integrity of the data. The lack of appropriate fire detection systems does not affect the integrity of the data but may affect the storage of the data.

57. Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

B. the magnitude of the impact should a threat source successfully exploit the vulnerability.

C. the likelihood of a given threat source exploiting a given vulnerability.

D. the collective judgment of the risk assessment team.

Answer: A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.

Explanation: Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

58. An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were ly authorized. This is an example of:

A. variable sampling.

B. substantive testing.

C. compliance testing.

D. stop-or-go sampling.

Answer: C. compliance testing.

Explanation: Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go

sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.\

59. A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

A. can identify high-risk areas that might need a detailed review later.

B. allows IS auditors to independently assess risk.

C. can be used as a replacement for traditional audits.

D. allows management to relinquish responsibility for control.

Answer: A. can identify high-risk areas that might need a detailed review later.

Explanation: CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Answer B is in, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Answer C is in because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Answer D is in, because CSA does not allow management to relinquish its responsibility for control.

60. Data flow diagrams are used by IS auditors to:

A. order data hierarchically.

B. highlight high-level data definitions.

C. graphically summarize data paths and storage.

D. portray step-by-step details of data generation.

Answer: C. graphically summarize data paths and storage.

Explanation: Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

61. The use of statistical sampling procedures helps minimize:

A. sampling risk.

B. detection risk.

C. inherent risk.

D. control risk.

Answer: B. detection risk.

Explanation: Detection risk is the risk that the IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when in fact they do. Using statistical sampling, an IS auditor can quantify how closely the sample should represent the population and quantify the probability of error. Sampling risk is the risk that in assumptions will be made about the characteristics of a population from which a sample is selected. Assuming there are no related compensating controls, inherent risk is the risk that an error exists, which could be material or significant when combined with other errors found during the audit. Statistical sampling will not minimize this. Control risk is the risk that a material error exists, which will not be prevented or detected on a timely basis by the system of internal controls. This cannot be minimized using statistical sampling.

62. What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

A. Business risk

B. Detection risk

C. Residual risk

D. Inherent risk

Answer: B. Detection risk

Explanation: Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

63. The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

A. Inherent

B. Detection

C. Control

D. Business

Answer: B. Detection

Explanation: Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks usually are not affected by the IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by the IS auditor.

64. Which one of the following could an IS auditor use to validate the effectiveness of edit and validation routines?

A. Domain integrity test

B. Relational integrity test

C. Referential integrity test

D. Parity checks

Answer: A. Domain integrity test

Explanation: Domain integrity testing is aimed at verifying that the data conform to definitions, i.e., the data items are all in the domains. The major objective of this exercise is to verify that the edit and validation routines are working satisfactorily. Relational integrity tests are performed at the record level and usually involve calculating and verifying various calculated fields, such as control totals. Referential integrity tests involve ensuring that all references to a primary key from another file actually exist in their original file. A parity check is a bit added to each character prior to transmission. The parity bit is a function of the bits making up the character. The recipient performs the same function on the received character and compares the result to the transmitted parity bit. If it is different, an error is assumed.

65. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.

B. Determine the risks/threats to the data center site.

C. Review business continuity procedures.

D. Test for evidence of physical access at suspect locations.

Answer: B. Determine the risks/threats to the data center site.

Explanation: During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

66. The PRIMARY purpose of audit trails is to:

A. improve response time for users.

B. establish accountability and responsibility for processed transactions.

C. improve the operational efficiency of the system.

D. provide useful information to auditors who may wish to track transactions.

Answer: B. establish accountability and responsibility for processed transactions.

Explanation: Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency,

since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

67. Which of the following would BEST provide assurance of the integrity of new staff?

A. Background screening

B. References

C. Bonding

D. Qualifications listed on a resume

Answer: A. Background screening

Explanation: A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

68. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

A. enterprise data model.

B. IT balanced scorecard (BSC).

C. IT organizational structure.

D. historical financial statements.

Answer: B. IT balanced scorecard (BSC).

Explanation: A Balanced Scorecard defines what management means by "performance" and measures whether management is achieving desired results. The Balanced Scorecard translates Mission and Vision Statements into a comprehensive set of objectives and performance measures that can be quantified and appraised. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, IS Auditor should review IT Balanced Scorecard.

69. The advantage of a bottom-up approach to the development of organizational policies is that the policies:

A. are developed for the organization as a whole.

B. are more likely to be derived as a result of a risk assessment.

C. will not conflict with overall corporate policy.

D. ensure consistency across the organization.

Answer: B. are more likely to be derived as a result of a risk assessment.

Explanation: A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

70. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer? Each Answer represents a complete solution. Choose all that apply.

A. Facilitating the sharing of security risk-related information among authorizing officials

B. Preserving high-level communications and working group relationships in an organization

C. Establishing effective continuous monitoring program for the organization

D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

Answer: A. Facilitating the sharing of security risk-related information among authorizing officials

Explanation: A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization. Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

71. A data administrator is responsible for:

A. maintaining database system software.

B. defining data elements, data names and their relationship.

C. developing physical database structures.

D. developing data dictionary system software.

Answer: B. defining data elements, data names and their relationship.

Explanation: A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

72. Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.

B. define key performance indicators.

C. provide business value to IT projects.

D. control IT expenses.

Answer: B. define key performance indicators.

Explanation: A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

73. A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilities.

B. reporting to the end-user manager.

C. having programming responsibilities.

D. being responsible for LAN security administration.

Answer: C. having programming responsibilities.

Explanation: A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

74. The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.

B. performance of a comprehensive security control review by the IS auditor.

C. adoption of a corporate information security policy statement.

D. purchase of security access control software.

Answer: C. adoption of a corporate information security policy statement.

Explanation: A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

75. Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response

B. ion

C. Detection

D. Monitoring

Answer: A. Response

Explanation: A sound IS security policy will most likely outline a response program to handle suspected intrusions. ion, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

76. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.

B. a lack of a methodology for systems development.

C. the technology not aligning with the organization's objectives.

D. an absence of control over technology contracts.

Answer: C. the technology not aligning with the organization's objectives.

Explanation: A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

77. When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy

B. Defining the corporate security policy

C. Implementing the corporate security policy

D. Defining security procedures and guidelines

Answer: A. Accountability for the corporate security policy

Explanation: Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

78. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services

B. Participating in systems design with the provider

C. Managing compliance with the contract for the outsourced services

D. Negotiating contractual agreement with the provider

Answer: C. Managing compliance with the contract for the outsourced services

Explanation: Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

79. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information

B. information security is not critical to all functions.

C. IS audit should provide security training to the employees.

D. the audit finding will cause management to provide continuous training to staff.

Answer: A. this lack of knowledge may lead to unintentional disclosure of sensitive information

Explanation: All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

80. Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

A. Security administrator

B. Systems auditor

C. Board of directors

D. Financial auditor

Answer: C. Board of directors

Explanation: Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

81. IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

    A. desired result or purpose of implementing specific control procedures.

    B. best IT security control practices relevant to a specific entity.

    C. techniques for securing information.

    D. security policy.

    Answer: A. desired result or purpose of implementing specific control procedures.

    Explanation: An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

82. Which of the following is the PRIMARY objective of an IT performance measurement process?

    A. Minimize errors.

    B. Gather performance data.

    C. Establish performance baselines.

    D. Optimize performance.

    Answer: D. Optimize performance.

    Explanation: An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability, and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

83. Which of the following would provide a mechanism whereby IS management can determine if the activities of the organization have deviated from the planned or expected levels?

    A. Quality management

    B. IS assessment methods

    C. Management principles

    D. Industry standards/benchmarking

    Answer: B. IS assessment methods

Explanation: Assessment methods provide a mechanism, whereby IS management can determine if the activities of the organization have deviated from planned or expected levels. These methods include IS budgets, capacity and growth planning, industry standards/benchmarking, financial management practices, and goal accomplishment. Quality management is the means by which the IS department processes are controlled, measured and improved. Management principles focus on areas such as people, change, processes and security. Industry standards/ benchmarking provide a means of determining the level of performance provided by similar information processing facility environments

84. Which of the following is the MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Explanation: Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules are also required along with the user's education on the importance of security.

85. The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.

B. security and control policies support business and IT objectives.

C. there is a published organizational chart with functional descriptions.

D. duties are appropriately segregated.

Answer: B. security and control policies support business and IT objectives.

Explanation: Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

86. Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A. Assimilation of the framework and intent of a written security policy by all appropriate parties

Explanation: Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

87. Which of the following would be a compensating control to mitigate risks resulting from an inadequate segregation of duties?

A. Sequence check

B. Check digit

C. Source documentation retention

D. Batch control reconciliations

Answer: D. Batch control reconciliations

Explanation: Batch control reconciliations are an example of compensating controls. Other examples of compensating controls are transaction logs, reasonableness tests, independent reviews and audit trails, such as console logs, library logs and job accounting date. Sequence checks and check digits are data validation edits, and source documentation retention is an example of a data file control.

88. Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements

B. Promoting ethical understanding

C. Security awareness programs

D. Effective performance incentives

Answer: C. Security awareness programs

Explanation: Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

89. To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

A. O/S and hardware refresh frequencies

B. Gain-sharing performance bonuses

C. Penalties for noncompliance

D. Charges tied to variable cost metrics

Answer: B. Gain-sharing performance bonuses

Explanation: Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

90. A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recovery.

B. retention.

C. rebuilding.

D. reuse.

Answer: B. retention.

Explanation: Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic "paper" makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

91. When are benchmarking partners identified within the benchmarking process?

A. In the design stage

B. In the testing stage

C. In the research stage

D. In the development stage

Answer: C. In the research stage

Explanation: Benchmarking partners are identified in the research stage of the benchmarking process.

92. In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized

B. Managed

C. Defined

D. Repeatable

Answer: B. Managed

Explanation: Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be "managed and measurable."

93. Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.

B. Data can be amended without authorization.

C. Unauthorized report copies can be printed.

D. Output can be lost in the event of system failure.

Answer: C. Unauthorized report copies can be printed.

Explanation: Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure

94. Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.

B. data will not be deleted before that date.

C. backup copies are not retained after that date.

D. datasets having the same name are differentiated.

Answer: B. data will not be deleted before that date.

Explanation: A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and, therefore, may well be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

95. Which of the following can be used to verify output results and control totals by matching them against the input data and control totals?

A. Batch header forms

B. Batch balancing

C. Data conversion error ions

D. Access controls over print spools

Answer: B. Batch balancing

Explanation: Batch balancing is used to verify output results and control totals by matching them against the input data and control totals. Batch header forms control data preparation; data conversion error ions errors that occur due to duplication of

transactions and inaccurate data entry; and access controls over print spools prevent reports from being accidentally deleted from print spools or directed to a different printer.

96. Which of the following would an IS auditor expect to find in a console log?

A. Names of system users

B. Shift supervisor identification

C. System errors

D. Data edit errors

Answer: C. System errors

Explanation: System errors are the only ones that one would expect to find in the console log.

97. A network diagnostic tool that monitors and records network information is a(n):

A. online monitor.

B. downtime report.

C. help desk report.

D. protocol analyzer.

Answer: B. downtime report.

Explanation: Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

98. Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server

B. Simultaneously duplicating the system log on a write-once disk

C. Write-protecting the directory containing the system log

D. Storing the backup of the system log offsite

Answer: B. Simultaneously duplicating the system log on a write-once disk

Explanation: A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which

could be the result of changes made by an intruder. Write protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

99. During an audit of the tape management system at a data center, an IS auditor discovered that parameters are set to bypass or ignore the labels written on tape header records. The IS auditor also determined that effective staging and job setup procedures were in place. In this situation, the IS auditor should conclude that the:

A. tape headers should be manually logged and checked by the operators.

B. staging and job setup procedures are not appropriate compensating controls.

C. staging and job setup procedures compensate for the tape label control weakness.

D. tape management system parameters must be set to check all labels.

Answer: C. staging and job setup procedures compensate for the tape label control weakness.

Explanation: Compensating controls are an important part of a control structure. They are considered adequate if they help to achieve the control objective and are cost-effective. In this situation, the IS auditor is most likely to conclude that staging and job setup procedures compensate for the tape label control weakness.

100. IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

B. The service provider does not have incident handling procedures.

C. Recently a corrupted database could not be recovered because of library management problems.

D. Incident logs are not being reviewed.

Answer: A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

Explanation: The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery..

101. Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location

B. Setting a boot password

C. Hardening the server configuration

D. Implementing activity logging

Answer: C. Hardening the server configuration

Explanation: Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent non-privileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario "€" it is a detective control (not a preventive one) and the attacker who already gained privileged access can modify logs or disable them.

102. An IS auditor detected that several PCs connected to the Internet have a low security level that is allowing for the free recording of cookies. This creates a risk because cookies locally store:

A. information about the Internet site.

B. information about the user.

C. information for the Internet connection.

D. Internet pages.

Answer: B. information about the user.

Explanation: The cookie file resides on the client machine. It contains data passed from web sites, so that web sites can communicate with this file when the same client returns. The web site only has access to that part of the cookie file that represents the interaction with that particular web site. Cookie files have caused some issues with respect to privacy. The four choices all relate to a cookie, but the fact that the cookie stores information about the user is the risk.

103. Which of the following is the MOST probable cause for a mail server being used to send spam?

A. Installing an open relay server

B. Enabling Post Office Protocol (POP3)

C. Using Simple Mail Transfer Protocol (SMTP)

D. Activating user accounting

Answer: A. Installing an open relay server

Explanation: An open relay (or open proxy) allows unauthorized people to route their spam through someone else's mail server. POP3 and SMTP are commonly used mail protocols. Activating user accounting does not relate to using a server to send spam.

104. Which of the following is the MOST probable cause for a mail server being used to send spam?

A. Installing an open relay server

B. Enabling Post Office Protocol (POP3)

C. Using Simple Mail Transfer Protocol (SMTP)

D. Activating user accounting

Answer: A. Installing an open relay server

Explanation: An open relay (or open proxy) allows unauthorized people to route their spam through someone else's mail server. POP3 and SMTP are commonly used mail protocols. Activating user accounting does not relate to using a server to send spam.

105. The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

A. contents are highly volatile.

B. data cannot be backed up.

C. data can be copied.

D. device may not be compatible with other peripherals.

Answer: C. data can be copied.

Explanation: Unless properly controlled, flash memory provides an avenue anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

106. The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.

B. increased redundancy.

C. unauthorized accesses.

D. application malfunctions.

Answer: B. increased redundancy.

Explanation: Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy (Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional, otherwise unnecessary, data handling efforts.) Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

107. Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and non-business materials.

B. maximize employee performance.

C. safeguard the organization's image.

D. assist the organization in preventing legal issues

Answer: A. protect the organization from viruses and non-business materials.

Explanation: The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved); however, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

108. Which of the following is the GREATEST risk related to the monitoring of audit logs?

A. Logs are not backed up periodically.

B. Routine events are recorded.

C. Procedures for enabling logs are not documented.

D. Unauthorized system actions are recorded but not investigated.

Answer: D. Unauthorized system actions are recorded but not investigated.

Explanation: If unauthorized system actions are not investigated, the log is useless. Not backing up logs periodically is a risk, but not as critical as the need to investigate questionable actions. Recording routine events can make it more difficult to recognize unauthorized actions, but the critical events are still recorded. Procedures for enabling and reviewing logs should be documented, but documentation does not ensure investigation.

109. An organization wants to enforce data integrity principles and achieve faster performance/execution in a database application. Which of the following design principles should be applied?

A. User (customized) triggers

B. Data validation at the front end

C. Data validation at the back end

D. Referential integrity

Answer: D. Referential integrity

Explanation: Referential integrity should be implemented at the time of the design of the database to provide a faster execution mechanism. All other options are implemented at the application coding stage.

110. To share data in a multivendor network environment, it is essential to implement program-to-program communication. With respect to program-to-program communication features, that can be implemented in this environment, which of the following makes implementation and maintenance difficult?

A. User isolation

B. Controlled remote access

C. Transparent remote access

D. The network environments

Answer: D. The network environments

Explanation: Depending on the complexity of the network environment, implementation of program-to-program communication features becomes progressively more difficult. It is possible to implement program-to-program communication to isolate a user in the multivendor network. Program-to-program communication can be implemented to control and monitor the files that a user can transfer between systems, and the remote program-to-program communication will be transparent to the end user. All of these are security features.

111. An IS auditor is reviewing the database administration (DBA) function to ascertain whether adequate provision has been made for controlling data. The IS auditor should determine that the:

A. function reports to data processing operations.

B. responsibilities of the function are well defined.

C. database administrator is a competent systems programmer.

D. audit software has the capability of efficiently accessing the database.

Answer: B. responsibilities of the function are well defined.

Explanation: The IS auditor should determine that the responsibilities of the DBA function are not only well defined but also assure that the DBA reports directly to the IS manager or executive to provide independence, authority and responsibility. The DBA should not report to either data processing operations or systems development management. The DBA need not be a competent systems programmer. Choice D is not as important as choice A.

112. Which of the following is a control over database administration activities?

A. A database checkpoint to restart processing after a system failure

B. Database compression to reduce unused space

C. Supervisory review of access logs

D. Backup and recovery procedures to ensure database availability

Answer: C. Supervisory review of access logs

Explanation: To ensure management approval of database administration activities and to exercise control over the use of database tools, there should be a supervisory review of access logs. Database administration activities include among others, database checkpoints, database compression techniques, and data backup and recovery procedures established and implemented to ensure database availability.

113. To maximize the performance of a large database in a parallel processing environment, which of the following is used for separating indexes?

A. Disk partitioning

B. Mirroring

C. Hashing

D. Duplexing

Answer: C. Hashing

Explanation: An essential part of designing a database for parallel processing is the partitioning scheme. Because large databases are indexed, independent indexes must also be partitioned to maximize performance. Hashing is a method used for index partitioning. It associates data to disks based on a hash key. Disk partitioning creates logical drives on the single disk for better management of the contents. Disk mirroring uses two identical disks. All operations on the two disks are performed so that each disk is a mirror image of the other. This provides redundancy in case of failure of one of the disks. Disk duplexing makes use of more than one disk with two separate controllers providing redundancy in case of a disk failure or a controller card failure.

114. Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity

B. Domain integrity

C. Relational integrity

D. Referential integrity

Answer: D. Referential integrity

Explanation: Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables. If this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

115. The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.

B. prevent integrity problems, when two processes attempt to update the same data at the same time.

C. prevent inadvertent or unauthorized disclosure of data in the database.

D. ensure the accuracy, completeness and consistency of data.

Answer: B. prevent integrity problems, when two processes attempt to update the same data at the same time.

Explanation: Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users and controls, such as passwords, prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

116. A referential integrity constraint consists of:

A. ensuring the integrity of transaction processing.

B. ensuring that data are updated through triggers.

C. ensuring controlled user updates to the database.

D. rules for designing tables and queries.

Answer: B. ensuring that data are updated through triggers.

Explanation: Referential integrity constraints ensure that a change in a primary key of one table is automatically updated in the matching foreign keys of other tables. This is done using triggers.

117. Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures

B. Table link/reference checks

C. Query/table access time checks

D. Rollback and rollforward database features

Answer: B. Table link/reference checks

Explanation: Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database) and thus provides the greatest assurance of database integrity. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

118. The database administrator has decided to disable certain normalization controls in the database management system (DBMS) software to provide users with increased query performance. This will MOST likely increase the risk of:

A. loss of audit trails.

B. redundancy of data.

C. loss of data integrity.

D. unauthorized access to data.

Answer: B. redundancy of data.

Explanation: Normalization is the removal of redundant data elements from the database structure. Disabling features of normalization in relational databases will increase the likelihood of data redundancy. Audit trails are a feature of DBMS software that can be lost by not enabling them. These are not connected to normalization controls. The integrity of data is not directly affected by disabling normalization controls. Access to data is set through defining user rights and controlling access to information, and is not affected by normalization controls.

119. In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries

B. Additional staff to provide separation of duties

C. Procedures that verify that only approved program changes are implemented

D. Access controls to prevent the operator from making program modifications

Answer: C. Procedures that verify that only approved program changes are implemented

Explanation: While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited, as suggested in choice B, this practice is not always possible in small organizations. The IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

120. Vendors have released patches fixing security flaws in their software. Which of the following should the IS auditor recommend in this situation?

A. Assess the impact of patches prior to installation.

B. Ask the vendors for a new software version with all fixes included.

C. Install the security patch immediately.

D. Decline to deal with these vendors in the future.

Answer: A. Assess the impact of patches prior to installation.

Explanation: The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions with all fixes included are not always available and a full installation could be time-consuming. Declining to deal with vendors does not take care of the flaw.

121. A programmer, using firecall IDs, as provided in the manufacture's manual, gained access to the production environment and made an unauthorized change. Which of the following could have prevented this from happening?

A. Deactivation

B. Monitoring

C. Authorization

D. Resetting

Answer: D. Resetting

Explanation: The vendor supplied firecall IDs should be reset at the time of implementing the system and new IDs generated. Deactivation may cause the disruption of a critical production job. Without resetting the vendor provided firecall IDs, monitoring and authorization of such IDs are not effective controls.

122. One of the purposes of library control software is to allow:

A. programmers access to production source and object libraries.

B. batch program updating.

C. operators to update the control library with the production version before testing is completed.

D. read-only access to source code.

Answer: D. read-only access to source code.

Explanation: An important purpose of library control software is to allow read-only access to source code. Choices A, B and C are activities which library control software should help to prevent or prohibit.

123. An organization is moving its application maintenance in-house from an outside source. Which of the following should be the main concern of an IS auditor?

A. Regression testing

B. Job scheduling

C. User manuals

D. Change control procedures

Answer: D. Change control procedures

Explanation: It is essential for the maintenance and control of software that change control procedures be in place. Regression testing is completed after changes are made to the software, and since the software is already being used, the job schedule must be in place and may be reviewed later. This change does not affect user manuals and any associated risks.

124. Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports

B. Library control software restricting changes to source code

C. Restricted access to source code and object code

D. Date and time-stamp reviews of source and object code

Answer: D. Date and time-stamp reviews of source and object code

Explanation: Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

125. An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.

B. Make changes to the database after granting access to a normal user account

C. Use the DBA user account to make changes, log the changes and review the change log the following day.

D. Use the normal user account to make changes, log the changes and review the change log the following day.

Answer: C. Use the DBA user account to make changes, log the changes and review the change log the following day.

Explanation: The use of a database administrator (DBA) user account is (should be) normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

126. Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

A. Review software migration records and verify approvals.

B. Identify changes that have occurred and verify approvals.

C. Review change control documentation and verify approvals.

D. Ensure that only appropriate staff can migrate changes into production.

Answer: B. Identify changes that have occurred and verify approvals.

Explanation: The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

127. After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

A. Differential reporting

B. False-positive reporting

C. False-negative reporting

D. Less-detail reporting

Answer: C. False-negative reporting

Explanation: False-negative reporting on weaknesses means the control weaknesses in the network are not identified and, hence, may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

128. The FIRST step in managing the risk of a cyber attack is to:

A. assess the vulnerability impact.

B. evaluate the likelihood of threats.

C. identify critical information assets.

D. estimate potential damage.

Answer: C. identify critical information assets.

Explanation: The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

129. Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits a vulnerability in a protocol?

A. Install the vendor's security fix for the vulnerability.

B. Block the protocol traffic in the perimeter firewall.

C. Block the protocol traffic between internal network segments.

D. Stop the service until an appropriate security fix is installed.

Answer: D. Stop the service until an appropriate security fix is installed.

Explanation: Stopping the service and installing the security fix is the safest way to prevent the worm from spreading. If the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits every software that utilizes it from working between segments

130. Which of the following is the BEST control to detect internal attacks on IT resources?

A. Checking of activity logs

B. Reviewing firewall logs

C. Implementing a security policy

D. Implementing appropriate segregation of duties

Answer: A. Checking of activity logs

Explanation: Verification of individual activity logs will detect the misuse of IT resources. Depending on the configuration, firewall logs can help in detecting attacks passing through the firewall. Implementation of a security policy and segregation of duties are deterrent controls that might prevent the misuse of IT resources.

131. A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

A. Most employees use laptops.

B. A packet filtering firewall is used.

C. The IP address space is smaller than the number of PCs.

D. Access to a network port is not restricted.

Answer: D. Access to a network port is not restricted.

Explanation: Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

132. .An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned, if a hacker:

A. compromises the Wireless Application Protocol (WAP) gateway.

B. installs a sniffing program in front of the server.

C. steals a customer's PDA.

D. listens to the wireless transmission.

Answer: A. compromises the Wireless Application Protocol (WAP) gateway.

Explanation: In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

133. Analysis of which of the following would MOST likely enable the IS auditor to determine if an unapproved program attempted to access sensitive data?

A. Abnormal job termination reports

B. Operator problem reports

C. System logs

D. Operator work schedules

Answer: C. System logs

Explanation: System logs are automated reports that identify most of the activities performed on the computer. Many programs that analyze the system log to report on specifically defined items have been developed. Abnormal job termination reports identify application jobs that were terminated before successful completion. Operator problem reports are used by operators to log computer operations problems and their solutions. Operator work schedules are maintained by IS management to assist in human resource planning..

134. A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies

B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing

C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format

D. Reengineering the existing processing and redesigning the existing system

Answer: C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format

Explanation: EDI is the best Answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls) EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

135. A number of system failures are occurring when ions to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

A. Unit testing

B. Integration testing

C. Design walk-throughs

D. Configuration management

Answer: B. Integration testing

Explanation: A common system maintenance problem is that errors are often ed quickly (especially when deadlines are tight); units are tested by the programmer and then transferred to the acceptance test area; this often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface ly.

136. A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

A. Comparing source code

B. Reviewing system log files

C. Comparing object code

D. Reviewing executable and source code integrity

Answer: B. Reviewing system log files

Explanation: Reviewing system log files is the only trail that may provide information

about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

137. An employee is responsible for updating daily the interest rates in a finance application, including interest rate exceptions for preferred customers. Which of the following is the BEST control to ensure that all rate exceptions are approved?

A. A supervisor must enter his/her password before a rate exception is validated.

B. Rates outside the normal range require prior management approval.

C. The system beeps an alarm when rate exceptions are entered.

D. All interest rates must be logged and verified every 30 days.

Answer: B. Rates outside the normal range require prior management approval.

Explanation: Prior approval of management for rates outside the normal range would be a proper control. Entering the password of a supervisor does not ensure authorization. A system alarm upon entry of a rate exception is only a warning. Logging of exceptions is a detective control..

138. An IS auditor is conducting a review of an application system after users have completed acceptance testing. What should be the IS auditorâ€™s major concern?

A. Determining whether test objectives were documented

B. Assessing whether users documented expected test results

C. Reviewing whether test problem logs were completed

D. Determining if there are unresolved issues

Answer: D. Determining if there are unresolved issues

Explanation :In assessing the overall success or failure of the acceptance test, the IS auditor should determine whether the test plans were documented and whether actual results were compared with expected results as well as review the test problem log to confirm resolution of identified test issues. The IS auditor should then determine the impact of the unresolved issues on system functionality and usability.

139. .By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

A. reliable products are guaranteed.

B. programmers' efficiency is improved.

C. security requirements are designed.

D. predictable software processes are followed.

Answer:D. predictable software processes are followed.

Explanation: By evaluating the organization's development projects against the CMM, the IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

140. Ideally, stress testing should be carried out in a:

A. test environment using test data.

B. production environment using live workloads.

C. test environment using live workloads.

D. production environment using test data.

Answer: C. test environment using live workloads.

Explanation: Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

141. In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handler.

B. EDI translator.

C. application interface.

D. EDI interface.

Answer: A. communications handler.

Explanation: A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs). An EDI translator translates data between the standard format and a trading partner's proprietary format. An application interface moves electronic transactions to or from the application system and performs data mapping. An EDI interface manipulates and routes data between the application system and the communications handler.

142. In an electronic fund transfer (EFT) system, which of the following controls would be useful in detecting a duplication of messages?

A. Message authentication code

B. Digital signature

C. Authorization sequence number

D. Segregation of authorization

Answer: C. Authorization sequence number

Explanation: All of these controls are necessary in an EFT system; however, the authorization sequence number is the control that will detect the duplication of a message. A message authentication code detects unauthorized modifications, a digital signature ensures non-repudiation, and the segregation of the creation of the message and the authorization will avoid dummy messages.

143. Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.

B. transaction journal.

C. automated suspense file listing.

D. user error report.

Answer: B. transaction journal.

Explanation: The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, and the user error report would only list input that resulted in an edit error.

144. Peer reviews to detect software errors during a program development activity are called:

A. emulation techniques.

B. structured walk-throughs.

C. modular program techniques.

D. top-down program construction.

Answer: B. structured walk-throughs.

Explanation: A structured walk-through is a management tool for improving productivity. Structured walk-throughs can detect an in or improper interpretation of the program specifications. This, in turn, improves the quality of system testing and acceptance of it. The other choices are methods or tools in the overall systems development process.

145. The MAJOR concern for an IS auditor reviewing a CASE environment should be that the use of CASE does not automatically:

A. result in a capture of requirements.

B. ensure that desirable application controls have been implemented.

C. produce ergonomic and user-friendly interfaces.

D. generate efficient code.

Answer: A. result in a capture of requirements.

Explanation: The principal concern should be to ensure an alignment of the application with business needs and user requirements. While the CASE being used may provide tools to cover this crucial initial phase, a cooperative user-analyst interaction is always needed. Choice B should be the next concern. If the system meets business needs and user requirements, it should also incorporate all desirable controls. Controls have to be specified since CASE can only automatically incorporate certain, rather low-level, controls (such as type of input data, e.g., date, expected). CASE will not (choice C) automatically generate ergonomic and user-friendly interfaces, but it should provide tools for easy (and automatically documented) tuning. CASE applications (choice D) generally come short of optimizing the use of hardware and software resources, precisely because they are designed to optimize other elements, such as developers' effort or documentation.

146. The request for proposal (RFP) for the acquisition of an application system would MOST likely be approved by the:

A. project steering committee.

B. project sponsor.

C. project manager.

D. user project team.

Answer: A. project steering committee.

Explanation: A project steering committee usually consists of a senior representative from each function that will be affected by the new system and would be the most appropriate group to approve the RFP. The project sponsor provides funding for the project. The project manager and user project team are responsible for drafting the RFP.

147. The use of a GANTT chart can:

A. aid in scheduling project tasks.

B. determine project checkpoints.

C. ensure documentation standards.

D. direct the post implementation review.

Answer: A. aid in scheduling project tasks.

Explanation: A GANTT chart is used in project control. It may aid in the identification of needed checkpoints, but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the postimplementation review.

148. Which of the following is a characteristic of timebox management? It:

A. is not suitable for prototyping or rapid application development (RAD).

B. eliminates the need for a quality process.

C. prevents cost overruns and delivery delays.

D. separates system and user acceptance testing.

Answer: C. prevents cost overruns and delivery delays.

Explanation: Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

149. Which of the following is an implementation risk within the process of decision support systems?

A. Management control

B. Semistructured dimensions

C. Inability to specify purpose and usage patterns

D. Changes in decision processes

Answer: C. Inability to specify purpose and usage patterns

Explanation: The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

150. Which of the following is the FIRST step in a business process reengineering (BPR) project?

A. Defining the areas to be reviewed

B. Developing a project plan

C. Understanding the process under review

D. Reengineering and streamlining the process under review

Answer: A. Defining the areas to be reviewed

Explanation: On the basis of the evaluation of the entire business process, ly defining the areas to be reviewed is the first step in a BPR project. On the basis of the definition of the areas to be reviewed, the project plan is developed. Understanding the process under review is important, but the subject of the review must be defined first. Thereafter, the process can be reengineered, streamlined, implemented and monitored for continuous improvement.

151. Which of the following is used to ensure that batch data is completely and accurately transferred between two systems?

A. Control total

B. Check digit

C. Check sum

D. Control account

Answer: A. Control total

Explanation: A control total is frequently used as an easily recalculated control. The number of invoices in a batch or the value of invoices in a batch are examples of control totals. They provide a simple way of following an audit trail from a general ledger summary item to an individual transaction, and back. A check digit is a method of verifying the accuracy of a single data item, such as a credit card number. Although a check sum is an excellent control over batch completeness and accuracy, it is not easily recalculated and, therefore, is not as commonly used in financial systems as a control total. Check sums are frequently used in data transfer as part of encryption protocols. Control accounts are used in financial systems to ensure that components that exchange summary information, such as a sales register and a general ledger, can be reconciled.

152. Which of the following should be included in a feasibility study for a project to implement an EDI process?

A. The encryption algorithm format

B. The detailed internal control procedures

C. The necessary communication protocols

D. The proposed trusted third-party agreement

Answer: C. The necessary communication protocols

Explanation: Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as

there may be significant cost implications, if new hardware and software are involved, and risk implications, if the technology is new to the organization.

153. A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house-developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.

B. A quality plan is not part of the contracted deliverables.

C. Not all business functions will be available on initial implementation.

D. Prototyping is being used to confirm that the system meets business requirements.

Answer: B. A quality plan is not part of the contracted deliverables.

Explanation: A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

154. A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders

B. Logging all customer orders in the ERP system

C. Using hash totals in the order transmitting process

D. Approving (production supervisor) orders prior to production

Answer: A. Verifying production to customer orders

Explanation: Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time-consuming, manual process that does not guarantee proper control.

155. A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification

B. One-for-one checking

C. Manual recalculations

D. Functional acknowledgements

Answer: D. Functional acknowledgements

Explanation: Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

156. A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be the IS auditor's main concern about the new process?

A. Are key controls in place to protect assets and information resources?

B. Does it address the corporate customer requirements?

C. Does the system meet the performance goals (time and resources)?

D. Have owners been identified who will be responsible for the process?

Answer: A. Are key controls in place to protect assets and information resources?

Explanation: The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the BPR process should achieve, but they are not the auditor's primary concern.

157. A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

A. payroll reports should be compared to input forms.

B. gross payroll should be recalculated manually.

C. checks (cheques) should be compared to input forms.

D. checks (cheques) should be reconciled with output reports.

Answer: A. payroll reports should be compared to input forms.

Explanation: The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

158. A data validation edit that matches input data to an occurrence rate is a:

A. limit check.

B. reasonableness check.

C. range check.

D. validity check.

Answer: B. reasonableness check.

Explanation: A reasonableness check is an edit check, wherein input data are matched to predetermined reasonable limits or occurrence rates. Limit checks verify that data do not exceed a predetermined amount. Range checks verify that data are within a predetermined range of values. Validity checks test for data validity in accordance with predetermined criteria.

159. A data warehouse is:

A. object-oriented.

B. subject-oriented.

C. departmental specific.

D. a volatile database

Answer: B. subject-oriented.

Explanation: Data warehouses are subject-oriented. The data warehouse is meant to help make decisions when the function(s) to be affected by the decision transgresses across departments within an organization. They are nonvolatile. Object orientation and volatility are irrelevant to a data warehouse system.

160. A debugging tool, which reports on the sequence of steps executed by a program, is called a(n):

A. output analyzer.

B. memory dump.

C. compiler.

D. logic path monitor.

Answer: D. logic path monitor.

Explanation: Logic path monitors report on the sequence of steps executed by a program. This provides the programmer with clues to logic errors, if any, in the program. An output analyzer checks the results of a program for accuracy by comparing the expected results with the actual results. A memory dump provides a picture of the content of a computer's internal memory at any point in time, often when the program is aborted, thus providing information on inconsistencies in data or parameter values. Though compilers have some potential to provide feedback to a programmer, they are not generally considered a debugging tool.

161. A decision support system (DSS):

A. is aimed at solving highly structured problems.

B. combines the use of models with nontraditional data access and retrieval functions.

C. emphasizes flexibility in the decision-making approach of users.

D. supports only structured decision-making tasks.

Answer: C. emphasizes flexibility in the decision-making approach of users.

Explanation: DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less-structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi-structured decision-making tasks.

162. Which of the following is a check (control) for completeness?

A. Check digits

B. Parity bits

C. One-for-one checking

D. Prerecorded input

Answer: B. Parity bits

Explanation: Parity bits are used to check for completeness of data transmissions. Choice A is in because check digits are a control check for accuracy. Choice C is in because, in one-for-one checking, individual documents are matched to a detailed listing of documents processed by the computer, but do not ensure that all documents have been received for processing. Choice D (prerecorded input) is a data file control for which selected information fields are preprinted on blank input forms to reduce the chance of input errors.

163. Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit

B. Existence check

C. Completeness check

D. Reasonableness check

Answer: C. Completeness check

Explanation: A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

164. Which of the following types of controls is designed to provide the ability to verify data and record values through the stages of application processing?

A. Range checks

B. Run-to-run totals

C. Limit checks on calculated amounts

D. Exception reports

Answer: B. Run-to-run totals

Explanation: Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer were accepted and then applied to the updating process.

165. The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.

B. central processing site during the running of the application system.

C. remote processing site after transmission of the data to the central processing site.

D. remote processing site prior to transmission of the data to the central processing site.

Answer: D. remote processing site prior to transmission of the data to the central processing site.

Explanation: It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

166. To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparation.

B. in transit to the computer.

C. between related computer runs.

D. during the return of the data to the user department.

Answer: A. during data preparation.

Explanation: During data preparation is the bestAnswer, because it establishes control at the earliest point.

167. Functional acknowledgements are used:

A. as an audit trail for EDI transactions.

B. to functionally describe the IS department.

C. to document user roles and responsibilities.

D. as a functional description of application software.

Answer: A. as an audit trail for EDI transactions.

Explanation: Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

168. The impact of EDI on internal controls will be:

A. that fewer opportunities for review and authorization will exist.

B. an inherent authentication.

C. a proper distribution of EDI transactions while in the possession of third parties.

D. that IPF management will have increased responsibilities over data center controls.

Answer: A. that fewer opportunities for review and authorization will exist.

Explanation: EDI promotes a more efficient paperless environment, but at the same time, less human intervention makes it more difficult for reviewing and authorizing. Choice B is in; since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the

source and does not include any distinguishing human element or signature. Choice C is in because this is a security risk associated with EDI. Choice D is in because there are relatively few, if any, additional data center controls associated with the implementation of EDI applications. Instead, more control will need to be exercised by the user's application system to replace manual controls, such as site reviews of documents. More emphasis will need to be placed on control over data transmission (network management controls).

169. Sales orders are automatically numbered sequentially at each of a retailer's multiple outlets. Small orders are processed directly at the outlets, with large orders sent to a central production facility. The MOST appropriate control to ensure that all orders transmitted to production are received and processed would be to:

A. send and reconcile transaction counts and totals.

B. have data transmitted back to the local site for comparison.

C. compare data communications protocols with parity checking.

D. track and account for the numerical sequence of sales orders at the production facility.

Answer: A. send and reconcile transaction counts and totals.

Explanation: Sending and reconciling transaction totals not only ensure that the orders were received, but also processed by the central production location. Transmission back to the local site confirms that the central location received it, but not that they have actually processed it. Tracking and accounting for the numerical sequence only confirms what orders are on hand, and not whether they actually have been completed. The use of parity checking would only confirm that the order was not changed during transmission.

170. Which of the following ensures completeness and accuracy of accumulated data?

A. Processing control procedures

B. Data file control procedures

C. Output controls

D. Application controls

Answer: A. Processing control procedures

Explanation: Processing controls ensure the completeness and accuracy of accumulated data, for example, editing and run-to-run totals. Data file control procedures ensure that only authorized processing occurs to stored data, for example, transaction logs. Output controls ensure that data delivered to users will be presented, formatted and delivered in a consistent and secure manner, for example, using report

distribution. "Application controls" is a general term comprising all kinds of controls used in an application.

171. A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness check.

B. parity check.

C. redundancy check.

D. check digits.

Answer: C. redundancy check.

Explanation: A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

172. Which of the following integrity tests examines the accuracy, completeness, consistency and authorization of data?

A. Data

B. Relational

C. Domain

D. Referential

Answer: A. Data

Explanation: Data integrity testing examines the accuracy, completeness, consistency and authorization of data. Relational integrity testing detects modification to sensitive data by the use of control totals. Domain integrity testing verifies that data conforms to specifications. Referential integrity testing ensures that data exists in its parent or original file before it exists in the child or another file.

173. Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check

B. Check digit

C. Validity check

D. Duplicate check

Answer: B. Check digit

Explanation: A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered, e.g., an in, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

174. Which of the following data validation edits could be used by a bank, to ensure the ness of bank account numbers assigned to customers, thereby helping to avoid transposition and transcription errors?

A. Sequence check

B. Validity check

C. Check digit

D. Existence check

Answer: C. Check digit

Explanation: A check digit is a mathematically calculated value that is added to data to ensure that the original data have not been altered. This helps in avoiding transposition and transcription errors. Thus, a check digit can be added to an account number to check for accuracy. Sequence checks ensure that a number follows sequentially and any out of sequence or duplicate control numbers are rejected or noted on an exception report. Validity checks and existence checks match data against predetermined criteria to ensure accuracy.

175. During an application audit, the IS auditor finds several problems related to corrupted data in the database. Which of the following is a ive control that the IS auditor should recommend?

A. Implement data backup and recovery procedures.

B. Define standards and closely monitor for compliance.

C. Ensure that only authorized personnel can update the database.

D. Establish controls to handle concurrent access problems.

Answer: A. Implement data backup and recovery procedures.

Explanation: Implementing data backup and recovery procedure is a ive control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, and monitoring for

compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is a preventive control.

176. An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.

B. Implement before-and-after image reporting.

C. Use tracing and tagging.

D. Implement integrity constraints in the database.

Answer: D. Implement integrity constraints in the database.

Explanation: Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

177. When assessing the portability of a database application, the IS auditor should verify that:

A. a structured query language (SQL) is used.

B. information import and export procedures exist with other systems.

C. indexes are used.

D. all entities have a significant name and identified primary and foreign keys.

Answer: A. a structured query language (SQL) is used.

Explanation: The use of an SQL is a key element for database portability. Import and export of information with other systems is an objective of a database interfaces review. The use of an index is an objective of a database access review, and the fact that all entities have a significant name and identified primary and foreign keys is an objective of a database design review.

178. In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.

B. consistency.

C. atomicity.

D. durability.

Answer:C. atomicity.

Explanation: The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions, and hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

179. Which of the following would help to ensure the portability of an application connected to a database? The:

A. verification of database import and export procedures.

B. usage of a structured query language (SQL).

C. analysis of stored procedures/triggers.

D. synchronization of the entity-relation model with the database physical schema.

Answer: B. usage of a structured query language (SQL).

Explanation: The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

180. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

A. Encrypting the hash of the payment instruction with the public key of the financial institution

B. Affixing a time stamp to the instruction and using it to check for duplicate payments

C. Encrypting the hash of the payment instruction with the private key of the instructor

D. Affixing a time stamp to the hash of the instruction before having it digitally signed by the instructor

Answer: B. Affixing a time stamp to the instruction and using it to check for duplicate payments

Explanation: Affixing a time stamp to the instruction and using it to check for duplicate payments makes the instruction unique. The financial institution can check that the instruction was not intercepted and replayed, and thus, it could prevent crediting the account three times. Encrypting the hash of the payment instruction with the public key of the financial institution does not protect replay, it only protects confidentiality and integrity of the instruction. Encrypting the hash of the payment instruction with the private key of the instructor ensures integrity of the instruction and non-repudiation of the issued instruction. The process of creating a message digest requires applying a cryptographic hashing algorithm to the entire message. The receiver, upon decrypting the message digest, will re-compute the hash using the same hashing algorithm and compare the result with what was sent. Hence, affixing a time stamp into the hash of the instruction before being digitally signed by the instructor would violate the integrity requirements of a digital signature.

181. An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

A. Analyze the need for the structural change.

B. Recommend restoration to the originally designed structure.

C. Recommend the implementation of a change control process.

D. Determine if the modifications were properly approved.

Answer: D. Determine if the modifications were properly approved.

Explanation: The IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the auditor find that the structural modification had not been approved.

182. An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

A. Consistency

B. Isolation

C. Durability

D. Atomicity

Answer: D. Atomicity

Explanation: Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends. Isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

183. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

Answer: C. preparing simulated transactions for processing and comparing the results to predetermined results.

Explanation: Preparing simulated transactions for processing and comparing the results to pre determined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

184. An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized software.

B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.

C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.

D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Answer: C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.

Explanation: The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. The IS auditor must convince the user and user management of the risk and the

need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

185. Which of the following is the GREATEST challenge in using test data?

A. Ensuring the program version tested is the same as the production program

B. Creating test data that covers all possible valid and invalid conditions

C. Minimizing the impact of additional transactions on the application being tested

D. Processing the test data under an auditor's supervision

Answer: B. Creating test data that covers all possible valid and invalid conditions

Explanation: The effectiveness of test data is determined by the comprehensiveness of the coverage of all the key controls to be tested. If the test data does not cover all valid and invalid conditions, there is a risk that relevant control weakness may remain undetected. Changes in the program, for the period covered under audit, may have been done to remove bugs or for additional functionalities. However, as the test data approach involves testing of data for the audit period, changes in the program tested may have minimal impact. Applications with current technology are usually not impacted by additional transactions. Test data are developed by the auditor; however, processing does not have to be under an auditor's supervision, since the input data will be verified by the outputs.

186. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs.

B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.

D. automatic flowcharting and analysis of the source code of the calculation programs.

Answer: C. preparing simulated transactions for processing and comparing the results to predetermined results.

Explanation: Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

187. Which of the following would BEST support 24/7 availability?

A. Daily backup

B. Offsite storage

C. Mirroring

D. Periodic testing

Answer: C. Mirroring

Explanation: Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

188. The PRIMARY purpose of implementing Redundent Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.

B. provide user authentication.

C. ensure availability of data.

D. ensure the confidentiality of data.

Answer: C. ensure availability of data.

Explanation: RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk. If disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

189. Which of the following is the MOST important criterion for the selection of a location for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.

B. given the same level of protection as that of the computer data center.

C. outsourced to a reliable third party.

D. equipped with surveillance capabilities.

Answer: A. physically separated from the data center and not subject to the same risks.

Explanation: It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other

choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

190. If a database is restored using before-image dumps, where should the process be started following an interruption?

A. Before the last transaction

B. After the last transaction

C. As the first transaction after the latest checkpoint

D. As the last transaction before the latest checkpoint

Answer: A. Before the last transaction

Explanation: If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

191. In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

A. Maintaining system software parameters

B. Ensuring periodic dumps of transaction logs

C. Ensuring grandfather-father-son file backups

D. Maintaining important data at an offsite location

Answer: B. Ensuring periodic dumps of transaction logs

Explanation: Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

192. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

A. The previous day's backup file and the current transaction tape

B. The previous day's transaction file and the current transaction tape

C. The current transaction tape and the current hard copy transaction log

D. The current hard copy transaction log and the previous day's transaction file

Answer: A. The previous day's backup file and the current transaction tape

Explanation: The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

193. An offsite information processing facility:

A. should have the same amount of physical access restrictions as the primary processing site.

B. should be easily identified from the outside so that, in the event of an emergency, it can be easily found.

C. should be located in proximity to the originating site, so it can quickly be made operational.

D. need not have the same level of environmental monitoring as the originating site.

Answer: A. should have the same amount of physical access restrictions as the primary processing site.

Explanation: An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site, and the offsite facility should possess the same level of environmental monitoring and control as the originating site.

194. An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.

B. regular hardware maintenance is performed.

C. offsite storage of transaction and master files exists.

D. backup processing facilities are fully tested.

Answer: C. offsite storage of transaction and master files exists.

Explanation: Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

195. Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

A. Reviewing program code

B. Reviewing operations documentation

C. Turning off the UPS, then the power

D. Reviewing program documentation

Answer: B. Reviewing operations documentation

Explanation: Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

196. A company performs full backup of data and programs on a regular basis. The primary purpose of this practice is to:

A. maintain data integrity in the applications.

B. restore application processing after a disruption.

C. prevent unauthorized changes to programs and data.

D. ensure recovery of data processing in case of a disaster.

Answer: B. restore application processing after a disruption.

Explanation: Backup procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Backup procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures are a necessary part of the recovery process following a disaster, they are not sufficient in themselves.

197. Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.

B. Paper documents are also stored in the offsite vault.

C. Data files that are stored in the vault are synchronized.

D. The offsite vault is located in a separate facility.

Answer: C. Data files that are stored in the vault are synchronized.

Explanation: Choice A is in because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not because the IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

198. Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.

B. validation checks.

C. input controls.

D. database commits and rollbacks.

Answer: D. database commits and rollbacks.

Explanation: Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

199. When developing a backup strategy, the FIRST step is to:

A. identify the data.

B. select the storage location.

C. specify the storage media.

D. define the retention period.

Answer: A. identify the data.

Explanation: Archiving data and backups is essential for the continuity of business. Selection of the data to be backed up is the first step in the process. Once the data have been identified, an appropriate retention period, storage media and location can be selected.

200. To provide protection for media backup stored at an offsite location, the storage site should be:

A. located on a different floor of the building.

B. easily accessible by everyone.

C. clearly labeled for emergency access.

D. protected from unauthorized access.

Answer: D. protected from unauthorized access.

Explanation: The offsite storage site should always be protected against unauthorized accesses and at least have the same security requirements as the primary site. Choice A is in because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.