# CISA NOTES

*Powered by madunix*

V1.0

*https://www.experts-exchange.com/members/madunix*

*https://www.linkedin.com/in/madunix*

**Best control** would be provided by having the production control group copy the source program to the production libraries and then compile the program.

**Decision Support** will be enhanced by using a data warehouse and data marts.

Primary objective of value delivery is to: **optimize security investments in support of business objectives.**

The MOST robust method for disposing of magnetic media = **Destroying**

**Data warehousing** involves data cleaning, data integration, and data consolidations.

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

**Fault=ST LOSS POWER Spike=ST HIGH Volt Sag=ST LOW Volt**

**Brownout=LT LOW Volt Surge=LT HIGH Volt Blackout= LT LOSS POWER**

The GREATEST challenge of performing a **quantitative risk analysis**; Obtaining accurate figures on the frequency of specific threats

**IDS** cannot detect attacks within encrypted traffic and it would be a concern if someone were misinformed and thought that the IDS could detect attacks in encrypted traffic.

**Standard establishes mandatory** rules, specifications and metrics used to measure compliance against quality, value, etc. Standards are usually intended for compliance purposes and to provide assurance to others who interact with a process or outputs of a process.

The board of directors and executive officers are accountable for the functionality, reliability, and security within **IT Governance**.

Web application attack facilitates unauthorized access to a database= **SQLI**

Regression testing is undertaken PRIMARILY to ensure that: **applied changes have not introduced new errors.**

**Capacity monitoring** the primary objective is to ensure compliance with the internal SLA between the business and IT, helps in arriving at expected future capacity based on usage patterns, helps in initiating procurement based on the current usage and expected future capacity.

**Cryptographic hash** is a primary defense against alteration attacks.

**Variable sampling** would be the best sampling technique to review an organization's balance sheet for material transactions. It is also known as dollar estimation.

**Integrity of data** = information are changed only in a specified and authorized manner

**CSA** highlight noncompliance to the current policy

**Batch control reconciliations** is a compensatory control for mitigating risk of inadequate segregation of duties

**RFID** = Any RFID signal you can read can be duplicated = Issues of privacy

**Concurrency control** manages simultaneous access to a database. It prevents two users from editing the same record at the same time and also serializes transactions for backup and recovery.

The first criteria must be to ensure that there is no **ambiguity** in the procedures and that, from a security perspective, they meet the applicable standards and, therefore, comply with policy.

The **information security manager** is responsible for developing a security strategy based on business objectives with help of business process owners.

**Load balancing** best ensures uninterrupted system availability by distributing traffic across multiple servers. Load balancing helps ensure consistent response time for web applications

The IS Auditor's main responsibility during the test of the plan is to act as an **observer** to the success of being able to resume timely business processing.

The IS **Auditor's observations** should be documented, analyzed with appropriate recommendations brought forth to management.

The level of effectiveness of employees will be determined by their existing knowledge and capabilities, in other words, their **proficiencies**.

Reviewing the access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system (**During a postimplementation**)

Supports the prioritization of new IT projects = **Investment portfolio analysis**

**Information security** is not only a technical issue, but also a business and governance challenge that involves risk management, reporting and accountability. Effective security requires the active engagement of executive management.

The **warm site** is acceptable to the business when the downtime is acceptable without breaching any legal requirements. Making a profit is not the reason for using a warm site.

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.

One of the features of **referential integrity** checking occurs when a record is deleted and all other referenced records are automatically deleted.

**RFID RISKS** = Business process risk + Business intelligence risk + Privacy risk + Externality risk

**Re-engineering** = reusing design and program components

Real-time application system = **transaction log**

**RACI chart** = responsibility assignment Matrix

**Information systems security policies** are used as the framework for developing logical access controls.

One way to remove data remanence is with a **degausser**

**Proactive management** means anticipating problems in advance and readying with solutions, and providing automation plans for the help desk.

**Audit program**— A step-by-step set of audit procedures and instructions that should be performed to complete an audit

**Cloud bursting** is an application deployment model in which an application runs in a private cloud or data center and bursts into a public cloud when the demand for computing capacity spikes

Ordering of biometric devices with the best response times and lowest EERs are palm, hand, iris, retina, fingerprint and voice, respectively. (**PH-I-RF-V**)

**Cloud bursting** for load balancing between clouds

To detect lost transactions **– automated systems balancing** could be used.

**Cloud bursting** is an application deployment model in which an application runs in a private cloud or data center and bursts into a public cloud when the demand for computing capacity spikes

Relative humidity (RH) is defined as the amount of moisture in the air at a given temperature in relation to the maximum amount of moisture the air could hold at the same temperature. In a data center or computer room, maintaining ambient relative humidity levels between **45% and 55%** is recommended for optimal performance and reliability.

It is a generally agreed upon standard in the computer industry that expensive IT equipment should not be operated in a computer room or data center where the ambient room **temperature has exceeded 85°F (30°C).**

Information gathering techniques – Brainstorming, Delphi technique, Interviewing, Root cause analysis
Quality Assurance is also a root-cause analysis process. Fishbone diagram/Ishikawa: Determines how various factors linked to potential problems or effects, it's majorly referred as "**root cause" analysis**.

**Network slow** = use a protocol analyzer to perform network analysis and review error logs of local area network (LAN) equipment.

**Threat is not vulnerability**. A threat exploits a vulnerability e.g. weak password (vulnerability) is exploited by a dishonest employee (threat) to commit fraud leading to financial losses

**Substantive testing** obtains audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period

**Batch controls**: total menetary amount, total items, total documents, hash totals

**Matrix organizational** structure combines functional and product departmentalization, creates a dual reporting structure, and is optimal where product groups are necessary.

**Corporate governance** consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of an organization's overall governance program. Risk management, reporting, and accountability are central features of these policies and internal controls

**Prototyping**: The process of quickly putting together a working model (a prototype) in order to test various aspects of a design, illustrate ideas or features and gather early user feedback.

**Unsuccessful logon** = monitored by the security administrator.

**The majority of project risk** can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with this risk.

**Frame Relay is more efficient than X.25**

**ATM is asynchronous**, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell

**Hash totals:** Verification that the total in a batch agrees with the total calculated by the system.

**The IS auditor** has an obligation to the project sponsor and the organization to advise on appropriate project management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

**Race conditions** occur due to interferences caused by the following conditions: Sequence or nonatomic + Deadlock, live lock, or locking failure.

**Prior to implementing new technology**, an organization should perform a risk assessment, which would then be presented to business unit management for review and acceptance

**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.

**Penetration test** is normally the only security assessment that can link vulnerabilities together by exploiting them sequentially.

**What is the difference between the false acceptance rate and false rejection rate?**
False acceptance means unauthorized user is permitted access= FAR-UP
False rejection is when authorized person is denied access= FRR- AD

**IaaS:** company is trying to reduce it's sever environment footprint, so the in-house application servers were moved to another location, hosted by a 3rd party. So the application software, application servers were being moved and supported by another company which is IaaS.

**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.

**VPN** = data confidentiality

An **Audit charter** should state management's objectives for and delegation of authority to IS auditors.

Provisioning access to data on a need-to-know basis PRIMARILY ensures **Data confidentiality**

**face to face communications** are an example of informal methods of monitoring and controlling a system development life cycle project since it is hard to document the communication all the time. Evidence is hard in informal methods

**LOG** can be maintained in a manual or automated form where activities are logged with a sequential control number for tracking purposes.

**ESCROW:** The client is entitled to the benefit of only using the software and not owning it, unless they pay more money. Escrow may provide some protection if the vendor goes out of business, but does not prevent software from being discontinued.

**4GL** provides screen-authoring and report-writing utilities that automate database access.

**4GL** tools do not create the business logic necessary for data transformation.

**Flowchart** is used to document internal program logic.

**Feasibility study** = should be the basis for management's decision to buy available software or to build a custom software application

**Recovery managers** should be rotated to ensure the experience of the recovery plan DRP is spread among the managers.

**Entity-relationship diagram** (ERD) is used to help define the database schema.

**Function point analysis** is used for estimation of work during the feasibility study.

**Parallel migration** increases support requirements but lowers the overall risk. The old and new systems are run in parallel to verify integrity while building user familiarity with the new system.

**Phased Changeover** In larger systems, converting to the new system in small steps or phases may be possible. This may take an extended period of time. The concept is best suited to either an upgrade of an existing system, or to the conversion of one department at a time. The phased approach creates a support burden similar to that of parallel operation. A well-managed phased changeover presents a moderate level of risk.

**Data-oriented databases (DODBs)** are designed for predictable data that has a consistent structure and a known or fixed length.

**Object-oriented databases (OODBs)** are designed for data that has a variety of possible data formats.

**Hard Changeover** In certain environments, executing an abrupt change to the new system may be necessary. This is known as a hard changeover, a full change occurring at a particular cutoff date and time. The purpose is to force migration of all the users at once. A hard changeover may be used after successful parallel operation or in times of emergency

**Checklists** are an example of a formal method of communication between the affected parties. A checklist provides guidelines for reviewing functions and activities for assurance and evaluative purposes. Checklists can detect whether activities were performed according to plans, policies, and procedures

**Agile** method places greater reliance on the undocumented knowledge contained in a person's head. Agile is the direct opposite of capturing knowledge through project documentation.

in the SDLC, **Approval by management to proceed to the next phase or possibly kill the project;** i.e. The review at the end of every SDLC phase is intended to prevent the project from proceeding unless it receives management's approval.

The **ACID** principle of database transaction refers to atomicity (all or nothing), consistency, isolation (transactions operate independently), and durability (data is maintained).

Major activities in **software quality assurance** include project management, software verification and validation, software configuration management, and software quality assurance. These activities become a baseline and any subsequent changes require management approvals. Proposed changes are compared to the baseline, which is the standard.

**Opportunity costs** are those costs inherent in selecting one option in favor of another. When a software package's implementation is delayed, inherent costs of other projects being deferred during its implementation is an example of opportunity cost. The time lost due to delayed implementation of a current project could have been applied to developing a new project. Opportunity costs are hard to quantify precisely, but can be among the most important factors in software selection

**Maintenance costs** are the costs to update and adapt software to match changing organizational needs. The maintenance costs of a system will vary widely, depending upon such factors as the type of application, the complexity of the system, and the need for periodic updates

If the database is not **normalized,** the IS auditor should review the justification since, in some situations, denormalization is recommended for performance reasons. The IS auditor should not recommend normalizing the database until further investigation takes place. Reviewing the conceptual data model or the stored procedures will not provide information about normalization.

**Spoofing** is a form of impersonation where one computer tries to take on the identity of another computer. When an attack originates from the external network, but uses an internal network address, the attacker is most likely trying to bypass firewalls and other network security controls by impersonating (or spoofing) the payroll server's internal network address.

**DoS attack** is designed to limit the availability of a resource and is characterized by a high number of requests which require response from the resource (usually a web site). The target spends so many resources responding to the attack requests that legitimate requests are not serviced.

**An application-layer gateway, or proxy firewall, and stateful inspection firewalls** provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

**Control objectives are developed to achieve acceptable levels of risk**. To the extent that is achieved is a good measure of the effectiveness of the strategy.

**Attribute sampling** is the primary sampling method used for compliance testing.

**Social engineering include** : impersonation through a telephone call, dumpster diving and shoulder surfing.

**Downtime reports**: Track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or other anomalous conditions are identified in a downtime report.

The first step in implementing information security governance is to define the **security strategy** based on which security baselines are determined

Risk created by **a reciprocal agreement** for disaster recovery = may result in hardware and software incompatibility

The **service delivery objective** (SDO) is the level of service to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs = **the minimum acceptable operational capability**.

**Assigning accountability** to individuals is most likely to ensure that duties are properly carried out.

An **Uninterruptible Power Supply (UPS)** system is a backup power system that utilizes batteries to provide short-term power when a power losses such as a black out or a brownout is detected. Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.

**Surge protectors** are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.

**Background checks** of prospective employees best prevents attacks from originating within an organization.

There are two modes for biometric recognition: **verification and identification**. In verification, an identity is claimed and the comparison process is limited to checking the reference corresponding to this identity. In identification, no claim of identity is necessary and the system searches its reference database to find if a stored reference matches the biometric characteristics recorded.

**Generator is used when a continuous power supply is needed in power loss situations** and is activated when a loss in power is detected. It does not protect electrical components from spikes in the power line.

**IT assets inventory** is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IT infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

**Outsourcing of some information security activities** can cut costs and increase resources for other security activities in a proactive manner, as can automation of some security procedures

**IT steering Committee** - The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives

**Change control board (CCB):** A management review to ensure awareness and management control of changes in the IT environment.

**Abrupt change over** – stop the existing system abruptly to shift over to new one

**Phased change over** – Both are run but output of both the systems is used since functions performed are different.

**Parallel change over** – Both systems are run simultaneously for a period of time and output of

**Emissions** can be detected by sophisticated equipment and displayed, thus giving access to data to unauthorized persons. They should not cause disruption of CPUs or effect noise pollution

**Hardening** a system means to configure it in the most secure manner (install latest security patches, properly define 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

**Pilot conversion** involves setting up the new system for a small group of users and participants, while the remaining majority of users and participants still interact with the current system. At some pre-determined period in time, the pilot system is installed for all users and participants and the current system is then switched off.

**Mandatory access controls MAC** are filters that cannot be altered by normal users and data owners, and they act by default to enforce a base level of security

**Privilege escalation attack** in the question I asked is a type of attack where higher level system authority is obtained by various methods in this example the task scheduler service runs with administrator permissions and a security flaw allows programs launched by the scheduler to run at the same permission level

**Non-repudiation**—The assurance that a party cannot later deny originating data, that is, the provision of proof of the integrity and origin of the data that can be verified by a third party. A digital signature can provide non-repudiation.

To address an organization's disaster recovery requirements, backup intervals should not exceed the: **RPO**

**Resource Management:** the optimal investment it, and the proper management of, critical IT resources: applications, information, infrastructure and people

Multiple components (N) have at least one (+1) independent backup component available = **N+1**

**Ad hoc networks** are a dynamic grouping of devices in ever-changing configurations. Imagine the wireless devices connecting via Bluetooth when you enter a coffee shop, client's office, or your own automobile. As you move though your activities each day, the configuration of this overall network is changing. Ad hoc means unstructured and ever changing.

When an organization is outsourcing their information security function, which of the following should be kept in the organization; **Accountability for the corporate security policy**

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); **References from other customers**

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider: **agrees to be subject to external security reviews.**

**Segregation of Duties** = Compensating Controls

**Incident response**: A response is required for skilled individuals to deal with technical problems or the failure of internal controls. When the cost of control is more than the cost of the risk, **the risk should be accepted.** Transferring, treating or terminating the risk is of limited benefit if the cost of that control is more than the cost of the risk itself.

The purpose of **the audit committee** is to provide advice to the executive accounting officer concerning internal control strategies, priorities, and assurances.

The **audit committee** manages planned audit activities and the results of both internal and external audits. The committee is authorized to engage outside experts for independent assurance.

**Inherent risk**: These are natural or built-in risks that always exist.

**Detection risks**: these are the risks that an auditor will not be able to detect what is being sought. It would be terrible to report no negative results when material condition (faults) actually exist. Detection risks include sampling and nonsampling risks.

**Sampling risks:** these are the risks that an auditor will falsely accept or erroneously reject an audit sample (evidence).

**Nonsampling risks**: these are the risks that an auditor will fail to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objective (detection fault)

Data transmitted between the biometric scanners and the access control system should use a securely encrypted tunnel to protect the **confidentially of the biometric data**.

To maximize the value an organization obtains from its **BI initiatives**, an effective BI governance process needs to be in place.

**Control risks**: that an auditor loses control, errors could be introduced, or errors may not be corrected in a timely manner.

**Business risks**: these are risks that are inherent in the business or industry itself (regulatory, contractual, financial)

**Technological risks**: these are inherent risks of using automated technology

**Operational risks:** these are the risks that a process or procedure will not perform correctly

**Residual risks:** these are the risks that remain after all mitigation efforts are performed

**Audit risks**: the combination of inherent, detection, control , and residual risks. These are the same risks facing normal business operations.

No computers or IT systems in places – **Cold Site**

Yes Computers or IT systems are in place but partially configured network – **Warm site**

Taking real time backup of applications – **Hot site** (Note: key word here is backup)

Taking real time replication of data – **Mirrored site** (Note: Key word here is replication)

**Bottom-up vs. a top-down** = errors in critical modules are detected earlier.

**Remote processing** site prior to transmission of the data to the central processing site

**Mapping** identifies specific program logic that has not been tested and analyzes programs during execution to indicate whether program statements have been executed

**Check digit** = detect data transposition errors

To ensure that all patches applied went through the change control process, it is necessary to use the **operating system (OS) patch logs** as a starting point and then check to see if change control documents are on file for each of these changes

If the RPO is low, data mirroring should be implemented as the **data recovery strategy**

Is developed for the organization as a whole – **Top Down**

Is more likely to be derived as a result of a risk assessment – **Bottom Up**

**Top Down**: will not conflict with overall corporate policy - ensures consistency across the organization.

**Risk management** ->> **Security policy decisions**

Determine the RPO for a critical process in an enterprise = **Extent of data loss that is acceptable**

**Security Baseline** – Sufficiency of control, doc, Implementation, Compliance

MOST important element for the successful implementation of IT governance = **Identifying organizational strategies**

**Rootkit** detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis.

After a disaster declaration, the media creation date at a warm recovery site is based on the = **RPO**

**Using data collection techniques:** Staff observation; Document review; Interviews; Workshop; CAAT; Surveys

**Classification of Audit:** Financial audit; Operational audit; Integrated audit (combines both financial and operational audit

To ensure that the organization is complying with privacy issues, an IS auditor should address **legal and regulatory requirements** first.

**Transborder data flow** refers to data transmission between two countries

A **password vault** is a software program that keeps a number of passwords in a secure digital location.

**Rapid elasticity** is a cloud computing term for scalable provisioning, or the ability to provide scalable services. Experts point to this kind of scalable model as one of five fundamental aspects of cloud computing

The **critical processes** will change as the business changes with new products and customers.

Two groups that have offered a baseline of definitions for Cloud **NIST and Cloud Security Alliance**

**PaaS**: Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider

**Phlashing**: Permanent denial-of-service (PDoS) attack, Damages a system hardware , Hardware Replacement

If the outsourcing vendor is from another country, the organization should be aware of **Cross-border legislation**

**IaaS** = cloud services puts IT operations into the hands of a third party.
**Security labels** are used in Mandatory access control model

DRP has a reciprocal agreement = **Mitigation**

**Preventive:** IDS= Installing an intrusion detection system (IDS), will make it possible to pinpoint the source of the attack, so that counter-measures may then be taken. An IDS is not limited to detection of attacks originating externally.

**Detective:** hash, checkpoints, echo, error messages, internal audit, performance log etc.

**Corrective:** BCP, backup, rerun procedures etc.

**Cell sampling**: random selection is performed at predefined intervals.

**Fixed Interval Sampling**: The sample existing at every n+ interval increment is selected for testing.

**RBAC:** create Matrix that documents the functions associated with particular kinds of work, typically referred to as a segregation of duties (SoD) matrix, shows which roles are required or permitted to have which permissions.

Real time Data Synchronization between DC and DR systems is done to avoid any data loss; measured by the **RPO** as a parameter

**SOD** is a basic, key internal control and one of the most difficult to achieve. It is used to ensure that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business.

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of **testing the controls and include additional substantive tests.**

**When dealing with offshore operations, it is essential that detailed specifications be created**. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptions and modifications may not be adequately communicated. Inaccurate specifications cannot easily be corrected.

The **top-down** approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early.

Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system

The Unified Modeling Language (**UML**) is a general-purpose, developmental, modeling language in the field of software engineering, that is intended to provide a standard way to visualize the design of a system.

**Simula 67** is seen as the first object oriented language.

In **object-oriented programming**, polymorphism refers to a programming language's ability to process objects differently depending on their data type or class. More specifically, it is the ability to redefine methods for derived classes

**Objects** usually are created from a general template called a class

**RAD** provides a means for developing systems faster while reducing cost and increasing quality.

**Scrum** aims to move planning and directing tasks from the project manager to the team

**Agile**: The use of small, time-boxed subprojects or iterations.

CAAT = meet predetermined criteria =>**CIS**

**Integrity:** The accuracy, completeness and validity of information

**COSO:** provides guidance and a comprehensive framework of internal control for all organizations

**Fault-tolerance** enables a system to continue operating properly in the event of the failure of some parts of it. It avoids total breakdown, and is particularly sought-after in high-availability environment full of business critical systems.

**Regression testing** is done in case of application programs in order to retest the program after making correction, in order to see that there is no other error cropping up.

**Sociability testing** is done for both hardware and software to assure that the program works well with the target system.

**Attribute sampling** is used to test compliance of transactions to controls—in this instance, the existence of appropriate approval.

**Risk Management:** the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization

**Variable sampling** is used in substantive testing situations and deals with population characteristics that vary, such as monetary values and weights.

**Stop-or-go sampling** is used when the expected occurrence rate is extremely low.

**Judgment sampling** refers to a subjective approach of determining sample size and selection criteria of elements of the sample.

**Abnormal server communication from inside the organization to external parties may be monitored to: should be recorded via APT.**

**Full** — backups all files, modified or not and removes the archive attribute

**Incremental** – backs up only those files that have been modified since the previous backup and removes the archive attribute

**Differential** – backs up files that have been modified since last full backup and does not touch the archive attribute

**ITF** 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.**

**Attribute sampling**: Determine whether an attribute is present or absent in the subject sample; The result is specified by the rate of occurrence-for example, the presence of 1 in 100 units would be 1%

**Stop-and-Go Sampling**: Used when few errors are expected. Stop-and-go allows the test to occur without excessive effort in sampling and provides the opportunity to stop testing at the earliest possible opportunity.

**Discovery sampling**: This 100% percent is used to detect fraud or when the likelihood of evidence existing is low. Forensics is an excellent example of discovery sampling.

**Precision, or Expected Error Rate:** The precision rate indicates the acceptable margin of error between audit samples and the total quantity of the subject population. Precision is usually expressed as a percentage.

**Interviewing selected personnel** is the best technique. Surveys, document review, and observations generate a lower yield. The **compliance test** uses precision to describe the rate of occurrence out of the sample population. The compliance testing uses precision to describe the expected error rate of the sample compared to total population. Precision is usually expressed as a percentage.

The **audit committee's** purpose is to review and challenge assurances made, and to maintain a positive working relationship with management and the auditors.

Standards are mandatory, and any **deviation** would require justification.

Periodic testing does not require separate test processes= **ITF**

**Purpose of Risk Analysis**, helps auditors to Identify threats to organizations to have controls in place//Evaluate countermeasures//Decide on auditing objectives//Support risk based auditing decision//Lead to implementation of internal controls

**Preventative**: determine issues, monitor operations; Prevents malicious acts.

**Detective**: mechanisms of reporting malicious act.

**PERT** will display the complete project and illustrate the various interdependencies between tasks

**Corrective**: basically minimizes the impact after the fact. Some type of Intrusion detention control, quarantine and remove the problem. Modify the system to make changes to take contingency planning and testing.

**Knowledge of information technology** helps the information security manager understand how changes in the technical environment affect the security posture.

**High risk tolerance** (i.e., a high degree of variability in acceptable risk) addresses the issue of uncertainty in the risk assessment process itself.

**Sociability testing** is used in Situation when one wants to see how the Software performs with other applications.

**System Programmer** = software installation.

**Objective of value delivery** is to optimize security investments in support of business objectives.

**Risk analysis** is a process by which the likelihood and magnitude of IT risk scenarios are estimated. Risk analysis is conducted to ensure that the information assets with the greatest risk likelihood and impact are managed before addressing risk with a lower likelihood and impact. Prioritization of IT risk helps maximize return on investment for risk responses.

**Risk analysis** = enable the prioritization of risk responses.

**Define the audit universe**; FIRST step performed prior to creating a risk ranking for the annual internal IS audit plan

**Project steering committee**; PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results

**Raid7**; to be configured into one large virtual disk partition using high-speed asynchronous data transfer

Dissemination of Tacit knowledge is done in, **Agile development**

Model does not support Planning: **RAD Model**

**Prototyping** as its core development tool is used in RAD completeness of inbound transactions via electronic data interchange (EDI); Segment counts built into the transaction set trailer

Thin client architecture = **Availability**

**Risk Appetite**: The extent to which the organization can take Risk and this is calculated without proper figures. Its "subjective".

**Risk Tolerance**: This is same as Appetite but calculated in "measurable units". Say, a stakeholder can take Risk up to some USD (with actual figures).

Defining and then building the system, in a top down fashion is followed in **structured analysis, design and development**

**Risk reduction mechanism** by controlled trial and error procedures is found in Prototyping evolutionary development

**Project steering committee** is ultimately responsible for all deliverables, project costs and schedules.

**Gantt chart** to determine whether the project is behind, ahead or on schedule compared to baseline project plan

BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness; **Preparedness**

**Residual Risk** the remaining level of risk once controls have been applied; can be used by management to further reduce risk by identifying those areas in which more control is needed

**SLA** a document that provides a company with a performance guarantee for services outsourced to a vendor mechanisms of risk allocation

**Benchmarking:** A process of continuously measuring system results, comparing those results to optimal system performance (industry standards or best practices), and identifying steps and procedures to improve system performance

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

**Segregation of duties** provides two benefits; first, a deliberate fraud is more difficult because it requires collusion of two or more persons, and second, it is much more likely that innocent errors will be found. At the most basic level, it means that no single individual should have control over two or more phases of a transaction or operation.

**An IS audit charter establishes the role of the information systems audit function**. The charter should describe the overall authority, scope and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee.

**Qualitative techniques** are more effective in evaluating things such as customer loyalty and goodwill.

**In the design phase**, security checkpoints are defined and a test plan is developed.

**Governance of Outsourcing** the set of responsibilities, roles, objectives, interfaces and controls required to anticipate change and manage the introduction, maintenance, performance, costs and control of third-party provided services

**Audit trails** retrace the flow of a transaction; recreates the actual transaction flow from the point of origination to its existence on an updated file

Management should assign responsibilities to ensure a **crosscheck of duties**.

**Library control software** is concerned with authorized program changes and would not move modified program changes into production unless and until the changes are authorized, which is what the software is designed to track.

**Preventive** — Designed to lower amount and impact of unintentional errors entering the system and to prevent unauthorized intruders from internally or externally accessing the system — actions to reduce risk Data validation, pre-numbered forms, and review for duplications.

**SSL** is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet

**SSL:** confidentiality of a message through symmetric encryption.

**Regression testing** is done in case of application programs in order to retest the program after making correction, in order to see that there is no other error cropping up.

The RPO is "the earliest point in time to which it is acceptable to recover the data." **If backups are not performed frequently enough to meet the new RPO**, a risk is created that the company will not have adequate backup data in the event of a disaster.

**Photoelectric** effect is the observation that many metals emit electrons when light shines upon them. Electrons emitted in this manner can be called photoelectrons. According to classical electromagnetic theory, this effect can be attributed to the transfer of energy from the light to an electron in the metal.

**Sociability testing** is done for both hardware and software to assure that the program works well with the target system.

When several applications are hosted on a server, the server's RTO must be determined by taking the RTO of the **most critical application**, **which is the shortest RTO**.

**Parallel operation** is designed to provide assurance that a new system meets its functional requirements. This is the safest form of system conversion testing because, if the new system fails, the old system is ready for production use.

**Risk analysis** is a process by which the likelihood and magnitude of IT risk scenarios are estimated.

By evaluating the organization's development projects against the CMM, an 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.

**Application controls** consist of edit tests, totals, reconciliations, and identification and reporting of incorrect missing or exception data.

**Decision support system:** Interactive system that provides the user with easy access to decision models and data from a wide range of sources – supports managers in decision making tasks for business purposes. Concentrates less on efficiency than on effectiveness (performing the right task). Usually based on 4GL languages. Improves managers decision making ability, but hard to measure. Implementation risk is inability to specify purpose and usage.

**Risk analysis** is conducted to ensure that the information assets with the greatest risk likelihood and impact are managed before addressing risk with a lower likelihood and impact.

**Prioritization of IT risk** helps maximize return on investment for risk responses

**A secure web connection or firewall is considered an external defense**.

**A firewall will find it more difficult to filter a specific file from a trusted source**.

**Inherent risk** - Inherent risk is normally high due to the number of users and business areas that may be affected

**Residual risk**-- Residual risk is the remaining risk after management has implemented a risk response,

**Compliance testing --unauthorized modification**

**Cost-effective approach to test the security of a legacy application**; Conduct a vulnerability assessment to detect application weaknesses

The FIRST step in data classification is to **establish ownership**.

**Disk-to-disk (D2D) backup** should not be seen as a direct replacement for backup to tape; rather, it should be viewed as part of a multitier backup architecture that takes advantage of the best features of both tape and disk technologies. Backups to disks are not dramatically faster than backups to tapes in a balanced environment.

**CAATS -** AUDIT PROGRAM

**CASE TOOLS** - AUDIT TRAIL

Approve changes to the audit charter = **Audit committee**

**Project steering committee**: PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results.

**BCP** should be tested = whenever there are significant changes in the organization and annually

**Library control software** restricts source code to Read-only access

The process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality = **Benchmarking**

**Parity bits** are a control used to validate Data completeness

**Run-to-run totals** can verify data through which stage(s) of application processing = various

**Data dictionary/directory system** (DD/DS) helps define and store source and object forms of all data definitions for external schemas, conceptual schemas, the internal schema and all associated mappings. The data dictionary (DD) contains an index and description of all of the items stored in the database. The directory (DS) describes the location of the data and the access method.

Important step in **maintaining a BCP** is to update and test it whenever relevant changes take place within the organization

**Balanced scorecard** is: to measure organizational performance and effectiveness against strategic

**Business understanding**= Obtain an understanding by reviewing relevant docs, inquiries, and conduct risk assessment.

Operational test = **Simulation Test**

The first steps in developing a business continuity plan = **Perform BIA**

**Snapshot tool** is most useful when an audit trail is required.

**Full operational test** one step away from an actual service disruption; a full test of the BCP

**News media attention should be** => Directed to a single designated spokesperson

**BCP** = regularly reviewed and updated.

**BCP** should be reviewed quarterly and updated at least annually. Updates should occur after each test, changes in personnel, or changes in business direction. Plans are often updated for changes in key customers and products.

**MAO** is the maximum acceptable outage that can occur before critical deadlines are missed or recovery is no longer feasible because of the amount of time lapsed. MAO also may be referred to as maximum tolerable downtime (MTD)

FIRST step in managing the risk of a cyberattack is to: **identify critical information assets**.

**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.

**Inherent risk:** it is a probability of risk because of an existing situation, considering that there is no compensation controls. For instance, money is more likely to be stolen than the power generators. These types of risks are independent of audit.

**Control risk:** it is a risk that an error cannot be prevented or detected by the existing controls. For instance, reviewing computer log manual is a control against unauthorized access. However, the manual review has a risk of missing or overlooking some activities because of human errors. Therefore, manual review always has a control risk.

**Ownership of intellectual property** will have a significant cost and is a key aspect to be defined in an outsourcing contract.

To ensure alignment, the information security program should **establish a steering committee that includes all business areas**.

**Dual Power Leads**: The best way to prevent power outages is to install power leads from two different power substations.

To collect evidence while transactions are processed = **embedding audit module** = EAM

**Detection risk**: it occurs when an IS auditor uses inadequate test procedures to detect a material error. If the error exists, the auditor will not find it because of using wrong test procedures. An auditor's ability to identify the detection risk enhances the probability of rectifying the material errors. The probability of detection risk can be minimized by choosing the right sampling procedures.

Remember that the audit risks are not the same as statistical sampling risks. **Sampling risk means selecting the incorrect samples.**

**The RPO is determined based on the acceptable data loss** in the case of a disruption of operations. RPO defines the point in time from which it is necessary to recover the data and quantifies, in terms of time, the permissible amount of data loss in the case of interruption.

**Audit hooks** are useful when only select transactions or processes need to be examined.

**There are costs associated with all activities and a disaster recovery plan is not an exception**. Although there are costs associated with a disaster recovery plan, there are unknown costs that are incurred if a disaster recovery plan is not implemented.

**Audit charter** establishes the role of the information systems audit function

An advantage of using **sanitized live transactions** in test data is that: test transactions are representative of live processing.

**Nonrepudiation** services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and message origin authentication. However, nonrepudiation provides stronger evidence because the proof can be demonstrated to a third party.

**Digital signatures provide nonrepudiation.**

**Message origination authentication** will only confirm the source of the message and does not confirm the specific action that has been completed.

**Continuous audit approach** - time sharing environments

**OTP:** A security system that requires a new password every time a user authenticates themselves, thus protecting against an intruder replaying an intercepted password. OTP generates passwords using either the MD4 or MD5 hashing algorithms.

**Structured programming** is a programming discipline that employs a top-down strategy, a single-entry module, a single-exist module, and the exclusive use of three basic programs constructs. These constructs include sequence, selection, and repetition.

**Domain Integrity Test** / INTEGRATED TEST FACILITY --- Effectiveness of the routines/ operations - The major objective of this exercise is to verify that the edit and validation (VERIFICATION/COMPARING) routines are working satisfactorily.

**Relational integrity tests** - Calculations / Statistical - 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** - Bench marking - involve ensuring that all references to a primary key from another file actually exist in their original file test data DISAVANTAGE - Creating test data that covers all possible valid and invalid conditions

When using **dynamic keys**, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted.

A **classification schema** is developed to define the various degrees of sensitivity and/or criticality of information that is in the care, control or custody of an organization

Important when an operating system (OS) patch is to be applied to a production environment = **Approval from the information asset owner**

**Encryption with static keys**—using the same key for a long period of time—risks that the key would be compromised.

**Encryption of the data on the connected device** (laptop, personal digital assistant [PDA], etc.) addresses the confidentiality of the data on the device, not the wireless session.

The goal of **IT risk analysis** is to enable the prioritization of risk responses.

**Business interruption** it covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IS organization

Types of **batch balancing** include: Batch registers + Control accounts + Computer agreement

**Information** is gathered through inquiry, observation and interviews, and analysis of data using computer-assisted auditing techniques (CAATs).

**Data owners** are concerned with and responsible for who has access to their resources and therefore need to be concerned with the strategy of how to mitigate risk of data resource usage.

**Quantitative**
- Objective
- Based on probability
- Annual loss expect
- ALE = SLE X ARO

**Data flow diagrams** - graphically summarize data paths and storage. (WORK FLOWS)

**Mantrap system** of two doorways may be used to prevent multiple persons from entering and exiting at the same time. A mantrap allows one person to enter and requires the door to be closed behind the person. After the first door is closed, a second door can be opened. The mantrap allows only one person to enter and exit at a time.

**Certification Practice Statement (CPS)** - it defines how to proceed in the invent of a compromised private key

**ORGANISATIONAL CHART** - RESPOSNISBILITIES/ DUTIES OF INDIVUUDLAS

**Encryption** = confidentiality

**The design of a honeypot** is such that it lures the hacker and provides clues as to the hacker's methods and strategies and the resources required to address such attacks.

**Validated digital signatures** in an email = help detect spam.

**A bastion host does not provide information about an attack.**

**IDS/IPS** are designed to detect and address an attack in progress and stop it as soon as possible.

**Nonrepudiation,** achieved through the use of digital signatures, prevents the senders from later denying that they generated and sent the message. (**identification of the customer**)

**Encryption** may protect the data transmitted over the Internet, but may not prove that the transactions were made.

Are developed for the organization as a whole. – **Top Down**

Are more likely to be derived as a result of a risk assessment. – **Bottom Up**

Will not conflict with overall corporate policy. - **Top Down**

Ensure consistency across the organization. - **Top Down**

**Audit trails** can assist in detecting security violations, performance problems, and flaws in applications.

**Audit trails** are considered only after a problem occurs.

**Compensating controls** would include: Audit trails + Reconciliation + Exception reporting + Transaction logs + Supervisory reviews + Independent reviews

To achieve **value delivery**, consider a continuous improvement (i.e., Kaizen) culture based on the understanding that security is a process, not an event

**Characteristics of a DSS** : Aims at solving less-structured - Combines the use of models - Emphasizes flexibility and adaptability to accommodate changes

**CSA** is the review of business objectives and internal controls in a formal and documented collaborative process. **It includes testing the design of automated application controls**

**Authentication** is necessary to establish the identification of all parties to a communication.

Data confidentiality is achieved through authorized restrictions on access and disclosure, including a means for protecting privacy and proprietary data. **Provisioning access to data on a need-to-know basis is the primary way to ensure data confidentiality.**

**Diverse Routing** means one provider, but multiple routes (or paths).

**Alternate Routing** means multiple network providers, and/or multiple mediums (fiber, cable, radio)

**Integrity** ensures that transactions are accurate but does not provide the identification of the customer.

**Honeypot** obtain information about the hacker's strategy and methods.

**DSS** developed using 4GL tools

**AUDIT RISK:** The risk that an auditor expresses an inappropriate audit opinion when the financial statements are materially misstated is called audit risk. This risk is reduced by designing and performing audit procedures to obtain sufficient appropriate audit evidence.

**Inherent risk:** Inherent risk is the susceptibility of an account balance or class of transaction to misstatement that could be material individually or collectively. Accounts derived from complex estimates are subject to greater uncertainty than accounts from simple, factual data.

**Control risk:** Control risk is the risk that a material misstatement would not be prevented, detected, or corrected by the accounting and internal control systems. The risk is the function of the effectiveness of the design and operation of internal control system in achieving the entity's objectives relevant to the preparation of financial statements.

**Detection risk:** The risk that auditor will fail to detect material misstatement is known as detection risk. This risk related to auditor. Detection risk is the function of the effectiveness of the audit procedures and of its application by the auditor. Due to sampling procedures, this risk cannot be reduced to ZERO.

The success of a **CSA** program depends on the degree to which line managers assume responsibility for controls. This enables line managers to detect and respond to control errors promptly.

**Employee Termination**: In order to protect IT assets, terminating logical access to IT resources is the first and most important action to take once management has confirmed the employee's clear intention to leave the enterprise.

Maintenance and protection of data = **Data custodian**

Organizational assets, including information = **board of directors**

Providing access to systems = **Data custodians**

Approving access to systems = **Data Owner**

Establishing authorization and authentication = **Data custodians**

Handling identity management = **Information security staff**

**Steering committee** should be in place to approve all security projects.

**System owner** to take corrective action => vulnerability in the security of a critical web server

**Cyberattack:** identify critical information assets -> evaluate the likelihood of threats -> assess the vulnerability impact-> estimate potential damage.

**EDI** usually decreases the time necessary for review.

**Always tested in this order:** Desk-Based Evaluation/Paper Test: A group steps through a paper procedure and mentally performs each step. Preparedness Test: Part of the full test is performed. Different parts are tested regularly. Full Operational Test: Simulation of a full disaster

**Critical:** Cannot be performed manually. Tolerance to interruption is very low

**Vital:** Can be performed manually for very short time

**Sensitive:** Can be performed manually for a period of time, but may cost more in staff

**Non-sensitive:** Can be performed manually for an extended period of time with little additional cost and minimal recovery effort

**RISK**= Threat+ Vulnerability + Exposure

**SCARF** works using predetermined exceptions. The constituents of "exceptions" have to be defined for the software to trap.

**GAS** is a data analytic tool that does not require preset information.

**The integrated test facility tests** the processing of the data and cannot be used to monitor real-time transactions.

**Snapshots** take pictures of information observed in the execution of program logic.

**The goal of the meeting is to confirm the factual accuracy of the audit findings** and present an opportunity for management to agree on corrective action.

The **optimal business continuity strategy** for an entity is determined by the: lowest sum of downtime cost and recovery cost.

**Rollback** procedures involve restoring all systems to their previous working state.

**Parallel changeover** involves first running the old system, then running both the old and new systems in parallel, and finally fully changing to the new system after gaining confidence in the functionality of the new system.

**Level 3 = Defined**

**Algorithms** is set of procedure to achieve certain objective

Protection of specific sensitive information stored in the data warehouse => **Implement column- and row-level permissions**

**Compliance testing** determines whether controls are being applied in compliance with policy.

**Variable sampling** is used to estimate numerical values such as dollar values.

**Substantive testing** substantiates the integrity of actual processing such as balances of financial statements**.**

**BCP should be reviewed every time a risk assessment is completed**

**Stop-or-go sampling** allows a test to be stopped as early as possible and is no appropriate for checking whether procedures have been followed.

**Attribute sampling** is the primary sampling method used for compliance testing.

**Data mart**: stores result from data mining. Data Mart The data mart is a repository of the results from data mining the warehouse.

**Likelihood** = Impact

The **risk appetite** of an organization shows how much an organization is willing to take a risk in order to grow itself. It is the amount of risk that an organization is willing to accept to attain its business objective."

**JAD** It is the people that are designing the computer systems, and therefore, getting the right people in the JAD meeting with high motivation levels is essential. **People are more important than things**.

**Attribute sampling** is a sampling model that is used to estimate the rate of occurrence of a specific quality in a population and is used in compliance testing to confirm whether the quality exists.

**Discovery sampling** is used to find 100 percent of everything possible when fraud is suspected or the likelihood of finding evidence is low.

**Expert systems** benefits: Capturing the knowledge and experience of individuals + Sharing knowledge and experience

Most **insurance** covers only financial losses based on the historical level of performance and not the existing level of performance

Sampling methods used in **compliance testing**: Attribute; Stop-and-go; Cell

**SNAPSHOT** = Require an AUDIT TRAIL

**CIS** = Require EXAMINATION

**Audit hoots** = meet specific criteria

**Policies** are high-level documents that represent the corporate philosophy of an organization

The purpose of the **out of scope** section is to make clear to readers what items are not considered project objectives so that all project stakeholders understand the project boundaries and what is in scope vs. out of scope.

**CA:** Continuous Auditing is a method used to perform audit-related activities on a continuous basis that covers control and risk assessment. Is generally carried out by Internal Audit and uses CA/CCM software.

**CCM:** Continuous (Controls) Monitoring are processes to ensure that policies/processes are operating effectively and to assess adequacy/effectiveness of controls; Is generally carried out by operational/financial management. Audit will independently evaluate.

**Continuous Auditing:** • Provide assurance in high risk areas • Increase audit oversight and detect issues sooner rather than later

**Out of scope items** are not part of the project, while nice to have items may be included in the project objectives. However, they may be the last priority on the list of all project objectives.

Once the interdependencies or critical path has been determined then a realistic assessment can be made of the **project schedule**

Proper IT management focuses **on proactive discovery of inconsistencies**, errors, and processing failures. The results can be used for secondary value in trend analysis and SLA reporting.

**Problem escalation** is used to ensure that the problem is analyzed by a competent individual with the proper training.

**Layer 3:** This layer handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer **does routing and forwarding.**

The primary responsibility of the IT information security person is to ensure the proper **implementation of data security policies and to monitor the level of compliance.**

**Short-term and long-term planning** is the responsibility of audit management.

**Audit trail** It's a series of logged events that can be followed back with relevant information alongside each event.

From a **control** perspective, a job description should establish responsibility and accountability.

**DS:** The signature on the digest can be used to authenticate the sender. Digitally signing an email message does not prevent access to its content and, therefore, does not assure confidentiality.

A **matrix organizational** structure combines functional and product departmentalization, creates a dual reporting structure, and is optimal where product groups are necessary

Commitment and rollback controls = **integrity**

**Compliance test** is done to check if an organization is complying with the control procedures. It helps to determine whether the applied controls are aligned with the organization's policy and procedures and operating the way it should be. Compliance tests ensure that the controls exist and the processes are effective. An example of a compliance test is to test whether the changes to the production programs are being authorized properly.

**Substantive test** checks the integrity and validity of processing such as transaction in financial statements. An auditor can use this test to find monetary errors or other errors in the data. It can also be used to find the accuracy of an inventory.

If a database is restored using before-image dumps, where should the process begin following an interruption? **Before the last transaction**

All performance by a third party under the service-level agreement should be compared to the service levels that the provider and the user of the service agreed on. (**Reviewed by management)**

Without an information **classification scheme**, the users and custodians will not know how to handle information. It would be impossible to control leaks, prevent inappropriate destruction, sanction personnel, or survive investigations. Both privileged and public information would become a confused mess, resulting in the wrong information being lost or breached via accidental disclosure.

Which of the following is the MOST efficient way to test the design effectiveness of a change control process? **Perform an end-to-end walk-through of the process**

**Table lookups** are preventive controls; data are checked against predefined tables, which prevent any undefined data to be entered

An **ITF** 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. Careful planning is necessary, and test data must be isolated from production data.

In **risk-based audit**, inherent risk assessment is completed first

**BPR** is the thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings

A **KPI** is a measure that determines how well the process is performing in enabling the goal to be reached.

**BPI**
- Six Sigma
- IT balanced scorecard (BSC)
- Key performance indicators (KPIs)
- Benchmarking
- Business process reengineering (BPR)
- Root cause analysis
- Life cycle cost-benefit analysis

Transport Layer Implement **Congestion control** using TCP window Flow Control Mechanism and congestion avoidance

**Turnaround time** — The time that the help desk or vendor takes to fix a problem from the moment it is logged in

**Implementation of a BCP** will be effective only if appropriate personnel are informed and aware of all the aspects of the BCP (communicated to appropriate personnel)

**Warm site** has the basic infrastructure facilities implemented, such as power, air conditioning and networking, but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

**Formal inspections** are a primary bug prevention method

**A logic bomb** is hidden code that will activate when certain conditions are met; **after a certain period of time.**

Programming languages, software compilers, and software testing are error **detection methods** due to their discovery of problems

**Compensating controls** may be used when segregation of duties is not practical for a **small staff**. Procedures must exist to verify that only approved program changes are implemented.

**GREATEST risk in EDI** = Lack of transaction authorizations

During **Post implementation**; Following implementation, a **cost-benefit analysis or return on investment (ROI)** should be re-performed to verify that the original business case benefits are delivered.

Financial controls and financial audits are based on following the **COSO controls**

An **SOA** relies on the principles of a distributed environment in which services encapsulate business logic as a black box and might be deliberately combined to depict real-world business processes.

**GAS** is not used to identify unauthorized access to data if this information is not stored in the audit log file

**SOAP** Used in XML programming to define the application programming interface (API) being used; Originally known as Simple Object Access Protocol.

**Auditing** is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person.

**Extensible Business Reporting Language (XBRL)** is a language for the electronic communication of business and financial data developed by a non-profit consortium of companies and government agencies to enhance the usability of financial information. XBRL is used to encode financial statements using data tags so that the financial information can be read automatically by XBRL-enabled software and more easily sorted and compared.

**Emergency changes** should still undergo the formal change management process after the fact.

**Protocol analyzers** are network diagnostic tools that monitor and record network information from packets traveling in the link.

**Digital signature** is an electronic identification of a person, created by using a public key algorithm, to verify to a recipient the identity of the source of a transaction and the integrity of its content. Since they are a "shared secret" between the user and the system itself, passwords are considered a weaker means of authentication.

**Encrypting** the transaction with the recipient's public key will provide confidentiality for the information.

Using a **PDF** will probe the integrity of the content but not necessarily authorship.

The risk level or exposure without taking into account the actions that management has taken or might take is **inherent risk**

A **risk-based audit** approach focuses on the understanding of the nature of the business and being able to identify and categorize risk. Business risks impact the long-term viability of a specific business.

**Information risk** reflects the possibility that the information upon which the business risk decision was made was inaccurate. A likely cause of the information risk is the possibility of inaccurate financial statements.

**Assessing risk**; Considering **both monetary value and likelihood of loss**

**Risk analysis** should take into account the potential financial impact and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus primarily on recent losses or losses experienced by similar firms. Although this is important supplementary information, it does not reflect the organization's real situation.

**Once the business process is identified**, the IS auditor should first identify the control objectives and activities that should be validated in the audit

**Standing data** should be purged from the equipment prior to disposal.

**SLA** is a guarantee that the provider will deliver the services according to the contract.

**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.

**Audit charter** should state management's objectives for the delegation of authority to IS audit.

The use of **continuous auditing techniques** can improve system security when used in time-sharing environments that process a large number of transactions.

**To assess IT risk**, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches.

Enabling **audit trials** helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system.

**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.

When designing an audit plan, it is important to identity the **areas of highest risk** to determine the areas to be audited.

**Preventive** — Designed to lower amount and impact of unintentional errors entering the system and to prevent unauthorized intruders from internally or externally accessing the system — actions to reduce risk Data validation, pre-numbered forms, and review for duplications

**Segmenting** a highly sensitive database results in: reduced exposure

**Detective** — Identify and react to security violations Track unauthorized transactions and lessen errors by detecting quickly.

**Corrective** — React to an attack and take corrective action Data recovery

**Recovery** — Restore the operating state to normal after an attack or system failure

The primary objective of the **initiation meeting** with an audit client is to help define the scope of the audit.

**Control Self Assessment (CSA)** is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. CSA is the review of business objectives and internal controls in a formal and documented collaborative process. The primary objective of a control selfassessment program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line manager. The success of a CSA program depends on the degree to which line managers assume responsibility for controls.

**The attributes of CSA** include: empowered employees, continuous improvement, extensive employee participation and training.

**The scope of an IS audit** should not be constrained by the ease of obtaining the information or by the auditor's by the auditor's familiarity with the area being audited.

An **assessment of risk** should be made to provide reasonable assurance that material items will be adequately covered during the audit work.

**Audit risk** is the combination of detection, control and inherent risks for a given audit assignment.

**Control risk** is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls.

**Inherent risk** is the risk that an error exists in the absence of any compensating controls.

**The primary objective of forensic software** is to preserve electronic evidence to meet the rules of evidence.

**Process owner** involvement is a critical part of the business impact analysis (BIA), which is used to create **DRP**

**Generalized audit software GAS** feature include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recompilations. The goal of the meeting is to confirm the factual accuracy of the audit findings and present an opportunity for management to agree on corrective action.

**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. An independent test performed by an IS auditor should always be considered a more reliable source of evidence than an confirmation letter from a third party since a letter does not conform to audit standards and is subjective.

In many instances, the reasons **given for failure of the CASE technology** include organizational issues, cultural factors, and poor implementation efforts, not the tools, not financial investments, not training, not lower return on investment, not inadequate testing, not lack of ongoing support.

**IDS cannot detect attacks within encrypted traffic** and it would be a concern if someone were misinformed and thought that the IDS could detect attacks in encrypted traffic.

**Hash totals** is an effective method to reliably detect errors in data processing.

**Firmware:** Memory chips with embedded program code that holds their content when power is turned off

**Foreign key:** A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value.

Ensures the availability of transactions in the event of a disaster; the only way to ensure availability of all transactions is to perform a real-time transmission to an **offsite facility**.

**Frame relay:** A packet-switched wide-area-network (WAN) technology that provides faster performance than older packet-switched WAN technologies

**IDS** is to warn you of suspicious activity taking place – not prevent them.

**Advanced persistent threat (APT)** refers to stealthy attacks not easily discovered without detailed analysis of behavior and traffic flows. Security information and event management (SIEM) solutions analyze network traffic over long periods of time to identify variances in behavior that may reveal APTs.

**Stateful inspection** is a function of some firewalls, but is not part of a security information and event management (SIEM) solution. A stateful inspection firewall keeps track of the destination IP address of each packet that leaves the organization's internal network. Whenever the response to a packet is received, its record is referenced to ascertain and ensure that the incoming message is in response to the request that went out from the organization.

**Zero-day attacks** are not advanced persistent threats (APTs) because they are unknown until they manifest for the first time and cannot be proactively detected by security information and event management (SIEM) solutions.

**Vulnerability assessment** identifies areas that may potentially be exploited, but does not detect attempts at exploitation, so it is not related to advanced persistent threat (APT).

**Integrated test Facility (ITF)** 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.

In developing a **risk-based** audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage.

**Understanding the business process** is the first step an IS auditor needs to perform.

**Operational audit** — a review of any part of an organization's operating procedures and methods for the purpose of evaluating efficiency and effectiveness

**Misstatement** in the financial statements can be considered material if knowledge of the misstatement will affect a decision of a reasonable user of the statements

**IT governance** is concerned with two issues: that **IT delivers value to the business and that IT risks are managed.**

The first is driven by **strategic alignment of IT** with the business. The second is driven by embedding accountability into the enterprise.

**ISDN internet service** is basically a telephone-based network system that operates by a circuit switch, or dedicated line.

**Exception report** is a processing control that should be generated when transactions appear to be incorrect.

**Audit committee** is a selected number of members of a company's board of directors whose responsibilities include helping auditors remain independent of management. Most audit committees are made up of three to five or sometimes as many as seven directors who are not a part of company management.

**IT governance** is the management system used by directors; the responsibility of the board of directors and executive management

**IT resources** should be used responsibly, and IT-related risks should be managed appropriately.

**This high-value goal** can be achieved by aligning IT governance framework with best practices.

Unapproved policies may present a potential risk to the organization; **IS auditor must report the finding**

**IT Governance**: Strategic alignment, Value delivery, Risk management, Resource management, Performance measurement. Board of directors & 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 enforce, and an IT security risk and impact analysis is consistently performed, it is said to be "**managed & measurable**"

**Compensating controls** are internal controls that are intended to reduce the risk of an existing potential control weakness that may arise when duties can't be appropriately segregated.

**Overlapping controls** are two controls addressing the same control objective or exposure. Since primary controls can't be achieved when duties can't 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.

In the **influence project management** style, the project manager has no real authority and the functional manager remains in charge.

**Access controls for resources are based on individuals and not on roles.**

Identification of the applications required across the network should be identified first; **Firewall Policy**

**IT Baseline Protection catalogs**: Detecting and combating security weak points in the IT environment.

**Substantive Testing**: this type of testing is used to substantiate the integrity of the actual processing. It is used to ensure that processes**, not controls,** are working as designed and give reliable results.

**Compliance Testing**: A compliance test determines if controls are working as designed; as policies and procedures are created, documented compliance testing looks for compliance to these management directives.

**Audit Classification:** Financial, operational, integrated, administrative, information systems, specialized (SAS 70), forensic auditing.

The **IT balanced scorecard (BSC)** is a process management evaluation technique that can be applied to the IT governance process in assessing IT functions and processes. BSC provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures of evaluate customer satisfaction.

**Exception reporting** is a processing control used to **capture input errors before processing occurs**. The exception may be held in suspension until the errors are corrected or rejected.

**Mitigation** is the strategy that provides for the definition and implementation of controls to address the risk described.

**Avoidance** is a strategy that provides for not implementing certain activities or processes that would incur risk.

**Transference** is the strategy that provides for sharing risk with partners or taking insurance coverage.

**Acceptance** is a strategy that provides for formal acknowledgement of the existence of a risk and the monitor of that risk.

To assess IT risks, threats and vulnerabilities need to be evaluated using **qualitative or quantitative** risk assessment approaches.

**Vulnerabilities** represent characteristics of information resources that may be exploited by a threat.
Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat. Impacts represent the outcome of result of a threat exploiting vulnerability.

**Nonce:** A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, **because a nonce is not necessarily unpredictable**.

**Enterprise architecture (EA)** involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective.

**Nonrepudiation:** The assurance that a party cannot later deny originating data; that is, it is the provision of proof of the integrity and origin of the data and can be verified by a third party.

**DS = nonrepudiation.**

In a public key infrastructure (PKI), to prove that an online transaction was authorized by a specific customer = **Nonrepudiation**

**SLM** = service level management is to: maintain and improve customer satisfaction and to improve the service delivered to the customer.

Internet banking application to mitigate the risk of internal fraud; **Transactions should be processed only if they are signed with the customer private key issued by a third-party certificate authority.**

The goals of **IT governance** are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business.

**IT governance** is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise.

**The IS auditor should first check the configuration settings for the current network layout** and connectivity and then, based on this, decide whether the security requirements are adequate.

**Corporate governance** is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

The risk that could be most likely encountered in a SaaS environment is speed and availability issues, due to the fact that **SaaS** relies on the Internet for connectivity.

Validated digital Signatures in an email detect **spam**

A sender encrypting a message using his / her private key provides non repudiation but not **confidentiality**

A sender encrypting a message using receiver's public key provides **confidentiality** but not non-repudiation

**Performance measurement** includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how they deliver it (process capability and performance).

**Strategic alignment** primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle.

**Resource management** is about the optimal investment in and proper management of critical IT resources.

**Waterfall life cycle**; requirements are well understood and are expected to **remain stable**, as is the business environment in which the system will operate.

**Through-the-computer auditing** refers to the whole information processing cycle from input through output of information. It usually includes the manual procedures associated with processing of input and verification of the output.

**Critical path diagrams are used to determine the critical path** for the project that represents the shortest possible time required for completing the project.

**PERT diagrams are a critical path method** (CPM) technique in which three estimates (as opposed to one) of timelines required to complete activities are used to determine the critical path.

**Attributes sampling:** A sampling plan enabling the auditors to estimate the rate of deviation (occurrence) in a population.

**Deviation rate:** A defined rate of departure from prescribed controls; Also referred to as occurrence rate or exception rate.

**Difference estimation**:A sampling pln that uses the difference between the audited (correct) values and book values of items in a sample to calculate the estimated total audited value of the population. Difference estimation is used in lieu of ratio estimation when the differences are not nearly proportional to book values.

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as: **SENSITIVE**

**Discovery sampling:** A sampling plan for locating at least 1 deviation, providing that the deviation occurs in the population with a specified frequency.

**Dual-purpose test:** A test designed to test a control and to substantiate the dollar amount of an account using the same sample.

**FPA is a technique used to determine the size of a development task,** based on the number of function points.

**Gantt charts help to identify activities that have been completed early or late through comparison to a baseline**. Progress of the entire project can be read from the Gantt chart to determine whether the project is behind, ahead of or on schedule.

**SLAs** are binding legal agreements between the service provider and the client. To guard the interests of the two parties involved, they must be reviewed by legal experts.

**The shorter RPO and RTO, the more costly a CDP implementation.**

Characteristic of **structured programming** is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures.

The appropriate recommendation is to review the results of stress tests during **user acceptance testing** (UAT) that demonstrated the performance issues

**hash totals** is an effective method to reliably detect errors in data processing, indicate an error in data integrity.

**PERT** = (P + 4M + O )/ 6

**Transparency** is primarily achieved through **performance measurement** as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

**Project Manager** cannot be a lead negotiator

**Work performance** measurements will ALWAYS compare actual progress vs planned progress. Work

**Performance Information** is information and data without any benchmark comparison.

**Sponsor provides** resources and support for the project and is accountable for enabling success.

**Business partners** are ALWAYS external organizations.

**Brainstorming** is also a Meeting.

**Hardening a system means to configure it in the most secure manner** (install latest security patches, properly define 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 integrity of the OS.

**Authenticity**, encrypt with sender's private key and decrypt with sender's public key

**Confidentiality**, encrypt with receiver’s public key and decrypt with receiver’s private key

**Certification Authority** = responsible for "maintenance" of certificates in PKI

**PKI**: Web based applications which need authentication ... e.g. banks ....
Generic scenario -> A and B dont know each other and don’t trust each other.... Both trust C ... Using PKI A and B can do business if C validates their identities to each other

**SSL** to encrypt the session data = Symmetric

**SSL** to share the session key = Asymmetric

**Hashes** can't be used to work backward

**To ensure authenticity and confidentiality**, a message must be encrypted twice: first with the sender's private key, and then with the receiver's public key. The receiver can decrypt the message, thus ensuring confidentiality of the message. Thereafter, the decrypted message can be decrypted with the public key of the sender, ensuring authenticity of the message. Encrypting the message with the sender's private key enables anyone to decrypt it.

**Email Confidentiality** Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key; Message is encrypted with public key of recipient and then decrypted by recipient private key

**XML**: Used to describe the capabilities of a web service as collections of communication endpoints capable of exchanging messages; WSDL is the language used by Universal Description, Discovery and Integration (UDDI). See also Universal Description, Discovery and Integration (UDDI).

**Mapping:** Diagramming data that are to be exchanged electronically, including how they are to be used and what business management systems need them.

**Unit testing**: A testing technique that is used to test program logic within a particular program or module.

**Corporate management's** responsibility to safeguard the company assets. This includes providing for contingency operations. Therefore, corporate management should supply the manpower and financial resources to develop and maintain the plan

**Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed**, identify the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made.

**Trend analysis** examines project performance over time to determine whether performance is improving or deteriorating.

**Encrypting** the client-server communication will not prevent internal fraud because encryption can be done at the application level The primary purpose for meeting with auditees prior to formally closing a review is to **gain agreement on the findings.**

**Emissions** can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to data.

**Retina** scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods.

**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.

When transmitting data; a **sequence number and/or time stamp** built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed.

**The primary activity of a CA i**s to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

**Online monitors** – measure telecommunications transmissions and their accuracy

**Protocol analyzer** – network diagnostic tool that monitors and records network information.

**Access control software** – designed to prevent unauthorized access to data and objects, unauthorized use of system functions or programs, unauthorized modification of data or unauthorized attempts to access computer resources.

**Internal control self-assessment (CSA**) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects.

It is critical that an independent **security review** of an outsourcing vendor be obtained.

**Performance indicators defenitaion** is required before implementing an IT balanced scorecard **BSC**

**Accountability** cannot be transferred to external parties.

**Why is self-signed didital certificate a security concern?** Because the essence of PKI is for an independent third party to sign the certificate so that the party dealing with the website can have reasonable assurance that it is dealing with a genuine entity

**The security policy** provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access.

Risks are mitigated by implementing appropriate security and **control practices**.

To ensure that noncompliance to information security standards is resolved = **Regular reports to executive management.**

Insurance is a mechanism **for transferring risk**. Audit and certification are mechanisms of risk assurance, and contracts and SLAs are mechanisms of risk allocation.

**Internal accounting controls** used to safeguard financial records..

**Strategic planning** sets corporate or departmental objectives into motion.

**Audit risk** represents the possibility that the auditor concludes after conducting an adequate audit that the financial statements were fairly stated when, in fact, they were materially misstated. Audit risk is unavoidable, because auditors gather evidence only on a test basis and because well-concealed frauds are extremely difficult to detect. An auditor may fully comply with auditing standards and still fail to uncover a material misstatement due to fraud.

**Audit failure** occurs when the auditor issues an incorrect audit opinion because it failed to comply with the requirements of auditing standards. An example is a firm assigning unqualified assistants to perform certain audit tasks where they failed to notice material misstatements in the client's records that a qualified auditor would have found.

**Legal liability** — the professional's obligation under the law to provide a reasonable level of care while performing work for those served

**Code signing** = the software has not been subsequently modified.

**Errors Versus** Fraud Auditing standards distinguish between two types of misstatements: errors and fraud. Either type of misstatement can be material or immaterial. An error is an unintentional misstatement of the financial statements, whereas fraud is intentional. Two examples of errors are: a mistake in extending price times quantity on a sales invoice and overlooking older raw materials in determining the lower of cost or market for inventory

**Strategies** are approaches followed by the entity to achieve organizational objectives. Auditors should understand client objectives related to: Reliability; Effectiveness and efficiency of operations; Compliance with laws and regulations

**EER:** equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. **In general, the device with the lowest EER is the most accurate.**

**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.

**Parameters that are not set correctly** would be the greatest concern when implementing an application software package.

**Risk assessment and business impact assessment** are tools for understanding business-for-business continuity planning.

**Business continuity self-audit** is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy.

**Gap analysis** can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

**Abrupt changeover**: a changeover approach where the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once the changeover to the new system takes place

**DAC** logical access protection that may be activated or modified by the data owner at his/her discretion; act as an additional filter, but cannot override MACs

**Lack of sufficient security controls is ulnerability, not a threat**

**DBA cannot delete activity logs**. Activity log is a strong detective control for DBA activities.

**Code signing** ensures that the executable code came from a reputable source and has not been modified after being signed.

**CMM** has 5 maturity levels. Maturity level 3 (defined) is the lowest level at which balanced score card (BSC) Exists.

**Depending on the complexity of an organization**, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan.

In BCP; **each plan has to be consistent with other plans to have a viable business** continuity planning strategy. It may not be possible to define a sequence in which plans have to be implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

**Obtaining sufficient and appropriate evidence assists the auditor in** not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

**Initiating and subsequently approving a change request** violates the principle of segregation of duties.

One of the strong **compensating controls** for DBA activity is ensure that DBA cannot delete activity logs. Activity log is a strong detective control for DBA activities.

The MOST efficient way to test the design effectiveness of a change control process => **Perform an end-to-end walk-through of the process**

Detect errors in data processing = **Hash totals**

**Table-top testing in BCP**: a walk through test on paper by major staff across the company, but no simulation; also to ensure that all the functional departments aware of their roles and responsibilities. Also to read and review the plan

Mandatory one-week vacation in financial institutions is a **detective control to find out illegal acts or improprieties if any.**

**Control Risk**; manual reviews of computer logs can be high because activities requiring investigation are often easily missed due to the volume of logged information.

**Walk-through** procedures usually include a combination of inquiry, observation, inspection of relevant documentation and reperformance of controls. A walk-through of the manual log review process follows from start to finish gaining a thorough understanding of the overall process and identifying potential control weaknesses

**Audit Risk:** It is the risk that Information may contain material error that may **go undetected** during the course of audit.

One of the first steps in creating a firewall policy is to identify network applications which need to **be externally accessed**

**Risk management is all about protecting assets**. Therefore the first step in a risk management program is to take **inventory of assets**.

**IT strategy committee** takes into account future business direction, future technological innovations, and regulatory compliance considerations

The risk of not using the results of the **business impact analysis** for disaster recovery planning means that the DRP may not be designed to recover the most critical assets in the correct order. As a result, the plan may not be adequate to allow the organization to recover from a disaster.

Minimize decision during crisis = **BCP**

The concerns in **BCP** include natural disasters, missed targets, and loss of profit. The goal of continuity is to ensure that important targets are not missed and revenue is not interrupted.

**BCP should be reviewed after Risk-Assement is completed**

**Mandatory vacation** = detective Control

**Systems usability** is measured by the end-user perception of the system

**IT risk is managed by embedding accountability into the enterprise**. The IS auditor should recommend the implementation of accountability rules to ensure that all responsibilities are defined within the organization.

Performing more frequent IS audits or recommending the **creation of a new role (CRO)** is not helpful if the accountability rules are not clearly defined and implemented.

**IT steering committee**: approving IT project plans and budgets

**Non repudiation** can only be possible with private key encryption

**System owners** are responsible for access rights and access levels

**People** is the weakest link in the information security chain

Main benefit of integrating TQM **total quality management** in the software development project is for **end-user satisfaction and not cost controls or meeting delivery dates or proper documentation**

**Steering committee** performs the financial evaluation of a project.

**Waterfall lifecycle model** in software development is best suitable when application system development requirements are well understood and expect to remain stable

If you do not know the requirements baseline, the best method for development would be agile, **because agile development follows an adaptive approach**

**Senior management** approves project and the resources it needs.

**Project steering committee** monitors costs and timelines and provides overall direction.

**Technical project manager** provides technical support

**Quality of metadata** = important factor in the design of a data warehouse.

While donating or disposing off used computers, organization must ensure that confidentiality is not being compromised. Tapes must be degaussed and magnetic disks must be demagnetized. It is also known as media **sanitization**.

**Run-to-run totals** will provide assurance that data converted from an old system to a new file system contains all the important elements

**Bottom up software** development and testing ensures that errors **in critical modules** are detected early on in the process

**A top down software** development and testing approach ensures that **interface errors** are detected and that critical functions are tested early on.

**Media Sanitization Methods** = Disposal + Clearing + Purging + Destroying

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the: requirement **for protecting confidentiality of information could be compromised.**

The **incident location** may be a technical crime scene. The response should be preplanned and structured to ensure that the value of evidence is not diminished and confidentiality is maintained.

**Regression testing is used to ensure that an application change has not altered the system functionality** that was not intended. Data used in regression test is the same as was used to perform the test before the change was enacted.

An auditor assigned to audit a **reorganized BPR project** should get the old process flow and the new process flow and ensure adequate controls in the new process.

**Encryption of data** is the most secure method of protecting confidential data from exposure.

**Program reverse engineering** usually involves reversing machine code into source code to understand its logic. It is usually done to understand a program whose source code has been lost.

**EVA (earned value analysis)** is an industry standard for measuring progress of a project at any stage. **It compares planned amount of work with completed amount of work.**

**Prototyping** always starts with high-level functions first; so effective testing for such functions is top down. RAD uses prototyping as its core strategy

**Detection Risk** is the risk that the auditor will not detect a misstatement that exists in an assertion that could be material, either individually or when aggregated with other misstatements

**RAP** = Risk Assessment Process = BO – IA – RA – RM – RT => Periodic Reevaluation

**Controls Development Life Cycle**: Design - Implementation - Operational effectiveness - Monitoring

The first person on the scene is the **incident commander**, regardless of rank or position. The incident commander may be relieved by a person with more experience or less experience, according to the situation. The incident commander will change throughout the crisis.

**Inspection of policies and procedures can provide some information as to whether monitoring exists**. The IT auditor needs to make inquiries of management and/or key employees to determine if this piece of **CDLC** is in place.

**Benchmarking**:determining the level of performance provided by similar information-processing-facility environments.

**Two-factor authentication** is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

**Population Value (PV):** the book value or monetary value of the population.

**Tolerable Misstatement (TM):** the tolerable margin of error or precision of the sample estimate of the population value (i.e. precision limit).

**Expected Misstatement (EM):** Expected amount of misstatement in the population value.

**Confidence Level (CL)**: Level of reliability or assurance required (i.e. complement of risk of incorrect acceptance)

**Internal Audit or External Auditors should be able to work independently** and report to the highest management level or audit committee or BOD.

Audit committee or IS Audit management should ensure the skill enhancements of the audit staff and also provide tools, methodology and work programs to auditors to help **them conduct audits of specialized nature**.

**Short term audit planning** covers audit issues on annual or yearly basis

**Audit planning** process should be reviewed on periodic basis, typically at least annually, to evaluate new control requirements based on changes in risk environment, technologies and business processes and enhanced audit evaluation techniques.

**Management Controls** modify processing systems to minimize the repeat occurrence of the problem

**Detective Controls:** help in detection and reporting of problems as they occur during a business process
Patches; Antivirus; Badges/ID's and Smart cards are is **preventive control** (help to prevent the problems before they happen)
Backups are a **corrective control** (helps to minimize the impact of a problem or risk)

**A website certificate** is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

The strength **of a secret key within a symmetric key cryptosystem** is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

IS auditors should **review access-control lists (ACL) to determine user permissions** that have been granted for a particular resource.

A major IS audit concern is users' ability to **directly modify the database**

The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster. **Total elimination of risk is impossible**.

If a database is restored from information backed up before the last system image, the system should be restarted before the last **transaction because the final transaction must be reprocessed**.

It depends. If IS audit is done **proactively** to identify the potential risks and address security early-on, then it is proactive and if it is done due to some major incident or some other business trigger to react to some event and to find specific weaknesses, then it can be **reactive**.

During **BCP** testing, the IS Auditor should act as: Observer

**BCP phases**: Project initiation – BIA – Recovery strategies – Plan design – Testing and training

The primary business objective of **BCP and DRP** is to mitigate the risk and impact of a business interruption, the dominating **objective remains the protection of human life**.

**Financial results** have traditionally been the sole overall performance metric.

**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.

**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.

Often, **mail filters** will quarantine zip files that are password-protected since the filter (or the firewall) is unable to determine if the file contains malicious code. Many zip file products are capable of using strong encryption. Such files are not normally corrupted by the sending mail server.

The **WEP** design has been broken and is considered insecure under all conditions.

**Prototype systems** can provide significant time and cost savings; however, they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated, and it often leads to functions or extras being added to the system that were not originally intended.

**Credit card transaction**: verify the format of the number entered then locate it on the database.

**Data owner** formally authorizes access and an administrator implements the user authorization tables.

**Consistency**—Transactions are processed only if they meet system-defined integrity constraints.

**Isolation**—the results of a transaction are invisible to all other transactions until the original transaction is complete.

**Durability**—Once complete, the results of the transaction are permanent.

**Preventive Controls** - These are controls that prevent the loss or harm from occurring. For example, a control that enforces segregation of responsibilities (one person can submit a payment request, but a second person must authorize it), minimizes the chance an employee can issue fraudulent payments.

**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 are invisible to external operations.

**Durability** guarantees that a successful transaction will persist, and cannot be undone.

**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.

**Discovery sampling**: Purpose is to detect at least one deviation, with a predetermined risk of assessing control risk too low if the deviation rate in population is greater than specified tolerable deviation rate Useful in suspected fraud.

**Sequential (Stop-or-Go) Sampling**: Audit sample taken in several stages

**Sampling risk**: risk that the auditors' conclusions based on a sample may be different from the conclusion they would reach if they examined every item in the population

**Nonsampling risk**: risk pertaining to non- sampling errors; can be reduced to low levels through effective planning and supervisions of audit engagements

**Stratification**: Technique of dividing population into relatively homogeneous subgroups

**Role-based access control defines roles for a group of users.** Users are assigned to the various roles and access is granted based on the user's role.

**Load testing** evaluates the performance of the software under normal and peak conditions.

**Stress testing determines the capacity of the software** to cope with an abnormal number of users or simultaneous operations. Because the number of concurrent users in this question is within normal limits, the answer is load testing, not stress testing.

**Recovery testing** evaluates the ability of a system to recover after a failure.

**Volume testing** evaluates the impact of incremental volume of records (not users) on a system.

**IS Control Objectives:** Safeguarding Assets //Ensuring integrity of operating systems, applications, data//Ensuring appropriate identification and authentication // Ensuring availability of services

Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. This number is called a **cyclical redundancy check (CRC).** When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred.

**Risk** should be addressed as early as possible in the development cycle. Risk should also be considered in the specification phase where the controls are designed, but this would still be based on the assessment carried out in the feasibility study.

**Nonrepudiation, achieved through the use of digital signatures**, prevents the claimed sender from later denying that they generated and sent the message. Encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made.

The recovery time objective **(RTO)** is the requirement for how quickly a business process or an IT service must be restored after a disaster. This affects the disaster recovery plan (DRP), but is dependent on the business impact analysis (BIA).

The **BIA** identifies the financial, operational and service impacts that may result from a disruption in a business process or IT service and therefore the **BIA is the primary driver for all the recovery plans including the technology recovery strategy.**

The **message digest** is calculated and included in a digital signature to **prove that the message has not been altered**. The message digest sent with the message should have the same value as the recalculation of the digest of the received message.

**Audit Risk** is a combination of detection, control and inheretant risks

**Standard methodologies** will provide consistency for all systems utilized in the company.

In a small organization, developers may release emergency changes directly to production. BEST control the risk in this situation: **Approve and document the change the next business day.**

**Information security policy** is management's formal declaration of security goals and objectives. Also the basis for access control authorization

**Atomicity** requires that a transaction be completed in its entirety or not at all = **data integrity**

**Escorting visitors** will provide the best assurance that visitors have permission to access defined areas within the data processing facility.

**Tape backup** = preventative control

**ITAF** = General standards + Performance standards + Reporting standards

The verify function (Backup) is a **detective control** intended to detect any discrepancies between the tape and the hard disk. It's a **detective control** because it still requires the operator to manually fix the problem after it is found.

An **audit module collects** data on transactions that may help identify fraudulent transactions, but it does not identify fraudulent transactions inherently.

**Process owner involvement is a critical part of the business impact analysis (BIA),** which is used to create the disaster recovery plan (DRP). If the IS auditor determined that process owners were not involved, this would be a significant concern.

**Suspense file**: A computer file used to maintain information (transactions, payments or other events) until the proper disposition of that information can be determined

**Switches**: reducing collision domains.

**Synchronous transmission:** Block-at-a-time data transmission

**System exit:** Special system software features and utilities that allow the user to perform complex system maintenance.

**System flowchart**: Graphic representations of the sequence of operations in an information system or program.
It is not possible to create business continuity plans BCP **without a current business impact analysis (BIA).** The BIA identifies critical processes and their dependencies.

**Consistency** ensures that all integrity conditions in the database be maintained with each transaction.

**Data center consolidation** is the process of reducing the volume of physical IT assets through highly efficient and scalable technologies,(reduce operating costs)

**Block data compression** reduces the size of data on disk, increasing available capacity up to 50 percent. Compression can be enabled automatically and operates in the background to avoid performance degradation.

**Prototyping** – creating system through controlled trial and error. Can lead to poor controls in finished system because focused on what user wants and what user sees. Change control complicated also – changes happen so quickly, they are rarely documented or approved. Also called evolutionary development. Reduces risk associated with not understanding user requirements. Just include screens, interactive edits and reports (no real process programs)

**Pooling compute resources** allows for simplified management, increased visibility of application workloads and cost transparency, ultimately accelerating business processes and cutting costs.

**Infrastructure-as-a-Service (IaaS)** is a complete IT infrastructure consumed as a service. Each user or tenant accesses a portion of a consolidated pool of federated resources to create and use their own compute infrastructure as needed, when needed, and how needed.

**PaaS** is used to develop and run software as an alternative to designing, building, and installing an in-house development and production environment.

**Replication** is the process of copying data within an array to another space within the same array, to a separate local array, or to a distant array. The purpose may be to relocate the data, to safeguard the data at a second location, or to locate the data at a secondary processing site so that operations may resume from there.

**Deduplication** is a data algorithm that breaks a file system into subfile, variable-length data segments to determine unique and repetitive segments. This dramatically reduces backup storage during the backup and recovery process.

**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

Creating a provision to **allow local policies** to take precedence where required by local authorities allows the organization to implement the optimal level of control subject to legal limitations**.**

The **RBAC model**, if implemented in the health care industry, for example, will assist in improving the protection of individuals' private health records and prevent identity theft**.**

**Protecting people's lives** should always be of highest priority in fire suppression activities. $CO_2$ and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards

**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

**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.

**Risk** is the combination of the probability of an event and its consequence.

**Risk Analysis** is a part of audit planning; identify risk and vulnerabilities; in order to determine the controls to mitigate those risks.

**Secure WLAN**: Disabling SSID broadcasting adds security by making it more difficult for unauthorized users.

The risk of not using the results of the **BIA** for disaster recovery planning means that the DRP may not be designed to recover the most critical assets in the correct order.

**The initiation of input transactions is always the function of the particular user area**. The data base administrator is responsible for the data base management system environment and the data that resides in it.

**Security procedures are usually detailed as step-by-step actions to ensure that activities meet a given standard.**

Recovery time objective (RTO) is based on the acceptable down time in case of a disruption of operations. **The lower the RTO, the higher the cost of recovery strategies**

IS Audit and Assurance Standards require that an IS auditor gather sufficient and appropriate audit evidence. The IS auditor has found a potential problem and now needs to determine whether this is an isolated incident or a systematic control failure; **Expand the sample of logs reviewed**.

Access control model **allows the system owner** to establish access privileges to the system - **Discretionary access control (DAC)**

**Crossover Error Rate (CER):** This is also called the equal error rate and is the point, generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal. **This has become the most important measure of biometric system accuracy.**

The accuracy of blocks of data transfers, such as data transfer from hard disks, is validated by a **CRC**

DBA != **control of data elements**

**Contradictory Evidence** Let the evidence tell the story. **Contradictory evidence suggests that either the auditor is doing something wrong** or you have discovered evidence proving a problem actually exists (nonconformity). The auditor needs to perform additional quality assurance checks and recheck the test results to determine the reason that this nonconformity has been detected.

**Rapid elasticity** is a cloud computing term for scalable provisioning, or the ability to provide scalable services. Experts point to this kind of scalable model as one of five fundamental aspects of cloud computing.

**GRC** is an effort to integrate assurance activities across an organization to achieve greater efficiency and effectiveness; **align organization assurance functions**.

**Scope creep** may indicate a lack of focus, poor communication, lack of discipline, or an attempt to distract the user from the project team's inability to deliver to the original project requirements.

**Uncontrolled changes** are often referred to as project scope creep; should be considered in the design phase.

**PERT chart:** will help determine project duration once all the activities and the work involved with those activities are known.

**PERT** = task interdependencies

**BEST backup strategy for a large database with data supporting online sales;** Mirrored hard disks will ensure that all data are backed up to more than one disk so that a failure of one disk will not result in loss of data.

**Function point analysis** : is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files.

**The critical path method** calculates the theoretical early start and finishes dates, and late start and finish dates, for all activities without regard for any resource limitations, by performing a forward and backward pass analysis through the schedule network.

**Rapid Application Development :** is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

**Completeness check:** is used to determine if a field contains data and not zeros or blanks.

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional **substantive tests.**

Ensuring that the project meets the intended business requirements is the primary objective of a **post-implementation review.** PIR should be scheduled some time after the solution has been deployed. Typical periods range from 6 weeks to 6 months, depending on the type of solution and its environment.

**The PIR is intended to be an assessment and review of the final working solution**. There should have been at least one full processing and reporting cycle completed.

**80/20 rule**, Quality is fitness for use, Top Management involvement required.

**Check digit:** is a digit calculated mathematically to ensure original data where not altered.

**Existence check**: checks entered data for agreement to predetermined criteria.

**Reasonableness check** : matches input to predetermined reasonable limits or occurrence rates.

**Functional acknowledgements** are standard electronic data interchange (EDI) transactions that tell trading partners that their electronic documents are received.

**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.

**Redundancy check:** detects transmission errors by appending calculated bits onto the end of each segment of data.

**Reasonableness check** : compare data to predefined reasonability limits or occurrence rates established for the data.

**The PMO provides** governance to coordinate and oversee all projects across the organization. This provides historical data for estimating, and success and failure criteria. PMO provides maturity to the process of managing projects

BEST help an IS auditor gain reasonable assurance that a project can meet its target date; **Extrapolation of the overall end date based on completed work packages and current resources**

**Parity check:** hardware control that detects data errors when data are read from one computer to another.

**Check digits**: detect transposition and transcription errors.

**Business continuity plans** span department boundaries.

**Change management**: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption; ensure that a good change management process is in place.

During audit, if there are material issues that are of concern, they need to be **reported immediately.**

**Prototype system** : provide significant time and cost savings. Also have several disadvantages like poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added.

**Decision support system (DSS):** emphasizes flexibility in the decision making approach of users. Advancements in computer programming technology and databases have led to the creation of decision support systems

**RTO** is the amount of time allowed for the recovery of a business function or resource after a disaster occurs; it does not determine acceptable data loss; greatest influence for **information processing facility**

**RPO** has the greatest influence on the **recovery strategies for given data**. It is determined based on the **acceptable data loss** in case of a disruption of operations. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

**MTO** is the amount of time allowed for the recovery of a business function or resource after a disaster occurs; it does not have a direct influence on data recovery.

**Authorization** should be separated from all

**Reconciliation** is ultimately the responsibility of the user department, In some organizations limited reconciliation of applications may be performed by the data control group with the use of control totals and balance sheets.

**EOC** is the Emergency Operations Center, staffed by the emergency management team during a crisis.

System development and system maintenance **SAME TASK**

**Data security officer** organization is recommending and monitoring data security policies

**Effective Bio: An overall metric that demonstrates that FAR and FRR rates are equal**

**COMPENSATING CONTROLS FOR LACK OF SEGREGATION OF DUTIES**: Reconciliation, Audit trails, Exception reporting, Transaction logs, Supervisory reviews, Independent reviews

**Noise:** Data or interference that can trigger a false positive

**Attacker or Intruder**: An entity who tries to find a way to gain unauthorized access to information, inflict harm or engage in other malicious activities.

**Residual biometric characteristics**, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access.

**A brute force attack** involves feeding the biometric capture device numerous different biometric samples.

**A cryptographic attack** targets the algorithm or the encrypted data

**Masquerader:** A user who does not have the authority to a system, but tries to access the information as an authorized user. They are generally outside users.

**Misfeasor:** They are commonly internal users and can be of two types:
An authorized user with limited permissions // A user with full permissions and who misuses their powers.

**Clandestine user**: A user who acts as a supervisor and tries to use his privileges so as to avoid being captured.

**Black Boxing** Tests the functionality of software by comparing the input and output, without understanding the internal process that creates the output. The internal logic is hidden from the tester

**SOD:** Ensure that no person can assume two roles: Origination, Authorization, Distribution, Verification

**Variance report** is the best example of a detective control. Detective controls attempt to detect problems

**Privacy:** Personal/private info is retained only when a true business need exists: Privacy is a liability
**Sanitized live transaction:** test data will be representative of live processing.

**Timebox management:** by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and rapid application development (RAD) and integrates system and user acceptance testining.

**Activities / roles must be segregated**: Authorization//Custody of Assets//Reconciliation//Record Keeping

**Balanced scorecard**: A management tool that aligns individual activities to the higher-level business objectives

**Residual Risks comprise of:** 1. Risk that remain after applying risk response strategies, and 2. Risks that we simply ACCEPT - if it happens, it happens, we have a plan to deal with it.

**Contingency Plans** deal with the outcome of Residual Risks on project.

**Table-top** testing is to practice proper coordination since it involves all or some of the crisis team members and is focused more on coordination and communications issues than on technical process details.

**Functional testing** involves mobilization of personnel and resources at various geographic sites. Full-scale testing involves enterprise wide participation and full involvement of external organizations.

**Walk-through** testing requires the least effort of the options given. Its aim is to promote familiarity of the BCP to critical personnel from all areas.

**Contingency Reserve** covers the outcome of Residual Risk, and account for the "Known Unknowns".

**Fallback Plans** are employed for Residual Risks when the Contingency Plans fail.

**Secondary Risks** are new risks that emerge as a result of Risk Response Plan.

**Throughput:** volume of work or information flowing through a system. Particularly meaningful in information storage and retrieval systems, in which throughput is measured in units such as accesses per hour.

**Scope Creep** - Poor initial requirements definition, Failure to involve users in early stages, missing Scope Baseline, Poor Change Control, Weak Management, Failure to manage user expectations.

**Flow Chart** shows how processes interrelate.

**Statistical Sampling** is a powerful tool where a RANDOM sample is selected instead of measuring the entire population.

**Attribute Sampling** is binary, it either conforms to quality or it doesn't **(YES or NO).**

**Variable Sampling** measures how well something conforms to quality **(RANGES).**

**Waterfall life cycle model:** best suited to the stable conditions where requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.

**Top-down approach** to testing ensures that interface errors are detected early and that testing of major function is conducted early.

**Bottom-up approach** to testing begins with atomic units, such as programs and module and works upward until complete system test taken place.

**Database view** allows the database administrator to control what a specific user at a specific level of access can see. For example, an HR employee may be able to see department payroll totals but not individual employee salaries

**Sociability testing** and **system tests** take place at a later stage in the development process.

**Utilization:** use of computer equipment and can be used by management to predict how/where/when resources are required.

Alternatives to **SoD**: Mandatory rotation of duties// Mandatory vacation //Analytical review

Segregation of Duties is a **Preventive Control**. In absence of this, compensating controls need to be identified to reduce or eliminate the business risks; Some of the **compensating controls** for Lack of Segregation of Duties are: Audit Trails//Reconciliation//Exception //Reporting//Transaction Logs//Supervisory Reviews//Independent Reviews

**Hardware error:** provide information to aid in detecting hardware failures and initiating corrective action.

**Availability report:** time periods during which the computer was available for utilization by uses or other processes.

**Identifying illegal software packages** loaded to the network can be checked by checking hard drives.

**Warm site**: A facility with basic utility services installed in some computer equipment but lacking all of the computer equipment necessary for recovery. The site will need to be built out before it can be used. **This site can be ready in days or weeks.**

**Hot site**: An alternate processing facility that is fully equipped with all the necessary computer equipment and capable of commencing operation as soon as the latest data files have been loaded. **Capable of being in full operation within minutes or hours.**

**Keyboard remapping: Changing the normal function of keys to execute different commands**

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

**PKI** is a framework, used to ensure CIA concept, an efficient use of public key infrastructure (PKI) should encrypt the: symmetric session key.

**Eavesdropping** is the act of secretly listening to the private conversation of others without their consent.

**Network Eavesdropping** or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.

**Agile** is an iterative process where each iteration or "sprint" produces functional code. If a development team was producing code for demonstration purposes, this would be an issue because the following iterations of the project build on the code developed in the prior sprint.

**Corrective action:** when an intervention is required to stop modifies or fix failures as they occur; Solving problem rather than covering it by hiding the truth.

**The business process owner should be consulted for any changes to the application**. The head of operations is ultimately accountable; in a privately owned enterprise, that would include the enterprise owner.

**Corrective controls** may also be relevant because they allow an error or problem to be corrected. Corrective controls remove or reduce the effects of errors or irregularities and are not exclusively regarded as compensating controls.

The **business process owner** should be consulted for any changes to the application. The head of operations is ultimately accountable; in a privately owned enterprise, that would include the enterprise owner.

When contracting with a service provider, it is a best practice to **enter into an SLA with the provider**. An SLA is a guarantee that the provider will deliver the services according to the contract. The IS auditor will want to ensure that performance and security requirements are clearly stated in the SLA.

**PPP** provides user authentication through PAP, CHAP, or EAP-TLS, whereas **IPSec provides system authentication**.

**Due diligence** = do check = investigate.

**Due care** = do act

**Managing risk does not deal with future decisions, but the future of present decisions**

A database designed so that knowledge of the format and structure of data is not required. Very flexible and may be quite complex; **Object-oriented database (OODB)**

**Data diddling** is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements

**Database renormalizing:** increased redundancy.

**Normalization** is optimization process for a relational database that minimizes redundancy

**Control group**— Members of the operations area that are responsible for the collection, logging and submission of input for the various user groups

**MTTR** is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device. (higher MTBF and a lower MTTR)

**MTBF** that are first reported represents flaws in the software that are reported by users in the production environment. This information helps the IS auditor in evaluating the quality of the software that is developed and implemented.( higher MTBF and a lower MTTR)

**SYN flood:** Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity of the target machine

**Referential integrity:** it ensures that a foreign key in one table will equal null or the value of a primary in the other table.

**Cyclical checking:** It is the control technique for the regular checking of accumulated data on a file against authorized source documentation.

**Domain integrity:** data item has a legitimate value in the correct range or set.

**Relational integrity:** performed at the record level and is ensured by calculating and verifying specific fields.

**Concurrency controls** prevent data integrity problems.

**Access control:** restrict updating of the database to authorized users.

**Quality controls:** such as edits ensures the accuracy, completeness and consistency of data maintained in the database.

**Database integrity =>** Table link/reference checks.

**Audit logs:** enable recording of all events that have been identified and help in tracing the events.

**Querying /Monitoring:** access time checks helps designers improve database performance.

**Rollback and roll forward**: ensure recovery from an abnormal disruption.

**Kiting**—using float to create cash by using multiple sources of funds and taking advantage of check clearing times = A proof of cash.

**Configuration management** is widely accepted as one of the key components of any network.

**CRC:** check for a block of transmitted data. CRC can detect all single-bit and bubble-bit errors.

**Parity Check:** Vertical redundancy check

**Echo checks:** detect line errors

**Screening router / Packet filter:** work at the protocol, service and port level. It analyzes from layers 3 and 4.

**DAC:** The creator of a file is the 'owner' and can grant ownership to others. Access control is at the discretion of the owner. Most common implementation is through access control lists.

**Mandatory (MAC): Much more structured. Based on security labels and categories**. Access decisions are based on clearance level of the data and clearance level of the user, and, classification of the object. Rules are made by management, configured by the administrators and enforced by the operating system. Mandatory access control is required for the Orange Book "B" Level.

**Role-Based (RBAC)**: (nondiscretionary access control) continually administered set of controls by role within organization. Roles are tighter controlled than groups. A user can only have one role. RBAC is best suited for companies with a high turnover rate. Used to handle inappropriate access to private and sensitive information through a business application

**Automatic logoff** is a method of preventing access on inactive terminals and is not a detective control.

**Unsuccessful attempts** to log on are a method for preventing intrusion, not detecting.

**Circuit gateway**: program that acts as an intermediary between external and internal accesses.

**Managing risk steps**: identification and classification of critical information > Identification of threats, vulnerabilities > calculation of potential damages.

**Screened-subnet firewall** : used as a demilitarized zone; Utilizes two packet filtering routes and a bastion host.

**Screened-host firewall:** utilizes a packet filtering router and a bastion host.

**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.

**Normalization:** The elimination of redundant data

**Isolation:** means that, while in a intermediate state, the transaction data are invisible to external operations.

**Durability** Guarantees that a successful transaction will persist, and cannot be undone.

**Hardware maintenance program** should be validated against vendor specifications.

**Maintenance schedules** normally are not approved by the steering committee. Unplanned maintenance can't be scheduled.

**Audit committee**: A committee of the board of directors composed of financially literate executives. The purpose of the committee is to challenge the assertions of management by using internal and external auditors.

**Library control software** should be used to separate test from production libraries in mainframe and / or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized.

**White hat**: An honest software tester working in the software development or audit department under a formal structured test procedure to determine system vulnerabilities by using known hacker techniques.

**Library control software is concerned with authorized program changes** and would not automatically move modified programs into production and can't determine whether programs have been thoroughly tested.

**Referential integrity** is provided by foreign key.

**Post-incident review PIR =** improve internal control procedures.

**Cryptography**: science of codes

**Cryptanalysis** is science of breaking codes

**Capacity management** is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. Determine unauthorized changes made to production code the auditor examine object code to find instances of changes and trace them back to change control records.

**Normalization:** is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create **redundancy and risk of not maintaining consistency of data,** with the consequent loss of data integrity.

**Coordinated release management** across projects and systems is a suitable strategy to employ in a complicated, dynamic system environment.

**Attribute sampling is used to test compliance of transactions to controls**—in this instance, the existence of appropriate approval.

**Variable sampling** is used in substantive testing situations and deals with population characteristics that vary, such as monetary values and weights.

**Continuous auditing** techniques SCARF/ EAM very complex method the application must contain embedded audit software to act as MONITORING AGENT cannot be used to interrupt regular processing

**Stop-or-go sampling** is used when the expected occurrence rate is extremely low.

**Judgment sampling** It refers to a subjective approach of determining sample size and selection criteria of elements of the sample.

**Certification Authority (CA):** A Certification Authority is a trusted third party that issues digital certificates and validates the identity of the holder of a digital certificate.

**Certificate Policy (CP**) Description of the rules governing the use of a public key certificate in a particular environment.

**Certificate Revocation List (CRL**): A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g. because of suspected key compromise, DN change) and then removed from it when it reaches the end of the certificate's validity period.

**Mandatory access controls** MAC are filters that cannot be altered by normal users and data owners, and they act by default to enforce a base level of security.

**Digital signature** is a mathematical technique used to validate the authenticity

**Digital certificate** is an electronic "passport" allowing people, computers or organizations to exchange secure information over network.

**DAC** will provide full access to a subject for an object so it does not help to ensure 100% confidentiality.

To ensure confidentiality, authentication, and integrity of a message, the sender should encrypt the hash of the message with the sender's: **Private key and then encrypt the message with the receiver's public key**.

One sample **system-generated exception report** for the review period with follow-up actions noted by the reviewer shows the best possible evidence as the effectiveness of the control can be evaluated.

**FPA** does not examine the number of expected users.

**In order to accept the risk**, management must first be made aware of the risk and its consequences. This includes a formal acceptance of the risk, which is usually evidenced by a sign-off.

**Discretionary access controls** DAC are filters that can be altered or modified by users or data owners and are used to further restrict access. **Discretionary access controls cannot overwrite mandatory access controls**.

**Least privilege access control** several individuals currently have local administrator rights on specific servers

**Role-based access controls** are filters created within an application to allow only certain functionality and processing abilities to specific roles

**Cryptography**: Transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.

**Decryption**: The act of restoring an encrypted file to its original state through the use of a key.

**Encryption**: The act of disguising information through the use of a key so that it cannot be understood by an unauthorized person.

Migrating from a legacy system to an enterprise resource planning (ERP) system; **correlation of semantic characteristics of the data migrated between the two systems.**

**IPSEC**: A developing standard for security at the network or packet processing layer of network communication; Especially useful for implementing virtual private networks and remote user access through dial-up connections.

**Attribute**: In computer programming, it is equivalent to a column in a database table; Refers to a specific characteristic of a database entry.

**Phishing** A social engineering technique called phishing (pronounced fishing) utilizes fake emails sent to unsuspecting victims, which contain a link to the criminal's counterfeit website. Anyone can copy the images and format of a legitimate website by using their Internet browser.

**Screened subnet** A subnet of multiple computer hosts protected by a firewall and accessible by both internal and external users. A screened subnet is also known as a demilitarized zone (DMZ). War veterans will tell you that you can still get killed in a demilitarized zone.

**Digital signatures** provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

**To secure email communication:** Establish public key/private key pairs with clients to encrypt email.

**Firewall**: The best method screened subnet, or DMZ design.

**Mapping identifies specific program logic that has not been tested** and analyzes programs during execution to indicate whether program statements have been executed.

**A snapshot records** the flow of designated transactions through logic paths within programs.

**Tracing and tagging** shows the trail of instructions executed during an application. **Logging is the activity of recording specific tasks for future review.**

The MOST effective way to ensure that **outsourced service providers** comply with the organization's information security policy would be **Regular audit exercise**

**Data owner** holds the privilege and responsibility for formally establishing the access rights.

**Control risk** can be high, but it would be due to internal controls not being identified, evaluated or tested, and would not be due to the number of users or business areas affected.

**Compliance risk** is the penalty applied to current and future earnings for nonconformance to laws and regulations, and may not be impacted by the number of users and business areas affected.

**Substantive test** includes gathering evidence to evaluate the integrity (i.e., the completeness, accuracy or validity) of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test.

Checking whether receipts and issues of tapes are accurately recorded is a **compliance test**.

**Sniffing** is an attack that can be illegally applied to capture sensitive pieces of information (password), passing through the network.

**Encryption** is a method of scrambling information to prevent unauthorized individuals from understanding the transmission.

**Spoofing** is forging an address and inserting it into a packet to disguise the origin of the communication.

**Inherent risk** is normally high due to the number of users and business areas that may be affected. Inherent risk is the risk level or exposure without taking into account the actions that management has taken or might take.

**Residual risk** is the remaining risk after management has implemented a risk response, and is not based on the number of user or business areas affected.

**Computer logs** will record the activities of individuals during their access to a computer system or data file and will record any abnormal activities, such as the modification or deletion of financial data.

Developing a risk-based audit program, focus on **Business processes**

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network; **traffic analysis**

**Neural network based IDS:** monitors the general patterns of activity traffic on network and creates a database.

**Tornado diagram** is a special type of bar chart used in sensitivity analysis (analyzing risk-taking scenarios)
When conducting a penetration test of an IT system; most important task is to be able to restore all systems to their **original state**

**Signature-based IDS**: Intrusive patterns identified are stored in the form of signatures.

**Lack of performance measures** will make it difficult to gauge the efficiency and effectiveness of the IT services being provided should be included in SLA

The need-to-know basis is the best approach to assigning privileges during the **authorization process**.

**A service-level agreement (SLA)** is a part of a service contract where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service or performance).

An IS auditor **should expect References from other customers** (an item) to be included in the request for proposal **(RFP)** when IS is procuring services from an independent service provider (ISP).

**SLA** is a part of a service contract where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service or performance).

**Steganography**: digital right management (DRM)

**Physiological**: Fingerprint, Hand, Iris, Face, DNA

**Behavioral**: keystroke, signature, voice

Main objectives of an audit are to **identify potential risk**; the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization.

**Remote booting** is a method of preventing viruses, and can be implemented through hardware.

**Hashing** is irreversible.

**Encryption** is reversible.

**Gantt chart** is a visual representation of a project where individual tasks occupy rows on a worksheet, and horizontal time bars depict the time required to complete each task relative to other tasks in the project.

**Gantt chart** can also show schedule dependencies and percent completion of each task

Not used in the **quality control process**; Control charts; Pareto charts; Statistical sampling.

**A flowchart is used to document internal program logic.** An entity-relationship diagram (ERD) is used to help define the database schema. Function point analysis is used for estimation of work during the feasibility study.

**Hashing** creates an output that is smaller than the original message and **Encryption** creates an output of the same length as the original message.

**Asymmetric algorithm** requires more processing time than symmetric algorithms

**Neural network:** large number; type of decision making system; IDS

**Immunizers** defend against viruses by appending sections of themselves to files.

**Accounting Policy** should be kept in the organization; **no outsourcing**

**Outsourcing:** The contractual arrangement to transfer ongoing operations to an **external service provider**.

**Behavior blockers** focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record.

**A Gantt chart** illustrates task duration, schedule dependencies, and percent completion. Gantt charts are basically Bar Charts to show progress to Team about the project work.

**Cyclical redundancy checkers (CRC)** compute a binary number on an known virus-free program that is then stored in a database file.'

**Computation speed**: elliptic curve encryption over RSA encryption. It use encryption methods support digital signatures, used for public key encryption and distribution and are of similar strength; Mobile devices

**PKI:** cryptography provides for encryption, digital signatures and no repudiation controls for confidentiality and reliability.

**SSL:** confidentiality

**IDS**: detective control

**VPN** : confidentiality and authentication (reliability), based on encapsulation

**Passive attack**: traffic analysis

**Active attack:** brute force, masquerading, packet reply, message modification, unauthorized access through the internet or web based services, denial-of-service attacks, dial-in penetration attacks, email bombing and spamming and email spoofing.

**CSF Critical success factor** is also known as a showstopper. Critical success factors must go right every time in order for recovery to be successful.

**KPI** is a numerical score.

**Hashing** is a method used for index partitioning.

**System downtime log** provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

**Steering committee** provides direction and control over projects to ensure that the company is making appropriate investments. Without approval, the project may or may not be working toward the company's goals.

**Key**: When used in the context of cryptography, a series of random numbers used by a cryptographic algorithm to transform plaintext data into encrypted data, and vice versa.

**Private Key:** A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information; one half of a **key** pair.

**Supervisor state** allows the execution of all instructions, including privileged instructions.

**DES**: block cipher — symmetric key — 56 bit key, plus 8 parity bits — 16 rounds of transpositions and substitutions

**End-to-end encryption** – encryption of data from source system to end system

**Authorization for changes** should be separated from other work if separation of duties cannot be achieved. Additional compensating controls would be required.

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.**

**Qualified certificate**: High level personal/professional digital identity assurance supporting legally valid digital signatures.

**Registration Authority (RA):** A person or organization responsible for the identification and authentication of an applicant for a digital certificate. An RA does not issue or sign certificates.

**Smart Card**: A device that is often the same size as a credit card but that is "smart" enough to hold its own data and applications and do its own processing. Smart cards can be used to store personal information, hold digital cash or prove identity.

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for **confirming the 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.

**Advanced Encryption Standard (AES):** symmetric — variable block and key length (128, 192, 256)

**Block sum check** – error detection only

**CRC** – error detection only

**Evidence** • Identify • Preserve • Analyze • Present

**Forward error control** involves transmitting additional redundant information with each character

Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level; **UPS**

**Vaccine**: A program designed to detect computer viruses.

**Write access to audit logs should be disabled**.

Data center should be positive pressure; **air flows out.**

**Humidity** – too much and get corrosion/condensation, too little and get static electricity.

**Microwave transmission**: A high-capacity line-of-sight transmission of data signals

**Post Project Review (PPR**) is to review the completed proj. and find lessons learnt on what went well, what could be done better.

The purpose of the **Post Implementation Review** (PIR) is to ensure that the project meets the intended business requirements. PIR should be scheduled some time after the solution has been deployed; Typical periods (6 weeks - 6 months) depending on the type of solution and its environment.

**Weekly full backup and daily incremental backup is the best backup strategy;** it ensures the ability to recover the database and yet reduces the daily backup time requirements. A full backup normally requires a couple of hours, and therefore it can be impractical to conduct a full backup every day.

**Clustered servers provide a redundant processing capability**, but are not a backup. Mirrored hard disks will not help in case of disaster.

The **data custodian** is responsible for Maintaining the data in proper condition

**User security awareness:** Best control to mitigate the risk of pharming attacks to an Internet banking application

**Pharming** (pronounced 'farming') is a form of online fraud very similar to phishing as pharmers rely upon the same bogus websites and theft of confidential information.

**Systems control audit review file (SCARF**): is the MOST effective tool for monitoring transactions that exceed predetermined thresholds.

**Understand the continuous auditing methods.** Continuous audit methods such as audit hooks or SCARF with embedded audit modules (SCARF/EAM) are used in environments where it is not possible to interrupt production.

Matching of **hash keys** over time would allow detection of changes to files.

**Having a log is not a control, reviewing the log is a control.**

**Tracing:** an audit procedure in which the auditor selects a basic source document and follows its processing path FORWARD to find its final recording in a summary journal or ledger, or BACKWARD to find its origin.

**Vouching** an audit procedure in which an auditor selects an item of financial information, usually from a journal or ledger, and follows its bath back through the processing steps to its origin (the source documents)

In BCP, **resumption of critical processes** has the highest priority because it enables business processes to begin immediately after the interruption and not later than the maximum tolerable period of disruption (MTPD) or maximum tolerable downtime (MTD).

Combining real and test data during an audit is known as: **Integrated testing facilities**

**Logical access controls**: securing software and data within an information processing facility.

**Call back features**: hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches.

**Call forwarding**: bypassing callback control.

**Logical access security**: unencrypted password is the greatest concern.

**Logical access control review**: to determine whether access is granted per the organization's authorities.

**Line grabbing**: enable eavesdropping, thus allowing unauthorized data access.

**First step of data classification is establish ownership of the data.**

**CSA** is a management technique that can be used to assure key stakeholders, both internal and external, that an organization's internal controls system is reliable

Role of **internal audit** is to evaluate Risk Control Governance.

When developing a security architecture, which of the following steps should be executed FIRST => **Defining a security policy**

**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. (Batch register, Control account, Computer Agreement)

**System generation parameters** determine how a system runs, the physical configuration and its interaction with the workload

**Proxy** server does not normally perform controls relating to data integrity.

If the IS auditor is granted direct access to the data => **Greater assurance of data validity**.

**Special or unusual flags** are input controls.

**The use of automated tools to support real-time and after-the-fact monitoring**; these are the best tools to achieve timelines from the information security point of view

**CSA** is the review of business objectives and internal controls in a formal and documented collaborative process. It includes testing the design of automated application controls. Exception reporting only looks at what has not been achieved. Manager involvement is important, but may not be a consistent or well-defined process compared to CSA. **CSA MOST important to ensure that effective application controls are maintained**

**Critical:** can't be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods.

When developing a large and complex IT infrastructure, the best practice is to use a **phased approach** to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

**Hash** is used for establishing integrity

**Hashing is an algorithm; it is irreversible (credit card transactions)**

**Vital:** can be performed manually but only for a brief period of time

**Non critical**: may be interrupted for an extended period of time at little or no cost to the company, require little time or cost to restore.

**Physical security** can meet the needs of data owners by making the information available for viewing and confidential from not allowing unauthorized access. The candidate must realize that in this answer the information is in hardcopy format and not softcopy.

The **IT strategic plan** exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the **business plan**.

**Defense-in-depth**: Firewall as well as logical access control on the hosts to control incoming network traffic.

**DIGITAL CERTIFICATE** => DIGITAL SIGNATURE

**Functions of digital signature (Integrity, Non repudiation)**

**PKI** uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

The primary purpose of **digital signatures** is to provide authentication and integrity of data.

UAT plans normally be prepared=> **Requirements definition**

FIRST generation **DES** - data encryption standard - 64 bits (56 bits are used for encryption and 8 bits parity check)

SECOND Generation **3DES** - 3* 64 bits - 192 bits (56*3 = 168 bits for encryption)

Third generation **AES** - 128 BITS/ 192/ 256 BITS

Web application system displays specific database error messages = **hijacking an administrator session**

**DSS:** emphasizes flexibility in the decision making approach of users.

**Sanitized live transaction:** test data will be representative of live processing.

**IS audit charter** establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function

**CSA** approach emphasizes management and accountability over developing and monitoring internal controls of an organization's sensitive and critical business processes.

**CIA**: to ensure confidentiality, authentication, and integrity of a message, the sender should encrypt the hash of the message with the sender's: Private key and then encrypt the message with the receiver's public key..

**Timebox management:** by its nature, sets specific time and cost boundaries. It is very suitable for **prototyping** and rapid application development (RAD) and integrates system and user acceptance testing.

The **CSA** process can generate benefits by empowering the staff to take ownership and accountability.

**GAP** analysis is used to determine the difference between the current environment and the proposed system; notice annual GAP analysis focus attention on areas in need of improvement

**Digital signature** is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private keys are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

**Manual controls** include separation of duties or responsibilities, which force collusion among employees to perpetrate fraudulent acts. In addition, batch control totals can be manually calculated and compared with matching computer-produced batch control totals.

**Sequence numbers** and time of arrival can be associated with data and checked to ensure that data has not been lost or reordered. Large volumes of data can be checked with utility or special-purpose programs.

**Unit testing** is testing of individual subprograms, subroutines, or procedures in a program. Its purpose is to check if the module code complies with the system internal specifications.

**Integration testing** (interface, incremental, string testing) is testing of program modules to see if they can work correctly as a whole without contradicting the system's internal and external specifications.

**Waterfall life cycle model** best suited to the stable conditions where requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.

**Top-down approach** to testing ensures that interface errors are detected early and that testing of major function is **conducted early**.

**Bottom-up approach** to testing begins with atomic units, such as programs and module and works upward until a complete system test taken place.

**Periodic review** of policies by personnel with specific knowledge of regulatory and legal requirements best ensures that organizational policies are aligned with legal requirements.

**System internal specifications** define processing logic, file structures, module interfaces, and system architecture, which is most useful in unit/integration testing

**Rapid Application Development RAD** approach is an: incremental and iterative development approach.

**Sociability testing** and system tests take place at a **later stage** in the development process.

**Diversity-in-defense**: Using two firewalls of different vendors to consecutively check the incoming network traffic.

**Piggybacking**: unauthorized persons following, either physically or virtually, authorized persons into restricted areas.

**Impersonation**: someone acting as an employee in an attempt to retrieve desired information.

**Dumpster diving**: Looking through an organization's trash for valuable information.

**Data diddling**: Changing data before they are entered into the computer.

The best control would be provided by having the **production control group** copy the source program to the production libraries and then **compile** the program.

**Software quality** can be expressed in two ways: defect rate and reliability. Software quality means conformance to requirements. If the software contains too many functional defects, the basic requirement of providing the desired function is not met. Defect rate is the number of defects per million lines of source code or per function point. Reliability is expressed as number of failures per 'n' hours of operation, mean time to failure, or the probability of failure free operation in a specified time

**Alternative routing provides** two different cables from the **local exchange** to your site, so you can protect against cable failure as your service will be maintained on the alternative route.

With **diverse routing**, you can protect not only against cable failure but also against local exchange failure as there are two separate routes from **two exchanges** to your site

**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.

**Alternative routing** provides two different cables from the local exchange to your site, so you can protect against cable failure as your service will be maintained on the alternative route. Furthermore, with **diverse routing**, you can protect not only against cable failure but also against local exchange failure as there are two separate routes from two exchanges to your site.

**Software quality program** should reduce defects, cut service costs, increase customer satisfaction, and increase productivity and revenues. To achieve these goals, commitment by all parties involved is the most important factor.

**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

The **incremental approach** - A service is designed bit by bit. Parts are developed separately and are delivered individually. Each piece supports one of the business functions that the entire service needs. The big advantage in this approach is its shorter delivery time. The development of each part, however, requires that all phases of the lifecycle are traversal.

The **iterative approach** - The development lifecycle is repeated several times. Techniques like prototyping are used in order to understand the customer-specific requirements better.

**The application gateway** is similar to a circuit gateway, but it has specific proxies for each service. (layer 7)

**Screening router and packet filter** 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).

**The importance of the network devices in the topology**.

**Reasonableness checks** A type of programmed edit check that tests whether the contents (e.g., values) of the data entered fall within predetermined limits.

**A circuit gateway** 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 established—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.

Initiating and subsequently approving a change request violates the principle of segregation of duties. **A person should not be able to approve their own requests.**

**Ineffective accounting** of production tape volumes could have serious implications such as loss of tape volumes containing critical information, improper disclosure of confidential data, and destruction of data caused by the improper use of tapes as scratch tapes.

Evidence must support the stated objectives of the organization. Software that is built or purchased should be carefully researched to ensure that it fulfills the organization's objectives. **Each phase of the life cycle should be reviewed and approved by management before progressing to the next phase**.

**Operations documentation** should contain recovery/restart procedures so that operations can return to normal processing, in a timely manner.

**Forward error control**: transmitting additional redundant information with each character or frame to facilitate detection and correction of errors.

**User management** assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirements definition, test case development, acceptance testing and user training.

**Feedback error control**: additional information is transmitted so the receiver can identify that an error has occurred.

**CRC:** a single set of check digits is generated, based on the contents of the frame for each frame transmitted.

**Bayesian filtering** applies statistical modeling to messages, by performing a frequency analysis on each work within the message and then evaluating the massage as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds.

Use of audit software merely refers to a technique that can be used in performing an audit. It has no relevance to the development of the **annual audit plan**.

**Bayesian filtering**; the filter spam based on probabilities and a score

**Biometric solution accuracy**: False Rejection Rate (FRR), Cross Error Rate(CER): When the false-rejection rate equals the false-acceptance rate and False Acceptance Rate

**False Acceptance Rate (FAR):** accepting an unauthorized person as authorized.

**False Rejection Rate (FRR)**: deny access to an authorized individual.

A common weakness in microcomputers is the = **Default booting from Drive** = may bypass installed security features.

**Equal Error Rate (ERR):** point where FAR equal the FRR
**A quality plan** is an essential element of all projects

**Segregating the Voice-over Internet Protocol (VoIP)** traffic using virtual local area networks (VLANs) would best protect the VoIP infrastructure from network-based attacks, potential eavesdropping and network traffic issues (which would help to ensure uptime).

Which of the following antispam filtering techniques would BEST prevent a valid, variable-length email message containing a heavily weighted spam keyword from being labeled as spam = **Bayesian (statistical)**

**Code correction** is a responsibility of the programming staff not the scheduling and operations personnel

Originating department to ensure that individual data elements are accurate != **DBA**

**False Identification Rate (FIR)**: probability that an authorized person is identified but is assigned a false ID.

Data may be permanently destroyed on a **hard disk** by a **wiping utility**, which uses random values to overwrite portions of the media. Security professionals use wiping utilities to clear hard disks for **redeployment**. Hackers use wiping utilities to destroy evidence, thereby covering their tracks.

**Reviewing system log** files is the only trail that may provide information about the unauthorized activities in the production library

**EDI** the communication's interface stage requires **routing verification procedures**

**EER** is the measure of the more effective biometrics control device.

**CER**: adjusting sensitivity of system

**Data classification** is the process of organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve = Reduced risk of inappropriate system access.

**Degaussing** is a popular technique for destroying data on magnetic storage tapes. By changing the magnetic field on the tape with a box-like device known as a degausser, the data on the tape can effectively be destroyed.

**Degaussing** the tapes is the process of magnetic tapes disposal.

**Message digests** in digital signature show if the message has been altered after transmission.

**CA (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.

**Registration Authority (RA):** responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA.

**Certificate Relocation List (CRL)**: instrument for checking the continued validity of the certificates.

**Certification practice statement**: is a detailed set of rules governing the certificate authority's operations.

Evaluating logical access controls should FIRST: **obtain an understanding of the security risk to information processing**.

**Digital signature** provides **integrity** and nonrepudiation. If we add hash it will provide confidentiality.

**Digital signature features**: Data Integrity, Authentication, Nonrepudiation, Replay Protection.

**Digital signature**: authenticity of the sender

**Nonrepudiation**: claimed sender can't later deny generating the sending the message.

**Data Integrity**: changes in the plaintext message that would result in the recipient failing to compute the same message hash.

**Authentication**: ensure that the message has been sent by the claimed sender.

**Replay protection**: method that a recipient can use to check that the message was not intercepted and replayed.

**Spoofing:** enable one party to act as if they are another party

**Repudiation of transactions**: cause major problems with billing systems and transaction processing agreements.

**Digital Certificates**: sender authentication method

**Digital Signature**: authentication and confidentiality, but the identity of the sender would still be confirmed by the digital certificate.

**Embezzlement**: a type of fraud involving employees or nonemployees wrongfully taking money or property entrusted to their care, custody, and control, often accompanied by false accounting entries and other forms of lying and cover-up

**RAID:**
RAID 0 = striping, no parity or mirroring
RAID 1 = mirroring
RAID 5 = striping with parity, supports drive failures, access speed depends on controller cache
RAID 6 = striping with double parity, supports faster access than RAID 5 (best price point and speed/redundancy)
RAID 10 = is a hybrid nested RAID configuration, has the fastest speeds and best redundancy but requires more drives

A read-only restriction= **integrity of stored data**

An **SLA** provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed-on service.

**Message authentication**: used for message integrity verification

**Authenticity**: pre-hash code using the sender's private key.

**Integrity**: Mathematically deriving the pre-hash code

**Asset classification** = determining the appropriate levels of information resource protection

**Confidentiality** = Encrypting the prehash code and message using the secret key

**SSL** provides data encryption, server authentication, message integrity and optional client authentication.

**SSL** use symmetric key for message encryption; use authentication code for data integrity; use hash function for generating message digest; use digital signature certificates for server authentication.

**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.

**Double-blind testing:** users are not aware about the penetration testing.

**Asymmetric Algorithms**
• RSA – factoring the product of two large prime numbers
• Diffie–Hellmann Algorithm – mathematical function based first on finding the primitive root of a prime number
• El Gamal – discrete logs
• Elliptic Curve Cryptography (ECC) - ECC implementations provides savings on computational power and bandwidth

**Targeted testing**: IT team is aware of the testing and penetration testers are provided with information related to target and network design.

The Code calls for informing appropriate parties of audit results, not interested parties = **ISCAF**

**RAID level 7** several high-speed disks (disk array) to be configured as one large virtual drive partition using asynchronous transfer mode

**Termination checklist** is critical to ensure the logical and physical security of an enterprise. In addition to preventing the loss of company property issued to the employee, there is the risk of unauthorized access, intellectual property theft and even sabotage by a disgruntled former employee. While the other choices are best practices, they do not present a significant risk to the organization.

The IS auditor should perform additional testing to ensure that it is a finding. An auditor can **lose credibility** if it is later discovered that the finding was not justified.

**Gateway** operates at application layer 7 in the OSI model. The function of the gateway is to convert data contained in one protocol into data used by a different protocol. An example is a PC-to-mainframe gateway converting ASCII to mainframe Extended Binary Coded Decimal Interchange Code (EBCDIC).

**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 (Prevents cost overruns and delivery delays)

**Confidentiality** - assurance that only owners of a shared secret key can decrypt a computer file that has been encrypted with the shared secret key.

**DFDs** = product of upper and middle CASE tools

**PBX Risks**: Theft of service - Disclosure of information - Data modification - Unauthorized access - Denial of service - Traffic analysis

Unless updated periodically, **anti-malware** software will not be an effective tool against malware

Application software package GREATEST risk = **Incorrectly set parameters**

**RA** - is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.

**TQM** purpose is end user satisfaction

**BCP takes into consideration**: •Those critical operations that are necessary to the survival of the organization •The human/material resources supporting them

Data warehouse = a repository of information of heterogeneous database

**BPR** = Envision, initiate, diagnose, redesign, reconstruct, evaluate

System migrations should include a phase of **parallel operation** or **a phased cut-over** to reduce implementation risk.

**Primary risk of BPR** is that controls are eliminated as part of the reengineering effort.

**An application-level edit check** to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

The **recovery point objective (RPO)** indicates the fallback position and duration of loss that has occurred. A valid RPO example is to recover by using backup data from last night's backup tape, meaning that the more recent transactions would be lost.

**Recovery time objective (RTO)** indicates a point in time that the restored data should be available for the user to access.

Understanding **complexity and risk**, and actively managing these throughout a project are critical to a successful outcome, main concern for IS Auditor.

Power Total failure = **blackout**

**Database views** are used to implement least privilege and restrict the data that can be viewed by the user.

**The manual log** will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a change log would most likely contain date information for the source and executable modules.

**Accreditation** A formal approval by management based on perceived fitness of use. Approval may be granted for a system, site location, or function. Accreditation occurs after system certification for a period of 90 days, 180 days, or one year. Systems must be reaccredited prior to expiration of their current accreditation period.

**Foreign key** Data in the database is stored in separate tables to improve speed. A foreign key is the link between data in different database tables. When the links are valid, the database has **referential integrity**.

**Referential integrity** When information contained in two or more data tables is valid across the links inside the database (foreign-key relationship). A failure of referential integrity indicates a failed program or corrupt database.

**Social engineering** is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal data.

**DAC** allows data owners to modify access, which is a normal procedure and is a characteristic of DAC.

**Best DRP**: Daily data backups that are stored offsite and a hot site located 140 kilometers from the main data center

**Post-Implementation Review (PIR)** is an assessment and review of the completed working solution. It will be performed after a period of live running; sometime after the project is completed.

**PIR:** to examine the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered. To learn lessons from this project, lessons which can be used by the team members and by the organization to improve future project work and solutions.

**PIR** should be scheduled some time after the solution has been deployed. Typical periods range from 6 weeks to 6 months, depending on the type of solution and its environment. The PIR is intended to be an assessment and review of the final working solution. There should have been at least one full processing and reporting cycle completed.

**PIR** should be timed to allow the final improvements to be made in order to generate optimum benefit from the solution. There is no point in waiting too long as the results are intended to generate that final benefit for the organization and team.

**Script-based** software is human readable and therefore can be crystal-box tested.

**Black-Box Testing** Intended to test the basic integrity of system processing. This is the most common type of test. The process is to put data through the system to see whether the results come out as expected. You do not get to see the internal logic structures; all you get is the output. Commercial software is compiled into a form that is nonreadable by humans.

**Black-box testing** is the standard test process to run when you buy commercial software. Black-box testing is often used for user acceptance tests.

**File layout**: Specifies the length of the file record and the sequence and size of its fields.

**White** = Crystal = Scripting

**Black** = Pre-Compiled

**SM = Senior Management =** ultimately responsible for information security within an organization

**Black Box** is to put data through the system to see whether the results come out as expected

**Guideline**: These are intended to provide advice pertaining to how organizational objectives might be obtained in the absence of a standard.

The **IDE integrated development environment** automates program code generation and provides online debugging for certain types of errors. It does not replace the traditional planning process. IDE does not alter the testing requirements in SDLC phase 4. Full testing must still occur.

**Certification is a technical testing process.** Accreditation is a management process of granting approval based on fitness of use.

**Policy**: Is an executive mandate to identify a topic containing particular risks to avoid or prevent. Policies are high-level documents signed by a person of significant authority with the power to force cooperation

**Procedures**: These are 'cookbook' recipes providing a workflow of specific tasks necessary to achieve minimum compliance to a standard. Details are written in step-by-step format from the very beginning to the end.

**Internal testing:** attacks and control circumvention attempts on the target from within the perimeter.

**External testing**: generic term that refers to attacks and control circumvention attempts on the target from outside that target system.

**Quality tools** = flow charts, Pareto chart, cause and effect (fishbone) diagram, Scatter diagram

Formal acceptance of an evaluated system by management = **Accreditation**

**Application software tracing and mapping**: Specialized tools that can be used to analyze the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences.

**Agile** method places greater reliance on the undocumented knowledge contained in a person's head. Agile is the direct opposite of capturing knowledge through project documentation.

Benefit of implementing an **expert system** is the: capturing of the knowledge and experience of individuals in an organization

**Session border controllers** enhance the security in the access network and in the core.

**Digital Signature**: used to detect unauthorized modifications and authenticate sender — provides non-repudiation — private key signs and public key verifies — used to authenticate software, data images, users, machines

**Key distribution center:** distribution method suitable for internal communication for a large group within an institution and it will distribute **symmetric keys** for each session.

**CA:** is a trusted third party that ensures the authenticity of the owner of the certificate.

**Kerberos** builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

**Retaining audit documentation:**In most cases, the archive of the integrated audit may need to be kept for seven years. Each type of audit may have a longer or shorter retention period, depending on the regulations identified during audit planning.

**L2-SW**: The purpose is to reduce network congestion by eliminating traffic that does not involve the specific station

**Replay attack**: residual biometric characteristics, such as fingerprints left on a biometric capture device may be reused to gain access.

The basis for continuous quality improvement is the **Plan-do-check-act** (PDCA) cycle.

**ITAF** includes three categories of standards-general, performance and reporting-as well as guidelines and tools and techniques

**Critical path** diagrams are used to determine the critical path for the project that represents the shortest possible time required for completing the project.

**Cold Site:** Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services.

**Compartmentalization:** A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.

The IPF should be visited on regular intervals to determine if **temperature and humidity are adequate.**

Preventing the leakage of confidential information in a laptop computer = DLP (**Encrypt the hard disk**)

A fire-suppression system with water stored in the pipes at all times; this type of system is susceptible to corrosion and freezing; **Wet pipe system**

**PERT** diagrams are a critical path method (CPM) technique in which three estimates (as opposed to one) of timelines required to complete activities are used to determine the critical path.

**FPA** is a technique used to determine the size of a development task, based on the number of function points.

**Gantt charts** help to identify activities that have been completed early or late through comparison to a baseline. Progress of the entire project can be read from the Gantt chart to determine whether the project is behind, ahead of or on schedule; important for IS Auditor in order to monitor the progress of the project.

**Escrow**: The client is entitled to the benefit of only using the software and not owning it, unless they pay more money. Escrow may provide some protection if the vendor goes out of business, but does not prevent software from being discontinued. The client is entitled to the benefit of only using the software, not the right of ownership. Software escrow may be requested by the client to gain full rights to the software if the vendor goes out of business

**Cryptographic attack**: Targets the algorithm or the encrypted data

**Mimic Attack:** reproduce characteristics similar to those of the enrolled user such as forging a signature or imitating a voice.

**Preparedness test involve simulation** of the entire environment and help the team to better understand and prepare for the actual test scenario.

**Preparedness test is a localized version of a full test**, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness.

**Walkthrough is a test involving a simulated disaster situation** that test the preparedness and understanding of management and staff rather than the actual resources.

**Paper Test (structured walk through) > Preparedness Test > Full Operational Test**

In **cost benefit analysis**, the total expected purchase and operational/support cost and qualitative value for all actions are weighted against the total expected benefits in order to choose the best technical, most profitable, least expensive, or acceptable risk option.

**A GPS receiver** reports on where the user is.

The most difficult part of a **quantitative risk analysis** is a determination of the probability that a threat will actually be realized. It is relatively easy to determine the value of an asset and the impact of a threat event.

**IT governance** is the mechanism through which IT strategy is established, controlled, and monitored through the balanced scorecard.

**Problem management** = processes is concerned with not only identifying the root cause but also addressing the underlying issue

Mitigate the risk of **internal fraud** = dealing with customers over the internet a trusted 3rd party should handle the CA.

Hardware is protected against power surges=**voltage regulator**

One of the advantages of **outsourcing** is: focus on core competencies.

It's a problem if you don't know when to **declare a crisis**

The use of an ID and password (what the user knows) is **a single-factor user authentication**.

The PRIMARY benefit organizations derive from effective information security governance is: ensuring **acceptable levels of disruption**.

The purpose of a **balanced scorecard** is: To measure organizational performance and effectiveness against strategic

The **project sponsor** is the owner of the project and therefore the most appropriate person to discuss whether the business requirements defined as part of the project objectives have been met.

The MOST important consideration in developing security policies is that: they are based on a **threat profile**.

**Checksum** calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications.

**Authenticity and authorization** cannot be established by a checksum alone and need other controls.

**Nonrepudiation** can be ensured by using digital signatures.

**Potential business impact** is only one part of the cost-benefit analysis.

**Integrity** of transaction process is ensured by database commits and rollbacks.

**A warm site** has the basic infrastructure facilities implemented, such as power, air conditioning and networking; but is normally lacking computing equipment.

**BIA** will identify the diverse events that could impact the continuity of the operations of an organization. Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers.

**DRP** is the technological aspect of business continuity planning (BCP). Business resumption planning addresses the operational part of BCP.

**Risk** The likelihood that an unfortunate event will occur and cause a loss of assets.

**Threat** A potential danger that, if realized, will have a negative effect on assets.

**The default login ID used for maintenance accounts** is frequently well known and commercially published.

**RTO** is an important parameter used when creating prioritization plans during the business continuity management process and is derived as a result of a business impact analysis (BIA**). RTO is best utilized to determine recovery prioritization.**

**Last mile circuit protection** Providing telecommunication continuity through providing redundant combinations of local carrier T1's, microwave and or local cable to access the local communication loop is the event of a disaster.

**Long haul network diversity** Providing diverse long distance network availability utilizing T-1 circuits among major long distance carriers.
**Diverse Routing:** Routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing.

**Alternate routing**: method of routing information via an alternative medium such as **copper cable or fiber optics**.

**Mitigation:** Schedule file and system backup

The use of an automated password management tool is a **preventive control measure.**

**Deterrence** : Installation of firewalls for information systems.

**Recovery** : hot site to restore normal business operations.

**BCP Process**: BIA => develop recovery strategy => developed, tested and implemented specific plans.

**Shadow file processing**, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently.

**Calculating cryptographic hashes** for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit.

**Electronic vaulting** electronically transmits data either to direct access storage, an optical disk or another storage medium; this is a method used by banks.

A server running a **DLP** software application uses predefined criteria to check whether any confidential documents or data are leaving the internal network.

The integrated development environment **IDE** automates program code generation and provides **online debugging** for certain types of errors. It does not replace the traditional planning process.

**IDE** does not alter the testing requirements in **SDLC phase 4**. Full testing must still occur.

**IDE = Debugging**

**Hard-disk mirroring** provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server.

**The best way to handle obsolete magnetic tapes is to degauss them**

The major benefit of implementing a **security program** is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risk.

**Electronic vaulting** A process of transmitting data to a remote backup site. This ensures that the most recent files are available in the event of a disaster. A common implementation is to transmit live data files to a remote server.

**The IS auditor should make the final decision about what to include or exclude from the audit report.**

**An ITF is an audit technique to test the accuracy of the processes in the application system.** It may find control flaws in the application system, but it would be difficult to find the overlap in key controls.

By testing controls to validate whether they are effective, the IS auditor can identify whether there are overlapping controls; however, **the process of implementing an automated auditing solution would better identify overlapping controls.**

Having the **service provider sign an indemnity clause will** ensure compliance to the enterprise's security policies because any violations discovered would lead to a financial liability for the service provider =NDA

**Recovery controls** restore lost computing resources or capabilities and help the organization to return to normal operations and recover monetary losses caused by a security violation or incident.

**Compensating controls** reinforce or replace normal controls that are unavailable for any reason. These are typically backup controls and usually involve higher levels of supervision and/or contingency plans.

**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

**Hot site** is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

**Indemnity** - protection against future loss

**Black-box** test is a dynamic analysis tool for testing software modules

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches = **Provide an audit trail**

**Employee access to information systems should be promptly terminated**. The accounts for contractors no longer employed by the organization should be suspended. All accounts should be reviewed before the account is deleted.

**Stress testing** should be carried out in a: test environment using live workloads.

The adequacy of **security awareness** content can best be assessed by determining whether it isperiodically reviewed and compared to industry best practices.

Change an organization's culture to one that is more security conscious; **Security awareness campaigns**

The recovery point objective (RPO) is the earliest point in time at which it is acceptable to recover the data. **A high RPO means that the process can wait for a longer time.**

**A high recovery time objective (RTO) means that additional time would be available** for the recovery strategy, thus making other recovery alternatives.

The **ratio of false positives to false negatives** will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while, at the same time, minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

Calculating the value of the information or asset is the first step in a **risk analysis** process to determine the impact to the organization, which is the ultimate goal.

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss => **Calculate the value of the information or asset**

**The lower the RTO the lower the disaster tolerance**

**NDMP** data service, tape service, Network Storage, translator service

**IT governance**: A clearly stated process of leadership to lead and control the performance expected from the IT function. The focus of IT governance is control over the technology environment.

**Periodic review of the access list by the business owner should determine whether errors in granting access have occurred**

**Business continuity self audit** is a tool for evaluating the adequacy of the business continuity plan.

**hashing algorithm** can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

**Resource recovery analysis** is a tool for identifying a business resumption strategy.

The main advantage of **elliptic curve encryption** over RSA encryption is its computation speed.

**Structural testing** != Stress testing

**Performance testing**: Spike testing; Volume testing; Endurance testing

**Performance testing**: eliminate bottlenecks and establish a baseline for future regression testing.

**Load testing** is usually defined as the process of exercising the system under test by feeding it the largest tasks it can operate with. Load testing is sometimes called volume testing, or longevity/endurance testing.

**Stress testing** tries to break the system under test by overwhelming its resources or by taking resources away from it (in which case it is sometimes called negative testing). The main purpose behind this madness is to make sure that the system fails and recovers gracefully -- this quality is known as recoverability.

**Gap analysis** in business continuity planning is to identify deficiencies in a plan.

**Fidelity insurance:** covers the loss arising from dishonest or fraudulent acts by employees.

**Business interruption insurance:** loss of profit due to the disruption in the operations of an organization

**IS steering committee** A committee composed of business executives for the purpose of conveying current business priorities and objectives to IT management. The steering committee provides **governance** for major projects and the IT budget.

IS policies, IS procedures, standards and guidelines are all structured to support the overall **strategic plan.**

**Load testing**- test of applications with large quantities of data to evaluate its performance = DB application concurrently

**Volume-testing** with an incremental volume of records to determine maximum volume of records (data) that appn can process

**Errors & omissions insurance:** legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client.

**Extra expense insurance:** designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

**Stockholders interview** = simplicity of the BCP

**Review plan and compare it with standards** = adequacy of the BCP

**(ROI) should be re-performed to verify that the original business case benefits are delivered.**

**Review result from previous test** = Effectiveness of the BCP

**In RAD model the functional modules are developed in parallel** as prototypes and are integrated to make the complete product for faster product delivery.

Something with DB architectures as a data-oriented structured database (DOSD) and an object-oriented structured database (OOSD)
**Compliance testing** determines whether controls are being applied in compliance with policy.

**Variable sampling** is used to estimate numerical values such as dollar values.

**Substantive testing** substantiates the integrity of actual processing such as **balances of financial statements**.

**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.

**Substantive test** includes gathering evidence to evaluate the integrity (i.e., the completeness, accuracy or validity) of individual transactions, data or other information. **Conducting a physical count of the tape inventory is a substantive test.**

**Attribute sampling** primary sampling method used for compliance testing.

**Prevent DOS = filter outgoing traffic with IP source addresses external to the network.**

**Attribute sampling** is a sampling model that is used to estimate the rate of occurrence of a specific quality in a population and is used in compliance testing to confirm whether the quality exists.

**An audit charter should state management's objectives for the delegation of authority to IS audit.**

The IS auditor needs to perform **substantive testing** and an additional analysis in order to determine why the approval and workflow processes are not working as intended.

**By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process.**

**CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.**

**Tracing involves** following the transaction from the original source through to its final destination. In **EFT transactions**, the direction on tracing may start from the customer-printed copy of the receipt, checking the system audit trails and logs, and finally checking the master file records for daily transactions

**MIS** an organized assembly of resources and procedures required to collect process and distribute data for use in decision making

**DATA Mapping:** diagramming data that are to be exchanged electronically, including how they are to be used and what business management systems need them.

Refers to a point backward in time to which the loss of data is acceptable. This means work created since the last data backup will be lost; **RPO**

**Masking:** A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report

**War driving** is a term used to describe the process of a hacker who, armed with a laptop and a wireless adapter card and traveling via a car, bus, subway train, or other form of mechanized transport, goes around sniffing for WLANs.

**War walking** refers to the same process, commonly in public areas like malls, hotels, or city streets, but using shoe leather instead of the transportation methods listed above.

**Pandemic planning**: presents unique challenges; unlike natural disasters, technical disasters, malicious acts or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration

If the IS plan is a separate plan, it must be consistent with and support the **corporate BCP**.

A risk-based audit approach focuses on the understanding of the nature of the business and being able to identify and categorize risk. Business risks impact the long-term viability of a specific business. Thus an IS auditor using a risk-based audit approach must be able to understand **business processes**.

Symmetric-key encryption= **WEP**

**Master file**: A file of semi-permanent information that is used frequently for processing data or for more than one purpose

**Contraband software**: At government offices, any system utility or special software not required in the specific performance of a person's job duties

Administrative process of being able to prove the documented design as built, by **verifying the correct version of all the individual components used in final construction**: **Configuration management**

**Materiality**: An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.

**Maturity**: In business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives

**Media access control:** Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card

**Media oxidation:** The deterioration of the media on which data are digitally stored due to exposure to oxygen and moisture

**Memory dump:** The act of copying raw data from one place to another with little or no formatting for readability

**Microwave transmission:** A high-capacity line-of-sight transmission of data signals through the atmosphere which often requires relay stations

**Monetary unit sampling**: a sampling technique that estimates the amount of overstatement in an account balance

**The inclusion of technical information in error messages**

**Mobile code:** software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

When reviewing system parameters, an IS auditor's PRIMARY concern should be that: **they are set to meet security and performance requirements.**

**CMM** is a qualitative approach typically using a 0 to 5 scale with each value assigned a set of attributes or characteristics to determine a relative level of competency and proficiency.

**In symmetric-key cryptography, symbols are permuted or substituted: in asymmetric-key cryptography, numbers are manipulated**

**Digital signature** needs a public-key system. The signer signs with her private key, the verifier verifies with the signer's public key.

**Cryptosystem** uses the private and public keys of the recipient: a digital signature uses the private and public keys of the sender.

**SSL:** Asymmetric encryption is necessary to verify the others identity and then symmetric encryption gets data.

**SSL** use to privately share the session key = Asymmetric

**SSL** use to encrypt the session data = Symmetric

**SSL** use Asymmetric and symmetric

Enabling **audit trials** helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system.

In **business process control assurance** you should look for: process map, process controls, benchmarking, roles and responsibilities and data restrictions.

When designing an audit plan, it is important to identity the **areas of highest risk** to determine the areas to be audited.

**Control Self Assessment (CSA)** is predicated on the review of **high-risk areas** that either need immediate attention or a more thorough review at a later date.

**CSA** is the review of business objectives and internal controls in a formal and documented collaborative process.

**The scope of an IS audit should not be** constrained by the ease of obtaining the information or by the auditor's by the auditor's familiarity with the area being audited.

An **assessment of risk** should be made to provide reasonable assurance that material items will be adequately covered during the audit work.

**Audit risk** is the **combination of detection, control and inherent risks** for a given audit assignment.

**Control risk** is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls.

**Substantive Testing:** Are transactions processed accurately? Are data correct and accurate? Double check processing, Calculation validation, Error checking, Operational documentation, If Compliance results are poor, Substantive testing should increase in type and sample number.

**Inherent risk** is the risk that an error exists in the absence of any compensating controls.

**RTO:** how long business can afford the downtime or crisis

**RPO:** till what point of time you want the data to be recovered

**BSC** does not measure financial growth

The primary objective of **forensic software** is to preserve electronic evidence to meet the rules of evidence.

**Generalized audit software** feature include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations.

The goal of the meeting is to confirm the factual accuracy of the audit findings and present an opportunity for **management to agree on corrective action.**

**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.

**If the RTO is high**, then the acceptable downtime is high. A **cold site** will be appropriate in such situations.

**Audit program**: A step-by-step set of audit procedures and instructions that should be performed to complete an audit.

**A directory server makes other users' certificates available to applications.**

A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population; **Statistical sampling**.

**Understanding** the business process is the first step an IS auditor needs to perform.

**Confidentiality** of customer data = IMPORTANT

**Reciprocal agreement**; hardware and software compatibility.

A testing approach that uses knowledge of a program/module's underlying implementation and code intervals to verify its expected behavior: **White box testing**

Compares data to predefined reasonability limits or occurrence rates established for the data; **Reasonableness check**

**Preparedness test** involve simulation of the entire environment and help the team to better understand and prepare for the actual test scenario; **Preparedness test** is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan

**Potential business impact** is only one part of the cost-benefit analysis.

**OOB:** Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks.

**Integrity** of transaction process is ensured by database commits and rollbacks.

A telecommunications methodology that controls traffic in which a complete message is sent to a concentration point and stored until the communications path is established. **Message switching**

A warm site has the basic infrastructure facilities implemented, such as power, air conditioning and networking. But **is normally lacking computing equipment.**

**Compliance tests are performed primarily to verify whether controls**, as chosen by management, are implemented.

**Verification of documents is not directly related to compliance testing.** Verifying whether access to users is provided is an example of compliance testing. Data validation procedures are part of application controls. Testing whether these are set as parameters and working as envisaged is compliance testing.

**Application Controls** are usually classified in three categories, Preventive, Corrective, or Directive. No control is gained by a routine that analyses an exposure.

Implement a properly documented process for **application role change requests**.

**Hot site:** An alternate processing facility that is fully equipped with all the necessary computer equipment and capable of commencing operation as soon as the latest data files have been loaded. **Capable of being in full operation within minutes or hours.**

**BIA** will identify the diverse events that could impact the continuity of the operations of an organization. Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers.

Proceeding with restore procedures of DB is a **corrective** control. Restore procedures can be used to recover databases to their last-known archived version.

Establishing standards is a **preventive control**

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.**

**FPA:** A software estimation method used to forecast development, based on the number of system inputs, outputs, and complexity. Used in the SDLC feasibility study to calculate resources and time required.

**DRP** is the technological aspect of business continuity planning (BCP). Business resumption planning addresses the operational part of BCP.

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear **business case**.

**RTO** is an important parameter used when creating prioritization plans during the business continuity management process and is derived as a result of a business impact analysis (BIA). RTO is best utilized to determine recovery prioritization. **A system that has a low level of confidentiality of information could have immediate recovery requirements.**

**The internal control objectives apply to all areas, whether manual or automated.** But the common control objectives in an IS environment remains unchanged from a manual environment.

The identification of key deliverables required to deliver business value is a key element of project planning. It provides the initial basis for planning and should be done during **initial planning**

**HIPAA** handles health care information of an organization.

**Succession planning** is a process for identifying and developing internal people with the potential to fill key business leadership positions in the company. Succession planning increases the availability of experienced and capable employees that are prepared to assume these roles as they become available

If the auditee disagrees with the impact of a finding, it is **important for an IS auditor to elaborate and clarify the risk and exposures**

**Procedures that verify that only approved program changes are implemented**

**Long haul network diversity** Providing diverse long distance network availability utilizing T-1 circuits among major long distance carriers.

**It is common for system development and maintenance to be undertaken by the same person.**

**Diverse Routing:** Routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing.

**CRL:** list maintained by the certificate authority indicating certificates that are revoked or expired

**Compliance** test is deals with test of details; **Substantive** deals with test of controls

**Alternate routing:** method of routing information via an alternative medium such as copper cable or fiber optics.

**Intrusion detection systems** detect intrusion activity based on the intrusion rules. It can detect both, external and internal intrusion activity and send an automated alarm message.

**Firewalls and routers** prevent the unwanted and well-defined communications between the internal and external networks. They do not have any automatic alarm messaging systems.

**System utilities** may enable unauthorized changes to be made to data on the **client-server database**. In an audit of database security, the controls over such utilities would be the primary concern of the IS auditor.

**Application program** generators are an intrinsic part of client-server technology, and the IS auditor would evaluate the controls over the generators access rights to the database rather than their availability.

**Security documentation** should be restricted to authorized security staff, but this is not a primary concern, nor is access to stored procedures.

**The services in the agreement** are based on an analysis of business needs**.**

**BCP Process**: BIA => develop recovery strategy => developed, tested and implemented specific plans.

**Shadow file processing**, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently.

What is the name of leftover disk space that may contain old deleted data that has not yet been overwritten: **Slack space**

**Dumpster diving**: The process of digging through trash to recover evidence or improperly disposed-of records. The same process is frequently used by government agents and law enforcement to gather evidence; therefore, it's completely legal unless the person is trespassing.

**CA** 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.

**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.

**CRL** is an instrument for checking the continued validity of the certificates for which the CA has responsibility.

**Default database configurations**, such as default passwords and services, need to be changed; otherwise, the database could be easily compromised by malicious code and by intruders.

Senior executives with full delegation of authority during business continuity events or disaster recovery to make decisions on behalf of the entire organization without additional delays or approval of other executives**: EMT**

**Electronic vaulting** electronically transmits data either to direct access storage, an optical disk or another storage medium; this is a method used by banks.

**Parallel redundant UPS configuration** requires models of the same capacity from the same manufacturer and isolated redundant does not.

**Isolated redundant UPS design** concept does not require a paralleling bus, nor does it require that the modules have to be the same capacity, or even from the same manufacturer.

**Hard-disk mirroring** provide redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server.

The process of removing duplicate, redundant data from a database; **Normalization**

To commit fraud by masquerading as a legitimate user or another system; **Spoofing**

The recovery point objective **(RPO)** is the earliest point in time at which it is acceptable to recover the data. A high RPO means that the process can wait for a longer time. A high Recovery time objective **(RTO)** means that additional time would be available for the recovery strategy, thus making other recovery alternatives.

**Data integrity**: the goal is to ensure that data is accurate and safely stored

**Backup and restoration**: what are the plans and procedures for data backup and restoration? The number one issue in IT is loss of data due to faulty backup

**Security management:** Without security controls, ensuring data integrity is impossible. Internal controls prevent unauthorized modifications.

**Mandatory versus Discretionary controls:** The organization needs to clearly identify its management directives for implementation of controls.

**Mandatory control: the strongest type of control.** The implementation may be administrative or technical. It is designed to force compliance without exception.

**Discretionary controls: the weakest type of control is discretionary**. In a discretionary control, the user or delegated person of authority determines what is acceptable.

**The lower the RTO is the lower the disaster tolerance.**

**Risk assessment and business impact assessment** are tools for understanding business-for business continuity planning.

**IT steering committee or IT strategy committee** is used to convey the current business requirements from business executives to IT executive. It should have a formal charter designating the participation of each member. This charter grants responsibility and authority in a concept similar to an audit charter.

The auditor should remain aware that a **shadow organization represents** a genuine control failure. This lack of integration represents an ongoing concern in the areas of cost control, duplication of effort, or a political difference in both direction and objectives.

**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.
**Business continuity self audit** is a tool for evaluating the adequacy of the business continuity plan.

**Resource recovery analysis** is a tool for identifying a business resumption strategy.

**Gap analysis** in business continuity planning is to identify deficiencies in a plan.

**Fidelity insurance** > covers the loss arising from dishonest or fraudulent acts by employees.

**Business interruption insurance:** loss of profit due to the disruption in the operations of an organization.

**Errors & omissions insurance:** legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client.

**Extra expense insurance** > designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

ECC was designed for appliances with low computing power such as **mobile phones**

**Stockholders interview** > simplicity of the BCP

**Review plan and compare it with standards** > adequacy of the BCP

**Review result from previous test** > Effectiveness of the BCP
Bank Wire Transfer: **Integrity represents accuracy of data**. Because this data is required by law, it must be accurate and validated.
**Having data in multiple countries is the greatest concern** because human resources (HR) applicant data could contain personally identifiable information (PII). There may be legal compliance issues if these data are stored in a country with different laws regarding data privacy

**PERT chart** > will help determine project duration once all the activities and the work involved with those activities are know.

**Function point analysis:** is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files.

**Standardized infrastructure** may simplify testing of changes, but it does not reduce the need for such testing.

**Standardized IT infrastructure** provides a consistent set of platforms and operating systems across the organization.

This standardization **reduces the time and effort required to manage a set** of disparate platforms and operating systems. It can help the organization **reduce the cost of IT service** delivery and operational support

**Rapid Application Development:** is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

**Object-oriented system development:** is the process of solution specification and modeling.

**Completeness check:** is used to determine if a field contains data and not zeros or blanks.

**Check digit:** is a digit calculated mathematically to ensure original data where not altered.

**Existence check:** checks entered data for agreement to predetermined criteria.

**Reasonableness check:** matches input to predetermined reasonable limits or occurrence rates.

**Functional acknowledgements** are standard electronic data interchange (EDI) transactions that tell trading partners that their electronic documents are received.

Risk within the process of decision support systems (DSSs) => **Inability to specify purpose and usage patterns**

**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.

**Wet pipes** have water right up to the sprinkler heads; that is, the pipes are "wet." The sprinkler head contains a metal (common in older sprinklers) or small glass bulb designed to melt or break at a specific temperature.

**Storing certificate revocation lists (CRLs)** is a role performed by a security server.

**Redundancy check** detects transmission errors by appending calculated bits onto the end of each segment of data.

**Reasonableness check** compare data to predefined reasonability limits or occurrence rates established for the data.

**Parity check:** hardware control that detects data errors when data are read from one computer to another.

**Generally a cold site is contracted for a longer period at a lower cost.**

**A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.**

**Compliance Testing:** Are controls in place and consistently applied? Access control, Program change control, Procedure documentation, Program documentation, Software license audits
System log reviews, Exception follow-ups

In general, an **audit charter** describes **all the scopes** of audit activities of an organization, whereas an **engagement letter** describes a particular audit activity that needs to be undertaken **to achieve a specific** objective of an Audit

**Check digits:** detect transposition and transcription errors.

**Prototype system:** provide significant time and cost savings. Also have several disadvantages like poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added.

**Isolation:** while in an intermediate state, the transaction data are invisible to external operations.

**To ensure authenticity and confidentiality**, two encryption operations are required. First the hash of the message will be encrypted with the sender's private key. This creates a digital signature of the message which proves message integrity and the sender's authenticity. Then the message must be encrypted with the receiver's public key, which provides message confidentiality

Encrypting a message with the recipient's public key and decrypting it with the recipient's private key ensures message confidentiality. Conversely, encrypting a message with the sender's private key and decrypting it with the sender's public key ensures that the message came from the sender; however, it does not guarantee message encryption. With **public key infrastructure** (PKI), a message encrypted with a private key must be decrypted with the responding public key, and vice versa.

**Unregulated compliance issues are a risk but do not measure the effectiveness of the controls**.

**Durability** Guarantees that a successful transaction will persist, and cannot be undone. Hardware maintenance program should be validated against vendor specifications. Maintenance schedules normally are not approved by the steering committee. Unplanned maintenance can't be scheduled.

**Library control software** should be used to separate test from production libraries in mainframe and / or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized.

**Library control software is concerned with authorized program changes** and would not automatically move modified programs into production and can't determine whether programs have been thoroughly tested.

**Referential integrity** is provided by foreign key.

**Post-incident review** improve internal control procedures.

**Capacity management** is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively.

Determine **unauthorized changes** made to production code the auditor examine object code to find instances of changes and trace them back to change control records.

**Normalization:** is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and risk of not maintaining consistency of data, with the consequent loss of data integrity.

**Software development project**: the users should be involved in the requirements definition phase of a development project and **user acceptance test specification** should be developed during this phase

**Compensating Controls** – They are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated.

**Preventive Controls** - These are controls that prevent the loss or harm from occurring. For example, a control that enforces segregation of responsibilities (one person can submit a payment request, but a second person must authorize it), minimizes the chance an employee can issue fraudulent payments.

**Determine future capacity**, is the first step in the capacity planning process.

Before implementing an **IT balanced scorecard**, an organization must define **key performance indicators.**
To assist an organization in planning for IT investments, the IS auditor should recommend the use of **enterprise architecture.**
**Controls** are basically to mitigate the risk.

Real time Data Synchronization between DC and DR systems is done to avoid any data loss. This can be measured by the **RPO** as a parameter

**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.

**capacity cushion:** Extra amount of capacity intended to offset uncertainty in demand

**The production libraries** represent executables that are approved and authorized to process organizational data.

**IS audit services can be provided externally or internally.**

The role of **IS internal audit** function should be established by an **audit charter approved by senior management.**
If IS audit services are **provided externally,** then it should be **documented in a formal contract or statement of work between the contracting org. and the service provider.**

**Swim lane** is a visual element used in process flow diagrams, or flowcharts, that visually distinguishes job sharing and responsibilities for sub-processes of a business process. Swim lanes may be arranged either horizontally or vertically. In the accompanying example, the swim lanes are named Customer, Sales, Contracts, Legal, and Fulfillment, and are arranged vertically.

**CSA techniques =** identify high-risk areas that might need a detailed review later.

An IS auditor should expect **References from other customers (an item)** to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP).

**Screened subnet** (also known as a "triple-homed firewall") is a network architecture that uses a single firewall with three network interfaces (External, Internal, DMZ).

Maintaining the integrity of the **evidence** should be the foremost goal

**IT governance** ensures that an organization aligns its IT strategy with enterprise objectives.

To propagate itself to the host systems, a **worm** typically exploits security weaknesses in operating systems' configurations. These problems are particularly severe in today's highly decentralized client-server environments.

**COSO** –They provide internal Control framework.

**Basel II Accord** – It regulates the minimum amount of capital 4 financial org. based on the level of risk faced by these org.
An IS auditor should ensure **that IT governance performance** measures **evaluate the activities of IT oversight committees.**

**IS strategic** plans would include analysis of future business objectives.

It's a file backup method that copies every file that has been added or changed since the last full backup. This type of **backup does not set the final archive bit flag**; **Diff Backup**

**Scope Creep - Scope creep (also called requirement creep and feature creep) in project management refers to uncontrolled changes** or continuous growth in a project's scope. This phenomenon can occur when the scope of a project is not properly defined, documented, or controlled. It is generally considered a negative occurrence, to be avoided.

**Discovery sampling**: The process of searching 100 percent of the available records for specific attributes to determine the probability of occurrence

**Foreign key:** Data in the database is stored in separate tables to improve speed. This provides a link between data in two different database tables.

**Waterfall model** : An early software development model that cascades the completion of each phase into the next phase

**Trapdoor**: A hidden software-access mechanism that will bypass normal security controls to grant access into the program

**Time bomb:** Technique used by programmers in computer software to disable the functionality of the program based on a specific date

**Compliance audit**: A type of audit to determine whether internal controls are present and functioning effectively.

The attack that has not been seen before called; **Zero-day attack**

Access control model allows the system owner to establish access privileges to the system = **DAC**

The protection of information held in secret for the benefit of authorized users > **Confidentiality**

**Hardware Configuration Analysis** is critical to the selection and acquisition of the correct operating system software**.**

When conducting a review of business process reengineering, IS auditor found that a key preventive control had been removed. The IS auditor should **inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.**

**Data sanitization** is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device.

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

Online vendor provides the use of commercial software through subscription; **SAAS**

Eavesdropping and other covert techniques used to collect information; **Passive attack**

**Worms** are malicious programs that operate independently exploiting authentication holes between systems.

**Viruses** attach to programs or files and travel when the host file is transferred.

Information in the computer's working memory (RAM) that will be lost when the power is shut off; **Volatile data**

Network diagram **is the most important first step in understanding the auditee's IT infrastructure**

A planned method of testing and tracking minor software updates prior to implementing them into production. The cost of separate testing can be justified by using the price of failure (price of nonconformance); **Patch management**

Proxy server = **circuit-level firewall**

What do you call a set of commands and macros developed into a custom template inside an integrated development environment (IDE) programming tool? **Pseudocode**
An organization decides to purchase a package instead of developing it. In such a case, the design and development phases of a traditional software development life cycle (SDLC) would be replaced with **selection and configuration phases.**

The goal of **computer forensics** is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

If you use an **HTTPS** connection to a web site, then the data is encrypted with a public key before it ever leaves the computer. So if someone is sniffing the connection with promiscuous WiFi, then it's useless data to them unless they have the private key.

A newer security protocol used in wireless networks with **automatic encryption-key generation** and authentication **EAP**

**Trend/variance detection tools** look for **anomalies in user or system behavior**, such as invoices with increasing invoice numbers.

**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.

**CASE** tools are used to assist in software development.

The process of determining risks affecting the actual steps necessary to produce the desired product or service, as in use by the organization; **BIA**

**Embedded (audit) data collection software**, such as systems control audit review file (SCARF) or systems audit review file (SARF), is used to provide sampling and production statistics, but not to conduct an audit log analysis.

**Information held in computer resources**, such as the contents of a server's random access memory (RAM) memory, is the best information source when investigating a server compromise.

**Wet stacking:** If this happens too often, generator fires can occur, usually when the generator is put under load due to a utility outage.

**UPS system** is an alternate or backup source of power with the electric utility company being the primary source. The UPS provides protection of load against line frequency variations, elimination of power line noise and voltage transients, voltage regulation, and uninterruptible power for critical loads during failures of normal utility source. An UPS can be considered a source of standby power or emergency power depending on the nature of the critical loads.

The objectives of CSA programs include education for line management in control responsibility and monitoring and concentration by **all on areas of high risk**

Used in disaster recovery testing to simulate the basic recovery process in order to clean any errors from the procedure; **Functional testing**

To sharpen the details of an average population by using a stratified mean (such as demographics) to further define the data into small units; **Defuzzification**

The risk that errors may be introduced or may not be identified and corrected in a timely manner; **Control risk**

Faster restoration of data files: **differential backup**

The probability of error; A rating of 95 percent is considered a **Confidence Coefficient** in IS auditing.

A standardized reference listing of all the programmer's data descriptions and files used in a computer program; **Data dictionary**

A secret point of entry into a system; usually a hidden access technique left in the software by the developer for future use by their technical support staff; **Trapdoor**

A historical score of business process performance; Unfortunately, the score may indicate that a failure has occurred before corrective action can be taken. **KPI**

The process of streamlining existing operations in an effort to improve efficiency and reduce cost; Benefits may be derived by eliminating unnecessary steps as the organization has progressed through the learning curve, or by expanding capability for more work. **BPR**

A malicious hacker program designed to unsuspectingly install a backdoor without the consent of the system user. This will subvert the operating system kernel security and operate in stealth to hide its existence. **ROOTKIT**

Data tables is valid across the links inside the database; **Referential integrity**

A system development technique used to create initial versions of software functionality. Focused on proving a method or gaining early user acceptance, usually without any internal controls; **Prototype**

Access control model grants a user a predetermined level of access based on the role the user holds in the organization; **RBAC**

A device used in forensic investigations to prevent any changes to the original data on the hard disk or media during bitstream imaging; **Write blocker**

**Capacity Management** process used to manage information technology (IT). Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner.

Persistent data retained on the hard disk and other storage media after system shutdown; **Nonvolatile data**

Eliminating the opportunity for a person to reject or renounce their participation; **Nonrepudiation**

Used to determine the critical path and to forecast the time and resources necessary to complete a project; **PERT**

Used to designate a prorated dollar amount or weight of effectiveness to an entire subject population; **Variable sampling**

A physical distance between two doorways that is designed to trap an unauthorized individual between the closed doors. Fully caged turnstiles can provide a similar means to capture potential intruders; **Mantrap**

Evidence that can be reassembled in chronological order to **retrace a transaction or series of transactions**; **Audit trail**
Low voltage for an extended period of time; **Brownout**

A technique used by antivirus software to replace the original **end-of-file (EOF)** marker with a new EOF marker generated by the antivirus program. Anything attempting to attach itself to the new EOF marker indicates a virus attack;
**Inoculation//Immunization**

A unique entry into a database record that is required for the record to be valid; **Primary key**

Adjusting the sensitivity of a biometric system to use a **50/50 compromise** of false acceptance and false rejection; **EER**

The process of physically marking insecure wireless access points to the Internet; **War chalking**

A special template of **biometric data** converted into a count of specific characteristics that are unique to each user; **Minutiae**

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 redundancy of data.**
**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**.**

**Resilience -** The ability to recover quickly from illness, change, or misfortune; buoyancy.

**Certification practice statement (CPS);** In public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key

**Input Authorization**: Online Access Controls, Signature on batch, unique password, terminal, source document.

High humidity = **Corrosion**

Low humidity = **generate static electricity**

**Above raised floor**: Humidity

**Under raised floor**: Detecting water leaks

**Library control software** - to provide reasonable assurance that program changes have been authorized.

**Enabling audit trails helps** in establishing the accountability and responsibility of processed transactions by tracing transactions through the system.

**Preparedness test** is a localized version of a full test, wherein resources are expended in the simulation of a system crash.

**Walk-through** is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff rather than the actual resources.

**Benchmarking** provides the BEST method for determining the level of performance provided by similar information-processing-facility environments.

**Traffic analysis**, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, the intruder is able to guess the type of communication taking place.

**Naming conventions** for system resources are important for access control because they reduce the number of rules required to adequately protect resources.

**Social engineering**: art of manipulating people into performing actions or divulging confidential information.

**Security awareness training** is the most effective way to reduce social engineering incidents.

The IS auditor must examine the **database initialization parameters.**

**Preparedness test**— Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash.

**EDI translator**— This device translates the data between the standard format (ANSI X12) and a trading partner's proprietary format.

**Digital signatures** are used for (authentication and nonrepudiation)

**Insurance coverage** = reflect the actual cost of recovery, coverage for media damage, business interruption, equipment replacement and business continuity processing should be reviewed for adequacy

The **data dictionary** contains an index and description of all of the items stored in the database.

The **directory system** describes the location of the data and the access method

**Effective security management** = Resource mangmnt + Process Intg. + Performance mangmnt.

**Inherent risks** exist independently of an audit and can occur because of the nature of the business

**Risk appetite** is the amount of risk that an enterprise is willing to take

**Risk appetite** is about the pursuit of risk while risk tolerance is about what the organization can deal with. Risk tolerance should therefore be within risk appetite levels. They are two different though closely related concepts

**Computer-assisted audit technique (CAAT)**— Any automated audit technique, such as generalized audit software (GAS), test data generators, computerized audit programs and specialized audit utilities

**Diff. backup:** A restore requires more media capacity

**Middleware** = transaction monitoring + remote call + object request + messaging server

The risk level or exposure without taking into account the actions that management has taken or might take is **inherent risk**

**Generally Accepted Accounting Principles (GAAP)** A well-recognized set of agreed-upon procedures for auditing financial records and information systems.

RPO indicates the latest point in time at which it is acceptable to recover the data.

Reviewing the conceptual data model or the stored procedures will not provide information about **normalization**.

**Certificate Authority:** A CA is a network authority that issues and manages security credentials and public keys for message encryption.

**Sniffing vs Spoofing -** sniffing: to gather information without actually touching it (or being detected or in hiding), e.g., network packet sniffing. Sniffing is "listening" to network traffic to collect information. A common usage of sniffing is to listen to network traffic to look for patterns of a worm spreading itself.

**Spoofing :** is sending network traffic that's pretending to come from someone else. a common usage for spoofing is sending an email message, but to reformat the header so it looks like it comes from someone else, like their boss.

**Network security reviews** include reviewing router access control lists, port scanning, internal and external connections to the system, etc.

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

**Concerns in BCP**; if nobody declares the disaster, the response and recovery plan would not be invoked

**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 data flow diagrams may be useful, detailed program diagrams and file definitions are not.

**Ensuring periodic dumps** of transaction logs is the only safe way of preserving timely historical data

**Avoid out-of-range data** = integrity constraints in the database

**NDMP** is more or less network attached storage-centric (NAS-centric) and defines a way to back up and restore data from a device,

**NDMP** defines three kind of services: data service + tape service + translator service performing

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

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.

**Pharming** can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS

The most reliable sender authentication method is **Digital Certificates.**

**Digital certificates** are issued by a trusted third party

BEST risk response to the risk of loss of confidentiality in cloud computing = **Public key infrastructure**

**Software size estimation**: Lines of code – SLOC (# of lines of source code), better for basic or Cobol//Function Point analysis – used to estimate complexity in developing large apps. **Software Cost estimates directly related to software size estimates.**

**Tape backup** = preventive control

**Verify the backup** = detective control

**Detective** = fix problem after it's found

**Verification and audits** = detective controls

An **integrated test facility** is a type of substantive test that uses data represented by fake entities such as products, items, or departments

An **application-level gateway** is **the best way to protect against hacking** because it can define with detail rules that describe the type of user or connection that is or is not permitted.

**Firewall** is software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set.

**Operating systems** include software-based firewalls

**Data integrity testing** is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data presently held in a system (Relational integrity tests + Referential integrity tests)

**Routers** that pass data between networks contain firewall components

**Cold start**: procedure for initially keying crypto-equipment

**Cold Site:** does not have the computer equipment in place

**Completeness check**: ensure no fields are missing from the record

**Compensating control:** internal control that reduce the risk of a potential control weakness

**False rejection rate or false non-match rate (FRR or FNMR)**: he probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

**ITAF includes three categories of standards – general, performance and reporting**.

**Current ISACA IT audit and assurance standards** include the following **general standards**: S2 Independence //S3 Professional Ethics and Standards//S4 Competence//**S6 Performance of Audit work**

**A Session Border Controller (SBC)** protects a VoIP infrastructure against a DOS.

**Honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

**VOIP**: A DDoS attack would potentially disrupt the organization's ability to communicate among its offices and have the highest impact.

**Open Source**: Mitigation of the risk of being locked into a single provider

**To address a maintenance problem**, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a **secure shell (SSH-2)** tunnel for the duration of the problem.

**Secure Shell (SSH) is** a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network.

**Substantive test** includes gathering evidence to evaluate the integrity (i.e., the completeness, accuracy or validity) of individual transactions, data or other information.

Who verifies that system changes are authorized, tested, and implemented in a controlled manner prior to being introduced into the production environment according to company's change and release management policies? **Quality Assurance Personnel**
**Conducting a physical count of the tape inventory is a substantive test.**

CSA require employees to assess the control stature of their own function. CSAs help increase the understanding of business risk and internal controls. Because they are conducted more frequently than audits, **CSAs help identify risk in a more timely manner (detect Risk SOONER)**

MOST appropriate to ensure the confidentiality of transactions initiated **via the Internet is the public key encryption.**
In the event of a data center disaster, the MOST appropriate strategy to enable complete recovery of a critical database is **Real-time replication** to a remote site.

**Feasibility Study**: Once the initial approval has been given to move forward with a project, an analysis begins to clearly define the need and to identify alternatives for addressing the need. This analysis is known as the feasibility study.

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: recommend that problem resolution be escalated**

**Batch Controls:** total monetary amount, total items, total documents, hash totals.

**Two roles of audit**: assurance and consulting Management implements controls; audit provides assurance they are effective and strong enough.

**Authority** of the board of directors delegated to audit through the charter.

**Audit committee determines what will be audited** but senior management has ultimate say on what will be audited and can change priorities.

**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 **RTO** is an indicator of the disaster tolerance; the lower RTO, the lower the disaster tolerance.

Provisioning access to data on a need-to-know basis is the primary way to ensure **data confidentiality**.

**If management disagrees with audit findings, audit explains the risk of the missing controls**.

**Risk**: any event that may negatively affect the accomplishment of business objectives.

**The use of unauthorized or illegal software should be prohibited by an organization**. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk.

**Software piracy can result in exposure and severe fines.**

**The potential or likelihood** that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat. Elements of Risk: threats, vulnerabilities, impact, likelihood Controls can reduce the risk down to acceptable levels.

**Risk assessment**: identify risk, vulnerabilities and threats // evaluate controls // determine audit objectives // supports risk based audit decision.

**Preventive (strongest) –** prevents threat from exploiting vulnerability

**Detective –** detects that a control has failed

**Corrective –** corrects situation and mitigates risk

**Compensating controls –** if another control fails or not possible, can mitigate risk through

**Internal Accounting Controls –** safeguarding assets and reliability of financial records

**Operational Controls -** protecting day to day operations

**Administrative Controls –** adherence to mgmt policies

**One of the basic purposes of any IS audit is to identify control objective. and the related controls that address objective.**

**Financial Audit–** correctness of financial statements

**Operational Audit–** evaluate internal control structure of a given process or area – app controls, logical security systems would be examples

**Integrated Audit–** combines financial and operational and looks at overall objectives of organization.

**Administrative Audit**– looks at issues related to efficiency of operational productivity

**IS Audit–** looks at systems to make sure assets safeguarded properly

**Forensic Audit–** fraud investigations

Antispam filtering techniques prevent a valid, variable-length email message containing a heavily weighted spam = **Bayesian (statistical)**

**An audit methodology** is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, statement of audit objectives and a statement of work programs.

**Audit Risk** is defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit.

The overriding of computer processing jobs by computer operators could lead to unauthorized changes to data or programs. **This is a control concern; thus, it is always critical**.

The IS auditor should perform **additional testing to ensure that it is a finding**. An auditor can lose credibility if it is later discovered that the finding was not justified.

**Materiality**, this refers to an error that should be considered significant to any party concerned with the item in question.

**SSL** generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality.

**Validity check** would be the most useful for the verification of passwords

**Materiality considerations** combined with an understanding of audit risk are essential concepts for planning areas to be audited.
Best method for mitigating against network denial of service attacks? **Employ packet filtering to drop suspect packets**

**Threats** are negative events that cause a loss if they occur. **Vulnerabilities** are paths that allow a threat to occur.
An intervention as required to stop, modify, or fix failures as they occur **corrective action**.

**Substantive Testing**: substantiates the integrity of actual processing – provides evidence of the validity and integrity of the balances in financial statements and the transactions that support these balances. Can include a count of physical items etc.

If **results of compliance testing reveals** the presence of adequate internal controls the confidence coefficient can be lowered and the auditor can minimize the amount of substantive testing required.

**Sampling Statistical:** objective method of determining sample size and selection criteria. Uses the mathematical laws of probability to calculate sample size, select sample items and evaluate sample results.

**Sampling Nonstatistical** – subjective aka judgment sampling; Uses auditor judgment to determine method of sampling.

**Variable sampling** – **used for substantive testing**; Deals with population characteristics like monetary values and weights. Integrity of the data – is the data correct.

**Attribute sampling** – looking for a % of occurrence - used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a given population.

**Stop or go sampling** – prevents excessive sampling of an attribute that allows the test to stop at any time

**Discovery sampling** – used when the expected occurrence rate is low

**Variable Sampling**: Different types of quantitative sampling models – all the mathematical stuff.

**CAAT:** Used to gather information and collect evidence during an audit; can be used in **continuous audit situations**.

**Risk reduction lowers risk** to a level commensurate with the organization's risk appetite.

**Risk transfer** does not always address compliance risk.

Provide a mirror image of the hard drive = **evidence collection**
**Risk transfer** typically addresses financial risk. For instance, an insurance policy is commonly used to transfer financial risk,while compliance risk continues to exist.

An ongoing audit program is part of the **risk-mitigation strategy**

**Risk avoidance does not expose the organization to compliance risk** because the business practice that caused the inherent risk to exist is no longer being pursued.

**Mitigating risk** will still expose the organization to a certain amount of risk. Risk mitigation lowers risk to a level commensurate with the organization's risk appetite.

**Risk mitigation treats the risk,** while risk transfer does not necessarily address compliance risk**.**

**BCM** represents the overall management of the project meant to ensure the continuity or uninterrupted provision of operations and services. It is an ongoing process that includes the processes of disaster recovery, business recovery, business resumption and contingency planning.

**GAS Generalized audit software**: can read and directly access data from databases and do all sorts of tests on the data collected

**Continuous audits** – usually done in parallel with normal operations, captures internal control problems as they occur. Used in critical, **complex systems that can't be shut down.**

In the business environment, a **disaster** is any event that creates an inability on an organization's part to support critical business functions for some predetermined period of time.

A **business continuity plan** is an approved set of advance arrangements and procedures that enable an organization to ensure the safety of its personnel, minimize loss, facilitate recovery of business operations and repair or replace the damaged facilities as soon as possible.

**Business continuity management** is a comprehensive and ongoing process to ensure the continuation of critical business operations in the face of whatever challenges the organization may face. It provides a strategic and operational framework for reviewing the way an organization provides its products and services, while increasing its resilience to disruption, interruption or loss.

**CSA (control self assessment)** – auditor is facilitator, early detection of risk; line managers involved and helps educate and motivate people. Helps focus on areas of high risk.

**IT Governance concerned with two issues**: that IT delivers value to the business and that IT risks are mitigated. The second is driven by embedding accountability into the enterprise thus, also ensuring achievement of the first objective.

**Governance** helps ensure the alignment of IT and business objectives.

**IT governance** is a subset of corporate governance.

**Bayesian** is looking at how often special words are used, and in what order, to make a determination.

**Audit provides recommendations to senior management** to help improve the quality and effectiveness of the IT governance initiatives.

**BoD** and Executive Management are responsible for IT Governance.

**Steering committee more technical in nature – oversees the project**

**Strategic plan** is more 3-5 years and based on mission, vision and business objectives.

**A project steering committee** is ultimately **responsible for all deliverables**, project costs and schedules

**Senior management**: demonstrates commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those who are needed to complete the project

**User management**: **review and approve system deliverables** as they are defined and accomplished to ensure the successful completion and implementation of a **new business system application**

**Data Dictionary**: The data dictionary is a central repository of data elements and **their relationships**. The Data Dictionary includes definitions of views, data sources, relationships, tables, indexes, etc. When new tables, new views or new schema are added, the data dictionary is updated to reflect this.

**Referential Integrity**: No record can contain a reference to a primary key of a non-existing record or NULL value. Database must also not contain unmatched foreign key values.

The **4GL** provides screen-authoring and report-writing utilities that automate database access. The 4GL tools do not create the business logic necessary for data transformation.

**Key logging** can circumvent normal authentication but not two factor authentications

Creating individual's **accountability** is dependent on OS control function but not a database access control

**Two factor authentication** can be compromised by man-in-the-middle attack

**IS short term plans are more operational or tactical in nature** – specific, short term requirements that are not necessarily strategic in nature.

**Risk Mgmt process** - Board and executive mgmt choose risk management strategy and action which may be mitigating the risk,

transferring the risk or accepting the risk.

**DDE enables different applications to share data by providing IPC**. DDE is a communication mechanism that enables direct connection between two applications.

**IT Balanced Scorecard** is used to measure effectiveness of IT.

**Pre-requisite for balanced scorecard are key performance indicators (KPI)** which should be applicable in the organizational context and have to be known what is being measured.

**Balanced Scorecard** used by strategy committee and management to achieve IT and business alignment.

**Risk Management Process**: Identification and classification of information resources or assets that need protection; Assess the threats and vulnerabilities associated with the assets and likelihood of occurrence. It includes impact analysis. Evaluate existing controls or new controls designed to address vulnerabilities.

Increase overhead/cost = **long asymmetric encryption key**

**In HTTPS protocol**, the types of data encrypted include URL, HTTP header, cookies, and data submitted through forms.

**Preparedness tests** involve simulation of the entire environment (in phases) at relatively low cost and help the team to better understand and prepare for the actual test scenario.

**Quantitative risk analysis Objective**: This is based on numbers – Wants to assign numeric values to the elements of the risk assessment and the potential losses; requires a lot of time and resources to do. **Estimate potential loss // Conduct a threat analysis // Determine annual loss expectancy**

The major difference between a router and a Layer 3 switch is that a router performs packet switching using a microprocessor, whereas a Layer 3 switch performs the switching using application **ASIC hardware**

SLE: **Single loss expectancy Dollar amount** of potential loss to an organization if a specific threat took place.

EF: **Exposure factor Percentage** of asset loss if threat is successful. Asset value * Exposure factor (EF) = SLE

ARO: **Annual rate of occurrence** # of incidents or exposure that could be expected per year.

**Firewall** mechanisms that are in place to mediate between the public network (the Internet) and an organization's private Network.

**The IT steering committee typically serves** as a general review board for major IT projects and should not become involved in routine operations; therefore, one of its functions is to **approve and monitor major projects**, such as the status of IT plans and budgets.

**Observation** is the best and most effective method to test changes to ensure that the process is effectively designed.

The key objective of an **IT governance program** is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance.

**ALE – Annual loss expectancy**
Annual Loss Expectancy = Single Loss Expectancy SLE x Annual Rate of Occurrence ARO
Safeguard value (ALE before safeguard) – (ALE after safeguard) – (Annual cost of safeguard) = Safeguard value

**Qualitative Risk Analysis:** subjective – based on high, medium, low ratings.

**Obtain evidence:** Inspection; Observation; Inquiry and confirmation; Reperformance; Recalculation; Computation; Analytical procedures

**Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

In performing **detailed network assessments** and access control reviews, IS auditor should first determine the **points of entry**
**Inherent risk**: assumes an absence of compensating controls in the area being reviewed

An **information security manager** should be involved in the earliest phase of the application development life cycle to effectively influence the outcome of the development effort.

**Worms**: Reproduce on their own with no need for a host application.

**Due Diligence** = did careful risk assessment (RA); so org. has implemented risk management and established necessary controls

**Due Care** = Implemented recommended controls from RA Liability minimized if reasonable precautions taken

**Downtime can be assessed only during BIA**

**Defined maturity level** is the best overall indicator of the state of information security governance. The maturity level indicates how mature a process is on a scale from 0 (incomplete process) to 5 (optimizing process).

**Logic Bomb**: Will execute certain code when a specific event happens.

**Trojan Horse**: Program disguised as another program.

**Outsourcing**: goal is to achieve lasting, meaningful improvement in business processes and services. But, requires management to actively manage the relationship and outsourced services.

**Auditors are concerned with SLAs.**

**SLA should serve as an instrument of control.** SLAs set the baseline by which the outsourcers perform the IS function (these are based on business requirements).

When **contracting** with a service provider, it is a best practice to enter into an **SLA** with the provider.
If outsource software development, **source code escrow is critical** as, in case company goes out of business, who owns the intellectual property is a concern to the auditor. BCP is also a concern. Also concerned about cross border issues (data) and if core business processes are being outsourced.

**Risk Management:**
Risk Management is aligned with business strategy & direction
Risk mgmt must be a joint effort between all key business units & IS
Business-Driven (not Technology-Driven)

Reducing the number of defects encountered during software development projects = **Implement formal software inspections**

**Steering Committee:**
Sets risk management priorities
Define Risk management objectives to achieve business strategy

**References** = part of the RFP.

**Accountability** = can never be outsourced

**Risk arising out of outsourcing can be mitigated if outsource to more than one vendor.**

**Quality Management** is the means by which IS department based processes are controlled, measured and improved.

A quality management system is based on a set of documents, manuals and records.
Problem: **The test environment is not configured with the same access controls that are enabled in the production environment.**

**Gap analysis** needed to check company against the requirements in the standards and then company can fill the gaps; **part of ISO 9001 quality management best practices.**

Several control mechanisms can be used to enforce **SOD**.

**Residual risk**: After eliminating, mitigating, and transferring risk, residual risk remains; the risk that is assumed after implementing controls is known as residual risk.

Offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment **COLD SITE;** its ready to receive equipment but does not offer any components at the site in advance of the need.

**Warm site is an offsite** backup facility that is partially configured with network connections and selected peripheral equipment—such as disk and tape units, controllers and central processing units (CPUs)—to operate an information processing facility.

**Compensating controls** for lack of segregation of duties (mostly detective in nature):
Audit trails// Reconciliation// Exception reporting //Transaction logs //Supervisory reviews//Independent reviews

**Hybrid sourcing** A combination of using in-house workers and outsourcing selected processes.

**Education of users is more important to the successful implementation and maintenance of a security policy** than management support.

**Compliance responsibilities** are usually shared **across organizational (ALL) units** and the results shared with executive management and the board of director's audit or compliance committee

**Email retention is an important focus.**

**Lack of security controls is vulnerability**.
The following functions is performed by a (VPN); **Hiding information from sniffers on the net**
**Projects** are unique, temporary and are developed progressively.

**Business case** – shows benefits to be achieved for the business and must be kept for lifecycle of project

**Influence** – Project Manager has no formal authority.

**Pure project** – Project Manager has formal authority over those taking part in project.

**Matrix project** – Project Manager Share authority with functional managers.

**Duration of a project**: since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration.

Project objectives must be SMART: **Specific // Measurable // Achievable // Relevant // Time bound**

Discovers that there is **no documented security procedures** => next step would be to identify and evaluate the practices used by the organization.

Project roles and responsibilities – purpose is to show **accountability**

**Senior Mgmt** - approves the resources for the project

**User Mgmt** – assumes ownership of project and resulting system

**Project steering committee** – overall direction and ensures stakeholders represented.

**Project sponsor** – provides funding and works with Project Manager to define critical success factors and metrics.

**Data and application ownership** assigned to sponsor
**System dev mgmt** – provides tech support

**Project manager** – provides day to day mgmt of project.

**Three critical elements to projects:** Time-duration: how long will it take? // Cost-resources : how much will it cost // Deliverables-scope : what is to be done

The **data owner** specifies controls, is responsible for acceptable use

**The auditor may discover information that could cause some level of damage to the client if disclosed.** In addition, **the auditor shall implement controls to ensure security and data backup of their work.**

**Valid audit types** are financial, operational (SAS-70), integrated (SAS-94), compliance, administrative, forensic, and information systems.

**A forensic audit** is used to discover information about a possible crime.

**Critical Path** – Longest path through the network;

**No slack time** for any activity on critical path and any activities with no slack time are on the critical path.

Every project schedule must have **at least one critical path**. Every activity that resides in the critical path has **no (zero) slack time**. If an activity has slack time then that is not part of the critical path.

**GANTT charts**: aid in scheduling of activities/tasks. Charts show when activities start and end and dependencies. Used for checkpoints/milestones too.

**PERT** – network management technique Shows relationships between various tasks and shows estimates/scenarios for completing tasks – three estimates shown – optimistic, most likely and pessimistic. It doesn't talk about costs.

**Time box**: project management technique for defining and deploying software deliverables within a short and fixed period of time with pre-determined resources. **Must be a software baseline.**

Traditional SDLC aka **waterfall**

**Data Conversion**: risk is you will not convert all the data – some will be missed. You also need to make sure that you are comparing **control totals** before and after conversion to avoid this.

**Control totals can be used to compare batches too.**

If **purchasing a system,** need to make sure decision makers are involved at all steps. Need to consider many things as part of acquisition including turnaround time (time to fix an issue from when it is first logged) and response time (the time a system takes to respond to a query by a user).

**SMALL BIZ** = > Supervision of computer usage.

**Asset mgmt – assets stand by themselves**

**Configuration management – interrelationships between assets.**

**Quality assurance** is responsible for ensuring that programs and program changes and documentation adhere to established standards.

**Early engagement of key users will help ensure business requirements will be met in software development process.**

**The mean time between failures** that are first reported represents flaws in the software that are reported by users in the production environment. This information helps the IS auditor in evaluating the quality of the software that is developed and implemented.

**Regression testing** a regression test means to run a particular test once again to make sure that the modification of the software has not introduced any new errors.

**All the data used in the original test need to be used in the regression test.**

**Project steering committee** approves the RFPs for software acquisitions. It is responsible for all costs and timetables.

**Bottom up** – begin testing each module and work your way up until whole system tested. Finds critical errors earlier because can start before system done – sort of white box testing.

**Top down** – start at interfaces of entire system and work your way down to each function/component – like black box testing – functional.

**Total Quality Management** purpose is end user satisfaction

A **standard** is implemented to ensure a minimum level of uniform compliance. **Guidelines** are advisory information used in the absence of a standard. **Compliance to standards is mandatory**; **compliance to guidelines is discretionary.**

**The policy should be signed** and enforced by the highest level of management.

**Unit testing** – testing of individual programs or modules – usually white box testing.

**System testing** – making sure that all modules function together properly.

**Integration testing** – evaluates connection of components that pass info to each other.
**Final acceptance testing** – done during implementation phase by QA and then UAT.

**White box** – assess effectiveness of software program logic.

**Black box** – testing of interfaces and general function – doesn't care about internal structure.

**Function/validation** – is similar to system testing, but often used to test the functionality of the system against requirements.

**Regression testing** – rerunning a portion of a test scenario to make sure that changes have not introduced new errors in other parts of app

**UDD I** – universal description, discovery and integration – acts as an electronic directory accessible via corporate intranet or internet and allows interested parties to learn of the existence of web services.

After an IS auditor has identified threats **and potential impacts, the auditor should then identify and evaluate the existing controls.**

The primary purpose of **audit trails** is to establish accountability and responsibility for processed transactions.

**Reengineering** – process of updating an existing system by extracting and reusing design and program components.

**Reverse engineering** – process of taking apart an app to see how it functions; can be done by **decompiling code**.

**Configuration management** – version control software and check out process. Used for software dev and for other stuff – programs, documentation, data. Change control works off of config mgmt.

**Logical path monitor** – reports on the sequence of steps executed by a programmer.

**QA = UT + FT + IT + RT + UAT**

**UNIT -> INTEGRATION -> SYSTEM -> AT**

**Program maintenance** is facilitated by more cohesive (the performance of a single, dedicated function by a program) and more loosely coupled (independence of the comparable units) programs.

**Structured walk** through is a management tool – it involves peer reviews to detect software errors during a program development activity.

**Salami technique**: It truncates the last few digits from a transaction. For instance, changing the value 125.39 into 125.30 or into 125.00 is an example of salami technique.

**Functional or validation testing:** it tests the detailed functionality of the system to ensure that if system is right for the customers. It is comparable to system testing.

**Parallel testing:** this test is done by feeding the same test data to the original system and the newly designed system to compare the results.

Wi-Fi Protected Access **(WPA2)** implements most security for WiFi.

First concern of an auditor is does the application meet **business requirements**; close second is there **adequate controls in place.**

CSE: **Automated tools to aid in the software development process**. Their use may include the application of software tools for requirements analysis, software design, code generation, testing, documentation generation. Can enforce uniform approach to software dev, reduces manual effort.

**digital signature mechanism ensures the integrity** of the message content by creating a one-way hash **at both the source and destination and then comparing the two.**

CASE: **Don't guarantee that software will meet user requirements or be correct.**

**Integrating BCP** into the development process ensures complete coverage of the requirements through each phase of the project

An excessive number of users with privileged access is not necessarily an issue if **compensating controls are in place.**

**Quantitative Risk**: Overall business risk takes into consideration the likelihood and magnitude of the impact when a threat exploits vulnerability, and provides the best measure of the risk to an asset.

(**Sharing Password**) users need to be aware of company policy and the risk that may arise from sharing passwords. Awareness training would help to address this issue.

**Business Process Re-engineering BPR**: this is the process of responding to competitive and economic pressures and customer demands to survive in a business environment. Important for the auditor to understand the flow charts showing the before and after processes to make sure appropriate controls in place.

**Selenium**: This is an open source tool used for automating web applications. Selenium can be used for browser based regression testing. It's tool used for both functional and regression testing. This is an open source tool used for automating web applications. Selenium can be used for browser based regression testing.

**Benchmarking:** improving business process – BPR technique (PROAAI) – SWOR, Comparing, Merge, Investment, Process design, BPR.

**Regression Testing is required when there is a**
Change in requirements and code is modified according to the requirement
New feature is added to the software
Defect fixing
Performance issue fix

**Run-to-run totals** A process that tracks the total number of submissions to ensure that all transactions have been processed.

**Sequence Check**: Sequence number use causes out-of-sequence and duplicate numbers to be rejected.

**Limit or Range Check**: Valid numbers are below or between a maximum values. E.g., checks should not exceed $

**Validity Check or Table Lookup**: Only certain values are accepted: Sex=M/F.

**Reasonableness Check**: Values entered are reasonable: A takeout order of 100 pizzas???

**Existence Check**: Required fields are entered correctly.

**Key Verification**: Input is double checked via second person OR all digits are entered twice.

**Check Digit**: A digit may verify the correct entry of other digits.

**Completeness Check**: Complete input is provided: zeros or spaces are checked for each required letter or digit

**Duplicate Check**: Duplicate transactions or transactions with duplicate IDs are checked for and rejected.

**Data owners** are primarily responsible for authorizing access to production data on a need-to-know basis

**Termination checklist** requiring that keys and company property be returned and all access permissions revoked upon termination.

**A redundancy check** detects transmission errors by appending calculated bits onto the end of each segment of data;

**Parity check just tells you if the data you send was an even or odd number of bits.** A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data.

**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.

**Application Controls**: to ensure the completeness and accuracy of the records and the validity of the entries made.

**The use of a digital signature** verifies the identity of the sender

**The recovery point objective (RPO)** is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption. **The media creation date will reflect the point to which data are to be restored or the RPO. The recovery time objective (RTO)** is the amount of time allowed for the recovery of a business function or resource after a disaster occurs.

**The service delivery objective (SDO)** illustrates the expected level of service during recovery. The organization may have several SDO targets based on the different phases of recovery. RTO is the recovery time objective, and RPO is the recovery point objective. ITO is a distractor.

**The service delivery objective (SDO**) is directly related to the business needs, and is the level of service to be reached during the alternate process mode until the normal situation is restored.

**Compliance** test is deals with test of details;

**Substantive** deals with test of controls;

**MTO** is the maximum time that an organization can support processing in alternate mode.

**Total Monetary amount** – total monetary amount of items processed = total monetary value of batch docs

**Total items** – total number of items on each doc in the batch = total number of items processed

**Data Validation** identifies data errors, incomplete or missing data or inconsistencies among related items and edit controls are preventive controls used before data is processed. Input data should be evaluated as close to the time and point of origination as possible

**Structured walkthrough** = a tabletop exercise.

**Batch total** checks provide a reasonably good test for completeness and accuracy of input.

**Sequence check** – is everything in sequence

**Limit check** – data should not exceed a certain predetermined limit

**Range check** – data should be within the range of predetermined values

**Validity check** – record should be rejected if anything but a valid entry is made – like marital status should not be entered into employee number field.

**Reasonableness check** – input data matched to predetermined reasonable limits or occurrence rates – normally receive 20 orders, if receive 25 then that's a problem

**Table lookups** – input data compared to predetermined criteria maintained in a lookup table.

**Hot sites can be made ready for operation normally within hours**

**Substantive** confirms integrity of a process. This test will determine whether tape library records are stated in a correct manner

**The purpose of the batch controls** is to ensure that the batch is not changed during processing.

**Existence check** – data entered correctly and meet predetermined criteria – valid transaction code must be entered in the transaction code field.

**Postevent reviews** to find the gaps and shortcomings in the actual incident response processes will help to improve the process over time.

To proactively **detect emerging risk in large volume of transaction** you need to use "**continuous auditing**" technique, which feeds real-time data to management so as a quick corrective action can be taken soon after the detection of any anomalies.

The first step before creating a risk ranking is to **define the audit universe**, which takes into account of organizational structure, authorization matrix and IT strategic plan

**Database normalization minimizes duplication of data** through standardization of the database table layout. Increased speed is obtained by reducing the size of individual tables to allow a faster search.

**Attribute sampling**, **used in compliance testing**, can effectively determine whether a purchase order has been authorized according to authorization matrix.

A change management process developed = **Design phase**

**Resource pooling**: Resources are pooled across multiple customers

**Rapid elasticity**: Capability can scale to cope with demand peaks

**SaaS**: applications are designed for end-users, delivered over the web

**PaaS**: is the set of tools and services designed to make coding and deploying those applications quick and efficient

**IaaS**: is the hardware and software that powers it all – servers, storage, networks, operating systems

**White box testing is performed much earlier in the software development life cycle than alpha or beta testing**.

**White box testing is used to assess the effectiveness of software program logic.**

The review of the test cases will facilitate the objective of a successful migration and ensure that proper testing is conducted. **An IS auditor can advise as to the completeness of the test cases.**

**Key verification** – keying in process repeated by two different people

**Check digit** – a numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect value submitted.

**Database normalization minimizes duplication** of data through standardization of the database table layout. Increased speed is obtained by reducing the size of individual tables to allow a faster search.

Detects transposition and transcription errors, Verifies data accuracy/integrity; **(checksum)**

The **inference engine** uses rules, also known as heuristics, to sort through the knowledge base in search of possible answers. The meaning of information in the knowledge base can be recorded in objects and symbols known as semantic networks.

**Completeness check** – a field should always contain data and not zeros or nulls

**Duplicate check** – new transactions matched to those previously input to make sure they were not entered previously.

**Domain integrity test** – verify that the edit and validation routines are working satisfactorily, all data items are in the correct domain.

**The scope of an IS audit is defined by its objectives**. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

**Run-to-run totals** – can verify the data through the stages of application processing.

**Programmed controls** – software can be used to detect and initiate corrective action for errors in data and processing.

**Parity checking** – checks for completeness of data transmissions/transmission errors.

**Redundancy check** - appends calculated bits onto the end of each segment of data to detect transmission

**CA** is a trusted third party that attests to the authenticity of a user's public key by digitally signing it with the CA's private key.

**Systems Control Audit Review File and Embedded Audit Modules (SCARF/EAM):** Embedding specific written audit software in organization's host application system; regular processing cannot be interrupted; complex High

**Integrated Test Facility (ITF):** Dummy entries are set up and include auditor's production file; it's not beneficial to use test data; Complex High

**Snapshots**: Pictures of the processes' path; An audit trail is required; Complex Medium

**Audit Hooks:** Embedding hooks in applications; Only select transactions or processes need to be examined; complex Low

When **developing a large and complex IT infrastructure**, the best practice is to use a **phased approach** to fit the entire system together. This will provide greater assurance of quality results.

**Continuous & Intermittent Simulation (CIS):** Simulates the instructions executed of the application; Transactions meeting certain criteria need to be examined; Complex Medium

**Preparedness test** = using actual resources to simulate a system crash.

**Relational integrity tests** – performed at the data element and record level – enforced through data validation routines or by defining input condition constraints and data characteristics or both. Is the data ok?

**Referential integrity tests**- these define existence relationships between entities in a database that need to be maintained by the DBMS. These relationships maintained through referential constraints (primary and foreign key). It is necessary that references be kept consistent in the event of insertions, deletions, updates to these relationships.

**Atomicity** – transaction either completed in its entirety or not at all

**Consistency** – all integrity conditions (consistent state) with each transaction – so database moves from one consistent state to another.

**Isolation** – each transaction isolated from other transactions so each transaction only accesses data that are part of a consistent database state

**Implementing risk management**, as one of the outcomes of effective information security governance, would require a **collective understanding of the organization's threat, vulnerability and risk profile as a first step.**

**Durability** – if a transaction has been reported back to the user as complete, the resulting changes will persist even if the database falls over.

**Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period** before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance.

**Encrypting and decrypting** data using an asymmetric encryption algorithm by using the receiver's private key to decrypt data encrypted by the receiver's public key.

**Snapshot – take snapshots of data as flows through the app. Very useful as an audit trail.**

Mapping – **identifies unused code and helps identify potential exposures**

Tracing/Tagging – **shows exact picture of sequence of events** – shows trail of instructions executed during application processing. Tagging involves placing a flag on selected transactions at input and using tracing to track them.

**BIA** will give the impact of the loss of each application. A BIA is conducted with representatives of the business that can accurately describe the criticality of a system and its importance to the business.

A **project steering committee that provides an overall direction for the enterprise resource planning** (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results.

**Test data/deck** – simulates transactions through real programs.

**Base case system evaluation** – uses test data sets developed as part of comprehensive testing programs; used to verify correct system operation before acceptance.

**Parallel operation** – put prod data through existing and new system and compare Integrated test facility – creates test file in prod system and those test transactions get processed along with the live data.

The **IT steering committee** provides open communication of business objectives for IT to support. The steering committee builds awareness and facilitates user cooperation. Focus is placed on fulfillment of the business objectives.

**CMM** is commonly used by entities to measure their existing state and then determine the desired one
Use of statistical sample for tape library inventory" is an example of **Substantive** type of sampling technique.

**Cost-benefit analysis** is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation.

**Extended records** – gathers all data that haven't been affected by a particular program.

**GAS** –includes mathematical computations, stratifications, statistical analysis, sequence and duplicate checking and recompilations; transactions that exceed predetermined thresholds.

**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

The **sender's private key is required to generate a digital signature**. The recipient uses the sender's public key to validate the digital signature.

Protect confidentiality = **Encryption**

**Project sponsor** is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project.

**Audit hooks** – embed hooks in app systems to function as red flags and to induce IS auditors to act before an error or irregularity gets out of hand. **Useful when only select transactions need to be examined**.

**ITF:** Continuous and intermittent simulation – as each transaction is entered, simulator decides whether transaction meets certain criteria and if so audits it.

**Data dictionary**: A database that contains the name, type, range of values, source and authorization for access for each data element in a database.

**Vulnerabilities** are a key element in the conduct of a risk analysis.

**Audit planning** consists of short- and long-term processes that may detect threats to the information assets.

**Controls** mitigate risks associated with specific threats.

**Liabilities are part of business and are not inherently a risk.**

An IS **audit charter** establishes **the role of the information systems audit function**. The charter should describe the overall authority, scope and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee.

**BCP** refers to the businesses ability to continue its fundamental functions in the event something deters (Org. issue), DR would be more for the planning for how to address the situations where accesses to crucial systems are unavailable. When systems are down and how to restore those systems (IT Department issue)

**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. So outline the overall authority, scope and responsibilities of the audit function.

Detects transmission errors by appending calculated bits onto the end of each segment of data; **Redundancy check**

**Range check**: Range checks ensure that data fall within a predetermined range.

**Application controls**: The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved..

**Communications software/handler**: process for transmitting and receiving electronic documents between trading partners.

**Risk mitigation** is the strategy that provides for the definition and implementation of controls to address the risk described. By requiring the system's administrator to sign off on the completion of the backups, this is an administrative control that can be validated for compliance.

The **resumption of critical processes** has the highest priority because it enables business processes to begin immediately after the interruption and not later than the maximum tolerable period of disruption (MTPD) or maximum tolerable downtime (MTD).

**BoD** = determining business goals

**Computer-aided software engineering (CASE)**: The use of software packages that aid in the development of all phases of an information system.

**Receipt of inbound transactions**: Controls should ensure that all inbound EDI transactions are accurately and completely received, translated and passed into an application, as well as processed only once.

**Outbound transactions**: Controls should ensure that only properly authorized outbound transactions are processed. This includes objectives that outbound EDI messages are initiated upon authorization, that they contain only pre-approved transaction types and that they are only sent to valid trading partners.

**Data dictionary**: A database that contains the name, type, range of values, source and authorization for access for each data element in a database.

**Digital signatures good way of getting rid of spam in email system**

**Payment systems**: Two parties involved in these – issuers (operates payment service) and the users (send and receive payments).

**Overall business risk for a particular threat can be expressed as**: A product of the probability and the magnitude of the impact if a threat successfully exploits vulnerability.

**The recovery time objective (RTO)** is the deadline for when the user must be processing again. IT is expected to have completed the necessary level of technical recovery. The user is able to resume processing work unless that RTO has failed
For a business having many offices within a region, a **reciprocal arrangement** among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach and would provide an acceptable level of confidence.

The effectiveness of the BCP can best be evaluated by **reviewing the results from previous business continuity tests** for thoroughness and accuracy in accomplishing their stated objectives

EMM – **electronic money model** – emulates physical cash – payer does not have to be online at the time of purchase, payer can have unconditional intractability.

**Content-filtering proxy** server will effectively monitor user access to Internet sites and block access to unauthorized web sites.

**Electronic Funds Transfer: EFT** is the exchange of money via telecommunications without currency actually changing hands. It is the electronic transfer of funds between a buyer, a seller and his/her respective financial institution.

**EFT refers to any Electronic financial transaction** that transfers a sum of money from one account to another electronically. In the settlement between parties, EFT transactions usually function via an internal bank transfer from one party's account to another via a clearinghouse network. Usually, transactions originate from a computer at one institution and are transmitted to another computer at another institution with the monetary amount recorded in the respective organization's accounts. **Very high risk systems**.

**Completely connected (mesh) configuration**: A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks).

**Integrated customer file** – where all the info about a given customer combined together into one file.

**ATM** = POS = point of sale devices.

Management should review administrator level activity to ensure that personnel with administrator access are not performing unauthorized functions; **SOD in small Organization**

**ISO9126**: Software Quality ISO Standards = Functionality, Reliability, Usability, Re-Usability, Efficiency, Maintainability, Portability

**ISO9126**: focuses on the end result of good software processes

**RFID uses radio frequency to identify objects that is tagged**. A tag consists of a chip and an antenna. The chip stores the ID of the object, and the antenna receives signal.

**RFP**: A document distributed to software vendors requesting them to submit a proposal to develop or provide a software product.

**Compliance testing**: Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.

**Data warehouse** – once data in warehouse, should not be modified

**Memory dump**: The act of copying raw data from one place to another with little or no formatting for readability.

**Supply Chain Management** = SCM = is about linking the business processes between the related entities (buyer and seller).

**Important for just in time inventory** – store does not keep inventory – stuff comes as you need it – should have multiple suppliers in case one fails or you could be in trouble.

**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.

**DID** = Simply because more than one security layer are implemented we are not satisfied by one of them we do use two or often more than two to achieve the most secure solution we can

**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.

**Application is critical,** the patch should not be applied without regard for the application; business requirements must be considered

**A government regulation** is a mandatory control that forces compliance.

**Acceptance testing** determines whether the solution meets the requirements of the business and is performed after system staff have completed the initial system test. This testing includes both quality assurance testing (QAT) and user acceptance testing (UAT), although not combined.

**Nonworking processes,** whether manual or automated, are usually the highest priority if their business value can be justified. The compliance test uses **precision** to describe the rate of occurrence out of the sample population.

**Strategy defines the primary business we are in for the next three to five years**. Using this information, the business can develop or adopt supporting standards and then create low-level procedures to accomplish the strategic objective.

The primary **risks during the BPR design** phase are improper scope, lack of necessary skills, political resistance, and a failure by management to support the project.

**Strategy defines the primary business we are in for the next three to five years.** Using this information, the business can develop or adopt supporting standards and then create low-level procedures to accomplish the strategic objective.

**PERT analysis shows the critical path to illustrate the minimum specific tasks necessary to complete the project's** objective. The CPM technique is a valuable tool for demonstrating what must be accomplished versus what was requested. High-dependency tasks get performed, while low-dependency tasks may be cancelled from the project.

**System testing** relates a series of tests by the test team or system maintenance staff to ensure that the modified program interacts correctly with other components. System testing references the **functional requirements** of the system.

**Integration testing** evaluates the connection of two or more components that pass information from one area to another. The objective is to utilize unit-tested modules, thus building an integrated structure **according to the design.**

**Unit testing** references the detailed design of the system and uses a set of cases that focus on the control structure of the procedural design to ensure that the internal operation of the program performs according to specification.

**Change management**: Changes must be requested, approved, documented and controlled. Changes to system parameters and libraries must be controlled.

**Monitoring:** Effective monitoring is a process that assesses the quality of the system's performance over time. It includes the regular management and supervisory activities as well as separate evaluations by central units, Internal Audit, or other independent parties.

**Audit charter** outline the responsibility, authority and accountability of auditor prior to commencing the audit assignment ant this must be agreed upon

The **engagement letter** is used with independent auditors to define the relationship. This letter serves as a record to document the understanding and agreement between the audit committee and the independent auditor. It provides the independent auditor the responsibility, accountability, and authority to conduct the audit.

**Help desk:** No. of issues successfully resolved on first call is indicator of success.

**Patch management** – first thing is to verify the validity of the patch first – that it came from the right place.

**Program Library Management software** – program library management facilitate effective and efficient management of data center software inventory. Includes, application and system software program code, job control statements

**Library control software** is used to separate test libraries from production libraries in mainframe and client server environment.

The **Capability Maturity Model** creates a baseline reference to chart current progress or regression. It provides a guideline for developing the maturity of systems and management procedures.

**Grid computing**: apps can be designed to use processing power of many computers.

**Audit charter's purpose** is to grant the right to audit and delegate responsibility, authority, and accountability

**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 timely basis by the system of internal controls. **This cannot be minimized using statistical sampling**

**Capacity management:** the planning and monitoring of computing resources to ensure that available resources are used efficiently and effectively.

**Detection Risk** = material error

**Substantive tests and Compliance tests**, using variable and attribute sampling methods

**Compliance testing** uses discovery sampling to detect fraud.

Sampling, control, detection, inherent = **interest to an IS auditor**

**Traditional independent audits** are conducted with formality and adherence to standards necessary for regulatory licensing and external reporting.

**Protocol analyzer**: network diagnostic tool that monitors and records network information.

**Access control software**: designed to prevent unauthorized access to data and objects, unauthorized use of system functions or programs, unauthorized modification of data or unauthorized attempts to access computer resources.

**Commitment and rollback controls are directly relevant to integrity.**

**Previous test results will provide evidence of the effectiveness of the business continuity plan**.

**BCP:** comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness.

**Sequential** – good for batch processing.

**Indexed sequential** – records are logically ordered according to a data related key and can be accessed based on that key; Very fast.
Direct random access – records are addressed individually based on a key not related to the data. **Based on hashing.**

**Metadata** – data about the data.

**Reliability** - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

**Functionality** - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.

**Usability** - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

**Efficiency** - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.

**Maintainability** - A set of attributes that bear on the effort needed to make specified modifications.

**Portability** - A set of attributes that bear on the ability of software to be transferred from one environment to another

**Data Dictionary/Directory System** – data dictionary contains an index and description of all items stored in the database. The DS describes the location of the data and the access method; it helps maintain integrity of the data and controls unauthorized access.

**Database structure** – can be hierarchical (tree), network – not really used, or relational

**Key feature of relational databases** – normalization – minimizes duplication of data (but can cause performance degradation, but if don't do it then you can have data integrity issues).

**Database controls:** Authorized access only // Concurrent access handling // Data accuracy and completeness // **Database checkpoints – to minimize data loss** // Database backup

The **IT BSC is a tool** that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. **(Effectiveness of an organization's planning and management of investments in IT assets)**

**Encryption is frequently used for authentication.**

By evaluating the organization's development projects **against the CMM**, an IS auditor determines whether the development organization follows a stable, **predictable software process**.

Successful attacks start by **gathering information** about the target system.

The IS department should specifically consider the manner in which **resources are allocated in the short term**.

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 disk based on a hash key.

In **a cost-benefit analysis**, the total expected purchase and operational/support costs and a qualitative value for all actions are weighted against the total expected benefits in order to choose the best technical, most profitable, least expensive, or acceptable risk option.

**CMMI** useful: evaluate management of computer center, development function management process, implement and measure change management.

The **ALE** is the expected monetary loss that is estimated for an asset over a one-year period.

**Potential business impact** is only one part of the cost-benefit analysis.

**Digital Right Management (DRM):** allow access to digital contents to the users. DRM helps to assign controls to the computer program to the usage of digital contents

**What is DDL (data definition language)?** This is a standard language to define data schema and object. Example of DDL statements or commands: CREATE, ALTER etc

**Program interface tests (integration test)**

Performing a **walk through** of the process/procedure allows the IS auditor to gain evidence of compliance and observe deviations, if any.

**WAN:** Message switching / Packet switching / Circuit switching / Virtual circuits / Dial up service

**A VPN is a technology** that uses encryption to make a secure virtual connection over public networks to extend the corporate network. It is a cost effective way to extend LANs across different parts of the world.

**Logging in using the named user account before using the DBA account provides accountability** by noting the person making the changes.

The ability to recognize a potential security incident is: **required of all personnel.**

**Security Policy**: No shared accounts. This is typically a security policy in many organizations. Each account only has the minimal permissions it needs to perform the task.

A relational database uses **normalization rules. The purpose of normalization rules is to get rid of the unnecessary data and to reduce the amount of** data required to fulfill the requirements of users' queries. Each data instance will have unique value for each attribute.

**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.

**Utility programs – these leave no audit trail.**

**Packet Switching - pay by amount, not by distance.**

An IS auditor reviewing a database discovers that the current configuration does not match the originally designed structure**: IS auditor should first determine whether the modifications were properly approved**.

**Layers of IT environment**: Network - Operating system – Database - application

**IPS (intrusion prevention system):** it can block unauthorized access attempts to a system. IPS works with routers, firewalls, proxy server and other access control devices. Once an IPS detects an illegal activity or access attempt, it sends notification to the

device to block that access attempt. The only problem with IPS is that it can block legitimate traffic presuming it to be an illegal activity.

**Logical access exposures** – list out all the various computer attacks like salami, smurf, logic bombs etc.

**CGI**: It is a program that **runs on the server**, and the web server can call it to perform a set of tasks such as verifying users input in web forms. CGI scripts (normally written in C or Perl) must be written carefully because they run on the server. A simple error in the script can give unauthorized person access to the server.

**Value delivery** means that good rates of return and a high utilization of resources are achieved

**SSL or secure socket layer** only provides data confidentially. It does not ensure integrity of the message.

The advantage of **steganography** is that the intended secret message does not attract attention to itself as an object of scrutiny; it's a practice of concealing a file, message, image, or video within another file, message, image, or video; so the existence of messages is hidden when using steganography.

**Confidentiality** — information classification

**Availability** – fault tolerance, backups

**Threat:** Hazard, potential loss

**Risk:** likelihood of potential loss

**Weakness:** risk not reduced to a low level by internal controls

**Exposure:** Size of potential loss associated with a control problem

**Expected loss** = exposure X risk

**Objective of Controls:** Minimize losses to organization resulting from threats

**Firewall implementation methods** Screened-host firewall //Dual-homed firewall//DMZ or screened subnet firewall.

**Screened host firewall**: this is the simplest method among all. It uses a packet filter router and a bastion host. No direct traffic from internal to the external network is allowed.

**Equal Error rate (ERR) - % showing when false reject and acceptance are equal. The lower the better.**
**Biometrics in order of effectiveness:**
1. Palm
2. Hand geometry
3. Iris
4. Retina – lowest FAR
5. Fingerprint
6. Face
7. Signature
8. Voice recognition

**PERT chart** will help determine project duration once all the activities and the work involved with those activities are known.

**Four objectives for controls**
- authorization (all transactions are authorized)
- recording (all transactions are recorded)
- access (allow access to assets only for authorized purposes)
- asset accountability (ensure that accounting records describe only real assets)
- In addition, accounting and data processing must be operationally efficient.

**The purpose of the change management process is to ensure that**:
- Standardized methods and procedures are used for efficient and prompt handling of all changes
- All changes to service assets and configuration items are recorded in the configuration management system
- Business risk is managed and minimized
- Addressing risk scenarios at various information system life cycle stages
- All authorized changes support business needs and goals
- All emergency changes should still undergo the formal change management process after the fact

**Function point analysis** is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc

The **long-term financial viability of a vendor** is essential for deriving maximum value for the organization—it is more likely that a financially sound vendor would be in business for a long period of time and thereby more likely to be capable of providing long-term support for the purchased product.

**Discovery sampling** = fraud has taken place or not.

**SOD:** Ensure that no single individual is given too much responsibility; no employee should be in a position to both perpetrate and conceal irregularities

**ISO/IEC 15504** is the reference model for the maturity models (consisting of capability levels which in turn consist of the process attributes and further consist of generic practices) against which the assessors can place the evidence that they collect during their assessment, so that the assessors can give an overall determination of the organization's capabilities for delivering products

An enterprise's risk appetite is BEST established by: **the steering committee.**

**Control self-assessments (CSAs)** require employees to assess the control stature of their own function. CSAs help increase the understanding of business risk and internal controls. Because they are conducted more frequently than audits, CSAs help identify risk in a timelier manner

**Hot site** — a fully configured computer facility with electrical power, heating, ventilation, and air conditioning (HVAC) and functioning file/print servers and workstations

**Warm site** — computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC), limited file/print servers and workstations

**Cold site** — computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC) – no computer hardware

**"ROM"** indicates a non-volatile memory

**Electronic Vaulting** – transfer of backup data to an offsite location — Done batch over telecom lines to alternate location

**BIA** has three goals: criticality prioritization, maximum tolerable downtime estimation, resource requirements

Effectively reduces the risk of piggybacking = **Deadman doors**

The use of statistical sampling procedures helps minimize = **Detection risk**

The security strategy will be most useful if there is a **direct traceable connection** with business objectives. Inferred connections to business objectives are not as good as traceable connections

The purpose of a **deadman door controlling** access to a computer facility is primarily intended to prevent piggybacking

**Steering committee** is to bring the awareness of business issues and objectives to IT management. An effective steering committee will focus on the service level necessary to support the business strategy.

**Release management** is the process to manage risk scenarios of production system deployment and is a component of change management. Also the BEST way to ensure that the tested code that is moved into production is the same use Release management software.

**Incident management** addresses impacts when or after they occur.

**Configuration management** is the specific process to manage risk scenarios associated with systems configuration and is a component of change management.

**Classification** allows the appropriate protection level to be assigned to the asset.

**Audit logging – tools for audit trail (log) analysis**
- Audit reduction tools – remove stuff that is not an issue from the logs before the auditor looks at it
- Trend/variance detection – looks for anomalies in user or system behavior
- Attack signature-detection – look for attack signatures.

**Naming conventions** for system resources are an important pre-requisite for efficient administration of security controls (aka logical access controls)

**Some of the benefits of blade servers include:** Reduced energy costs; Reduced power and cooling expenses; Space savings; Reduced cabling; Redundancy; Increased storage capacity; Reduced data center footprint; Minimum administration; Low total cost of ownership

**Virtual private network (VPN) concentrator:** A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services. It is a type of router device, built specifically for creating and managing VPN communication infrastructures. **A VPN concentrator is typically used for creating site-to-site VPN architectures.**

**Prevention** (prevent threats from occuring)

**Detection** (detect problems if they occur)

**Correction** (change the system so problems do not reoccur)

The ideal **length of passwords should be at least eight characters long**. A passphrase is generally considered as a more secure form of password

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them (**provide a basis for drawing reasonable conclusions**).

**Client server security** has to do with identifying all the access points.

**Firewalls control traffic** between two or more networks.

**Sociability testing:** it confirms that if a new system can perform in the target platforms and environment without causing any problem to existing system.

While developing a risk-based audit program, which of the following would the IS auditor MOST likely focus on? **Business processes**

**Sequence check** - numerical or alphabetical order

**Field check** - Proper type of data (numeric vs alphabetic), category, or length

**Sign check** - appropriate arithmetic sign

**Validity check** - already authorized account number

**Limit or range check** - does not exceed limit

**Logical reasonableness** -- debit vs credit accounts

**Redundant data cross-check** -- enter account number & name, look up account number and cross-check name for match (valid-combinations test)

**Parallel testing** is the process of feeding data into two systems—the modified system and an alternate system—and computing the results in parallel. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions.

**Integration testing** is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure. In this case, the tests are not necessarily between systems that interact with one another so sociability testing is a better answer.

**Reviewing data and time stamp** is the most effective control to make sure that both the source and object codes are synchronized.

An **accreditation** is senior management's decision which authorize IS operation and accept the risks (risks in IT assets, operation, individuals). It is considered as a form of quality control, which challenges IS managers and staff to implement highly effective security controls in the organization's IT systems.

**Firewall rules** are derived from company policies and standards; One of first steps in setting up a firewallis to see what apps need to be externally accessed. The security administrator should perform periodic reviews to validate firewall rules.

**Router/packet filtering** – simplest – operates at layer three, examines the header for IP info. Has filtering rules and vulnerable to attacks from misconfigured filters.

**Application firewalls** – application and circuit level – act kind of like proxies, but operate at higher **L7**. Hide internal network from outside, separate proxy needed for each app (circuit level does not require this). Can be slow, but allow most granular control.

**Stateful inspection** – keeps track of communications in a state table. More efficient than app ones and better than packet filtering. can be complex to administer. **Layer 4**

**IDS =** • Sensors • Analyzers • Admin Console • User interface

The following actions should take place immediately after a security breach is reported to an information security manager => **Confirm the incident**

Network performance metric is **throughput**. It is the number of bytes transmitted by a communication channel in a second.

**Worms** are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

**Private key cryptography** (secret key) – symmetric encryption. Key exchange is the big problem. – DES, AES, 3DES; Fast and efficient.

Techniques useful for **verification**: static analysis, reviews, inspections, walkthroughs

**Public key cryptography** – created to solve key distribution issues – RSA, ECC (elliptical curve cryptography).

While undertaking an audit, if the auditor suspects that an attack or any suspicious activity is going on, at first he should inform **the management about the incident**.

When developing audit plan an auditor need to identify the highest-risk system and plan the audit accordingly. The auditor **should never rely on the report of the previous year's audit plan** since it may not have been designed on risk-based audit approach.

The main advantage of **continuous auditing** is that it improves security of time-sharing system that process large number of transactions.

**IT Governance** =value delivery+ risk management

**Audit Risk**: It is the risk that Information may contain material error that may go undetected during the course of audit.

**Control Risk** example: Manual reviews of computer logs can be high because activities requiring investigation are often easily missed due to the volume of logged information.

**The objectives of BSC are to establish a vehicle for management to report to the board**, to foster consensus among key stakeholders about strategic aims of IT, to demonstrate the effectiveness and benefits of IT, and to communicate the performance of IT, the risks and capabilities of IT.

**Data mining** uses rules to drill down through the data in the data warehouse for correlations. The results of data mining are stored in the data mart. The **DSS presentation program** may display data from the data mart in a graphical format.

**Risk analysis methods:** Qualitative analysis; Semi-qualitative analysis( descriptive ranking( e.g. low, medium, high)+ numeric scale) ; Quantitative analysis(numeric value only)

**Quantitative risk is preferred over qualitative approach. It gives assumption that is more objective**

**ALE**= value (v) x probability (p)

Board of director and senior management are responsible for **IT security governance**, which can be delegated to CEO

**Board of directors is primarily responsible for IT governance**

When we fail to apply **SOD** properly, we need to use compensating controls (an internal control) in order to reduce the existing control weakness.

**IT governance implementation** = Determine stakeholder requirements and involvement.

**Integrity of a new staff can be best assured by background checking**

**Database administrators** are the **custodian** for organization's data. They are also responsible for defining and maintaining database structure

The advantage of using **bottom-up** approach to develop organizational policy is that the policy will be derived from the outcome of risk assessment process

**Matrix project management:** In this project organization forms, both the project manager and the department heads **share the authority over the project**.

**Function Point Analysis:** It measures software size indirectly. Function point analysis is used to estimate the complexity of large application programs used in businesses, it considers the following parameters: Number of user input - Number of outputs - Number of user inquiries - Number of files - Number of external interfaces.

**Scalability** is the ability to move application software source code and data into systems and environments that have a variety of performance characteristics and capabilities without significant modification. It entails determining the, impact of increased scale on client performance. A system that scales well should degrade gracefully as saturation is reached.

Only the activities that are **not in the critical path have the slack time**. Each activity outside the critical path has the earliest and the latest completion time, considering the latest completion time does not affect the overall project completion time. The difference between latest and the earliest completion time called **slack time**

This **Gantt chart** helps to schedule a project, from starting to the end, along a time line. It also shows what percentage of resources is allocated to each task. With **Gantt chart**, a project progress can be tracked including milestones and major achievements.

**Bottom up:** it starts from small units such a programs or module and go upward until the entire system has been tested. It helps to **identify errors before all the modules** or program of a system get completed.

**Top down:** it is the opposite approach of bottom-up testing. It helps to **test critical functions early** and to detect interface errors sooner. It also raises developers' confidence since it shows that the system is working.

**The bottom-up** approach is used to test large application systems.

**Negotiation and signing a contract is the last step in software acquisition process.**

**BIA** helps to determine maximum downtime possible for a particular application and that amount of data that could be lost without causing major impact

**Digital signature:** Create a hash of the entire message, encrypts that hash with sender's private key. Provides integrity, authentication, non-repudiation, **but not confidentiality**

**Digital envelope** - Sender encrypts the message with a symmetric key (session key). The session key is encrypted with the receiver's public key and sent. **Provides confidentiality**.

**Digital Certificate** A digital credential which is composed of public key and identifying information about the owner of the public key. These certificates are signed by a trusted 3rd party like verisign using verisign's private key.

**Referential integrity** means a valid link exists between data in different tables.

Objects contain **both methods and data** to perform a desired task. The object can delegate to another object.

**Certificate Authority**: authority in a network that issues and manages security credentials and public keys for message signature verification or encryption

**RA** – takes some of the administrative functions from CA

**Certification practice statement (CPS)** – details set of rules governing CA operations.

Major system migrations **should include a phase of parallel operation or a phased cut-over to reduce implementation risk.** Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly.

It essential to have copies of all **BCPs** stored onsite and offsite for ease of access and readability.

**Anti-malware** – scanner - Active monitor - Integrity CRC checkers - Behavior Blockers - Immunizer

**SSL and TLS** – SSL provides point to point authentication and communications privacy over the internet using cryptography. Server authenticated, but client usually not.

**SHTTP** – similar to SSL, but not session oriented – does it based on message

**IPSEC** – VPN – tunneling (more secure – with AH and ESP) whole packet encrypted and transport (header not encrypted)

**Increasing the length of an asymmetric key** can increase processing time more than the use of a symmetric algorithm.

**Digital certificates are better than digital signatures because digital certificates are issued by trusted third parties.**

**Humidity** – too much get corrosion/condensation, too little and get static electricity.

**ISO15504**: level0 incomplete process, level1 performed process, level2 managed process, level3 establish process, level4 predictable process, level5 optimal process.

**Business continuity** recovery of the business processes so business can operate and can survive as a company.

"**due diligence**" can be rephrased as "do check" and "**due care**" can be rephrased as "do act".

A company will perform **due diligence** when they **are evaluating a new product or new vendor**. Does the new product or vendor meet the business requirements, security requirements? A company will perform **due care** when they **are securing systems** or applications to adequately protect customer or company data.

**Security** is also the best in the three-tier architecture because the middle tier protects the database tier.
There is one major drawback to the **N-tier architecture** and that is that the additional tiers increase the complexity and cost of the installation.

**BCP** is the most critical corrective control. The plan is a corrective control.

**A recovery strategy** is a combination of preventive, detective and corrective measures.

**Business continuity** has to be aligned to change management process – for updating the plan.

**BCP** focuses on availability and is primarily the responsibility of senior management.

**BIA** – business impact analysis is a critical step in this process. – need to understand the organization, business processes in order to be able to do this properly. Outputs are RPO and RTO.

**Different BIA approaches** Questionnaire // Interview key users // Work group – bring people together to discuss

**The process to review and approve the contract** is one of the most important steps in the software acquisition process. An IS auditor **should verify that legal counsel reviewed and approved the contract** before management signs the contract

**BIA** = defining the recovery strategies.

Could be used to provide automated assurance that proper data files are being used during processing **Internal labeling, including file header records**

The common practice, when it is difficult to calculate the financial losses, is to take a **qualitative risk approach**

**Auditor can review past transaction volume to determine impact to the business if the system was unavailable.**

**Two cost factors** associated with this: Down time cost // Recovery

**Risk based auditing** approach does not consider detection risk, inherent risk and control risk as a major concern.

**Replay attacks**: An attack in which the attacker records data and later replays it in an attempt to deceive the recipient.

**Parity check** just tells you if the data you send was an even or odd number of bits. It was great in the days of old modems. While you are used to seeing CRC, it is just a particular type of Redundancy check. The CRC or **Cyclic Redundancy Check** is based on a different algorithm and is used to ensure that data hasn't been altered in the process of transmission or writing to storage.

**Smurf:** A malicious attack where the hacker sends a large number of spoofed ping packets to broadcast addresses, with the intent that these packets will be magnified and sent to the spoofed addresses. This has exponential possibilities, depending on how many hosts respond.

The chair of the **steering committee** should be a senior person (executive level manager) with the authority to make decisions relating to the business requirements, resources, priority and deliverables of the system.

**Decision trees** use questionnaires to lead a user through a series of choices until a conclusion is reached.

**Encryption:** The process of taking an unencrypted message (plaintext); applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (cipher text)

**Encryption key**: A piece of information; in a digitized form; used by an encryption algorithm to convert the plaintext to the cipher text

**Postimplementation** review collects evidence to determine whether the organizational objectives have been fulfilled. The review would include verification that internal controls are present and in use.

**Waterfall** model has been best suited to stable conditions and well-defined requirements; Finish-To-Start

**Fraggle:** the same as Smurf attack but uses UDP

**Teardrop**: sending smaller size packet or fragmented packets

**DoS:** Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. usually flooding a system to prevent it from servicing normal and legitimate requests.

**DDoS:** same as DoS but uses several systems to flood. Password sniffing: Attack in which someone examines data traffic that includes secret passwords in order to recover the passwords, presumably to use them later in masquerades.

**IP spoofing**: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address. Routers and other firewall implementations can be programmed to identify this discrepancy.

**Dumpster diving**: going through trash to find information

**Wiretapping**: attaching a special device to the line so that the person can secretly listen to a conversation.

**Scanning attack**: hacking technique checking ports to reveal what services are available in order to plan an exploit those services, and to determine the OS of a particular computer.

**Parallel operation** = provide assurance that a new system meets its functional requirements.

The purpose of **regression testing** is to ensure that **a change does not create a new problem** with other functions in the program. After a change is made, all of the validation tests are run from beginning to end to discover any conflicts or failures. Regression testing is part of the quality control process.

**Synchronous** – distances shorter, but no data loss (two systems are synchronized). Asynchronous – can be data loss, but distance is greater, systems not synchronized and data transferred at set times or when possible..

**Recovery Time objective** (MTD – maximum tolerable downtime); Acceptable downtime for a given app. The lower the RTO, the lower the disaster tolerance; can't meet RTO unless you have met RPO.

**Recovery Strategies**: First approach in a recovery strategy is to see if built in resilience can be implemented. A disaster recovery procedure will address everything not covered by resilience.

**Preparedness tests** involve simulation of the entire environment (in phases) and help the team to better understand and prepare for the actual test scenario. (**Efficient way to determine the effectiveness of the plan**)

**Hot sites** – can be ready in minutes or hours

**Warm sites** – don't have computers, but have basic network and some peripheral equipment

**Cold sites** – have very basic stuff – facility, environmental controls

**Mobile sites** – for branches

**Reciprocal arrangements – not good because software changes** between companies and might cause incompatibility issues

**Incident response team** – respond to incidents and do reporting and investigation

**Emergency action team** – first responders

**Damage assessment** – assesses the extent of the damage

**Emergency management team**: responsible for coordination of activities in disaster.

**Alternative routing** – using an alternative cable medium like copper instead of fiber.

**Diverse routing** – method of routing traffic through split cable or duplicates cable facilities.

**Paper test** – paper walk through of the plan with major players.

**Preparedness test** – usually a localized version of a full test – simulated system crash

**Full operational test** – shutting down a data center etc.

**Backup – son is daily backup, father end of week, grandfather end of month.**

**Disaster starts when the disaster starts. IT does not declare disaster.**

**Not testing your BCP plan is one of the worst things you can do.**

**Fidelity coverage** against fraud =bonding
Which of the following should an incident response team address FIRST after a major incident in an information processing facility;

**Containment at the facility** Which of the following should the IS auditor review to ensure that servers are optimally configured to support processing requirements? **Server utilization data**

**Business case** should demonstrate feasibility for any potential project. By including a feasibility study in the business case along with a cost-benefit analysis, management can make an informed decision.

Generation of an activity log is not a control by itself. **It is the review of such a log that makes the activity a control**

Accurately capture data from the organization's systems without **causing excessive performance problems.**

**People and then data are the most important things.**

**Logical access controls**: securing software+ data within an IPF. (LAC = collection of policies + procedures)

**Call back features**: hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches.

**Call forwarding**: bypassing callback control.

**Dumpster diving**: looking through an organization's trash for valuable information.

**Data diddling**: changing data before they are entered into the computer.

**Poor biometric implementations** are vulnerable to spoofing and mimicry attacks.

**Accountability** = implement a log management process

**Data, voice and video** throughput requirements for all users will define the business needs on which one can base the design of the appropriate LAN technology

**Steganography**: digital right management (DRM)

**Remote booting** is a method of preventing viruses, and can be implemented through hardware.

**Nonrepudiation**, achieved through the use of digital signatures, prevents the senders from later denying that they generated and sent the message.

**Encryption** may protect the data transmitted over the Internet, but may not prove that the transactions were made.

**Authentication** is necessary to establish the identification of all parties to a communication.

**Integrity** ensures that transactions are accurate but does not provide the identification of the customer.

**Hashing is irreversible**.

**Encryption is reversible.**

**Hashing creates** an output that is smaller than the original message and encryption creates an output of the same length as the original message.

**Mandatory vacations** help uncover potential fraud or inconsistencies. Ensuring that people who have access to sensitive internal controls or processes take a mandatory vacation annually is often a regulatory requirement and, a good way to uncover fraud.

**Asymmetric algorithm** requires more processing time than symmetric algorithms

**Immunizers** defend against viruses by appending sections of themselves to files.

**Behavior blockers** focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record.

**Cyclical redundancy checkers (CRC)** compute a binary number on a known virus-free that is then stored in a database file.

**CA** is a trusted third party that ensures the authenticity of the owner of the certificate.

**Out-of-band connectivity**: OOB is something that is not in the same channel of communication. Common example is the OTP that you receive on your mobile, for authorization of any payment that you make online.

**IDEA (International Data Encryption Algorithm)** is a symmetric encryption used in PGP software. This 64-bit block cipher uses a 128-bit key. Although it has been patented by a Swiss company, it is freely available for noncommercial use. It is considered a secure encryption standard, and there have been no known attacks against it. DES, SHA, and Tiger typically are not used in PGP.

**Kerberos Authentication system** the function of a key distribution center by generating tickets to define the facilities on networked machines which are accessible to each user (Network Authentication Protocol based on ticketing)

All the decisions regarding purchasing existing software or building a custom application should be made by using data from the **feasibility** study and business specifications

**Replay attack**: residual biometric characteristics, such as fingerprints left on a biometric capture device may be reused to gain access.

The **IS steering committee** is a decision-making body composed of top-level functional managers and IS specialists that provides planning and control for the organization's IS function.

**SAN** is a special-purpose network in which different types of data storage are associated with servers and users. A SAN can either interconnect attached storage on servers into a storage array or connect the servers and users to a storage device that contains disk arrays.

**Brute force**: feeding the biometric capture device numerous different biometric samples.

**Cryptographic attack**: Targets the algorithm or the encrypted data

**Mimic Attack**: reproduce characteristics similar to those of the enrolled user such as forging a signature or imitating a voice.

**Professional ethics:** Encourage compliance with standards, Be objective, Serve in the interest of stakeholders in a lawful and honest manner, Maintain privacy and confidentiality

**Elements of Risk:** threats, vulnerabilities, impact, likelihood

**Controls** can reduce the risk down to acceptable levels.

**Risk transfer typically addresses financial risk**. For instance, an insurance policy is commonly used to transfer financial risk, while compliance risk continues to exist.

**Metadata** – data elements required to define a database – data about the data.

**Data Dictionary/Directory System** – data dictionary contains an index and description of all items stored in the database. The DS describes the location of the data and the access method; it help maintain integrity of the data and controls unauthorized access.

**Database structure** – can be hierarchical (tree), network – not really used, or relational

**Audit logging** – tools for audit trail (log) analysis

**Disaster recovery** has to do with IT and is a subset of business continuity.

**Business continuity**: Readiness, Respond, Recovery, Resume, Repair, Return

**BCP (business continuity policy)** is the most critical corrective control. The plan is a corrective control.

**Recovery strategy** is a combination of preventive, detective and corrective measures.

**Business continuity** has to be aligned to change management process – for updating the plan.

**Risk assessment** is the first step to find the processes most important to the business

**BCP** focuses on availability and is primarily the responsibility of senior management.

**BIA** – business impact analysis is a critical step in this process. – need to understand the organization, business processes in order to be able to do this properly. Outputs are RPO and RTO.

**Different BIA approaches**: Questionnaire, Interview key users, Work group – bring people together to discuss

**Auditor can review past transaction volume** to determine impact to the business if the system was unavailable.

**Two cost factors associated with this:** Down time cost – how much does it cost you if the app is down? Recovery cost – cost of the strategies to minimize your downtime.

**The primary concern is to establish a workable DRP**, which reflects current processing volumes to protect the organization from any disruptive incident.

**Business unit management** assumes ownership of the project and the resulting system. It is responsible for acceptance testing and confirming that the required functions are available in the software.

**Reciprocal arrangements** – not good because software changes between companies and might cause incompatibility issues

**Redundancy** – use of dynamic routing protocols, extra capacity etc.

**Alternative routing** – using an alternative cable medium like copper instead of fiber.

**Diverse routing** – method of routing traffic through split cable or duplicate cable facilities.

**Long haul network diversity** – use t1 circuits

**Disaster starts when the disaster starts. IT does not declare disaster.**

**Not testing your BCP plan is one of the worst things you can do.**

**Fidelity coverage**: coverage against fraud aka bonding

**People and then data** are the most important things.

**Test data** runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unauthorized changes or unexercised portions of a program.

**Code review** is the process of reading program source code listings to determine whether the code follows coding standards or contains potential errors or inefficient statements. A code review can be used as a means of code comparison, but it is inefficient and unlikely to detect any changes in the code, especially in a large program.

**An automated code comparison** is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure.

**Integrity:** Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?

**System administration review:** This includes security review of the operating systems, database management systems, all system administration procedures and compliance.

**Network security review:** Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.

**Validation** is the process of checking that the SW does what the customer wants
**Verification** is the process of checking that the SW matches the requirements

**Business continuity review:** This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.

**Data integrity review:** The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software GAZ (e.g., computer assisted audit techniques CAAT).

**IS auditor** should consider the resource requirement of audit project and match audit resources to the defined tasks.

An **audit charter** should exist to clearly state management's responsibility, objectives for, and delegation of authority to, IS audit. This document should outline the overall authority, scope and responsibilities of the audit function. The highest level of management should approve this charter and once established, **this charter should be changed only if the change can be and is thoroughly justified.**

**Audit charter:** The responsibility, authority, and accountability of the information systems audit function are to be appropriately documented in an audit charter or engagement letter.

**Independence:** The IS auditor must be able to exercise its assignment on its own initiative in all departments, establishments and functions of the organization. It must be free to report its findings and appraisals and to disclose them. The principle of independence entails that the IS audit department operates under the direct control of either the organization's chief executive officer or the board of directors or its audit committee (if one exists), depending on the corporate governance framework. Independence also requires that the IS auditors should not have a conflict of interest with the area under audit.

**Professional ethics and standards:** The information systems auditor is to adhere to the Code of Professional Ethics of the Information Systems Audit and Control Association. Due professional care and observance of applicable professional auditing standards are to be exercised in all aspects of the information systems auditor's work.

**Performance of audit work:** Information systems audit staff are to be appropriately supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the information systems auditor is to obtain sufficient, reliable, relevant, and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

The **audit report** is to state the scope, objectives, period of coverage, and the nature and extent of the audit work performed. The report is to identify the organization, the intended recipients and any restrictions on circulation. The report is to state the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

**Follow-up activities:** The information systems auditor is to request and evaluate appropriate information on previous relevant findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

**GUIDELINES:** provide guidance in applying IS Auditing standards.

**PROCEDURES:** provide examples of procedures an IS auditor might follow in an audit engagement.

**Time stamps** are an effective control for detecting duplicate transactions such as payments made or received.

Audit planning also includes **risk analysis** to identify risks and vulnerabilities that help devise controls to control them. IS auditor has to identify different types of risks associated with information system. The IS auditor is often focused towards a particular class of risks associated with information and the underlying information systems and processes.

**Business risks** are those risks that may influence the assets or processes of a specific business or organization. The nature of these risks may be financial, regulatory, or operational and may arise because of the interaction of the business with its environment, or because of the strategies, systems, processes, procedures, and information used by the business.

The purpose to install **internal control system** is to provide reasonable assurance that organizational objectives will be achieved and undesired risk events are prevented, detected, and corrected on timely basis. Internal control is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within an organization.

**The IT BSC is designed to measure IT performance**. To measure performance, a sufficient number of "performance drivers" or KPIs must be defined and measured over time. Failure to have objective KPIs may result in arbitrary, subjective measures that may be **misleading**.

**Preventive:** Preventive controls are designed to detect problems before they arise. For example, to prevent from accident in plant, it is ensured that only qualified technicians are appointed. Another example could be the use of proper login mechanism before any person is allowed to access the sensitive business data.

**Detective:** After an error or problem has been occurred, the most important area is to detect the cause. It is generally said that once the causal factor is identified, major part of problem solving process is complete. Variance analysis is considered the one of the most effective detective control to identify and report weaknesses in the overall process.

**Corrective:** Once detective control has identified the cause of the problem, corrective control comes into play. It intends to adapt processes so as to minimize the future occurrence of the event.

**Accounting controls:** Accounting controls are principally concerned with safeguarding assets and providing assurance that the financial statements and the underlying accounting records are reliable. Stated broadly, **the accounting function must be kept separate from the custody of assets.**

**Operational controls:** Operational controls are concerned with day to day operations of an organization to ensure that operations run smoothly. For example, plan maintenance review is scheduled every week so as to avoid breakdown.

**Administrative controls:** Administrative controls are measures that apply principally to operating efficiency and compliance with established policies. These controls have no direct bearing on the reliability of financial statements and other accounting records. Consequently, administrative controls are not of direct interest to accountants and auditors.

**AUDIT METHODOLOGY:** It is a set of documented audit procedures designed to achieve planned audit objectives.
The first step of the review of the software quality management process should **be to determine the evaluation criteria in the form of standards adopted by the organization**

**Financial audit**: The purpose of a financial audit is to assess the correctness of an organization's financial statements. A financial audit will often involve detailed, substantive testing. This kind of audit relates to information integrity and reliability.

**Operational audit:**
An operational audit is designed to evaluate the internal control structure in a given area. IS audits of application controls or of logical security systems, are examples of operational audits.

**Integrated audit** combines both financial and operational audit steps. It assesses the overall objectives of an organization, related to financial information and assets safeguarding and efficiency.

**Administrative audit**
It is oriented to assess issues related with the efficiency of operational productivity within an organization.

**Information systems audit** The process of collecting and evaluating evidence to determine whether an information system safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently.

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs**, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.**

**Forensic audits:** Audits specialized in discovering fraud and crimes.

**RISK BASED AUDIT APPROACH:** This approach is used to assess risk and to assist with an IS auditor to either compliance testing or substantive testing. This approach determines the nature and extent of testing. The IS auditor doesn't just rely on risk; they also rely on internal controls and business knowledge.

**ADVANTAGES of risk assessment:**
- Helps allocate audit resources.
- Helps collect relevant information.
- Provides basis for managing audit departments.

**Transaction Validation:**
- Sequence Check: Sequence number use causes out-of-sequence and duplicate numbers to be rejected.
- Limit or Range Check: Valid numbers are below or between a maximum value. E.g., checks should not exceed $3,000
- Validity Check or Table Lookup: Only certain values are accepted: Sex=M/F.
- Reasonableness Check: Values entered are reasonable: A takeout order of 100 pizzas???
- Existence Check: Required fields are entered correctly.
- Key Verification: Input is double checked via second person OR all digits are entered twice.
- Check Digit: A digit may verify the correct entry of other digits.
- Completeness Check: Complete input is provided: zeros or spaces are checked for each required letter or digit
- Duplicate Check: Duplicate transactions or transactions with duplicate IDs are checked for and rejected.
- Consistency or Logical Relationship Check: Data is consistent with other known data: An employee's birth date must

**Compliance tests** show that internal control system is functioning properly.

**Example of Compliance & Substantive Testing:**
Auditor first reviews the company policy for controls and on the basis of result he decide either he will use compliance testing or substantive testing to verify the controls according to the management specified policy. This detailed review in which auditor use actual data is called substantive testing e.g. the IS auditor may use CAAT tolls to extract data from the actual database and check the validity of the record.

In a risk-based audit approach, the IS auditor identifies risk to the organization based on the nature of the business. In order to plan an annual audit cycle, the types of risk must be ranked. To rank the types of risk, the auditor must first define the **audit universe** by considering the IT strategic plan, organizational structure and authorization matrix

Risk associated with electronic data interchange **(EDI)** is improper/insufficient transaction authorization.

**Data Conversion:** Organizations use different types of software to store their data. This data should be converted from the stored software to the auditing software. This is done using special software programs known as package and utility programs. This ensures that there is no inconsistency when auditing data stored in different software.

**Evidence** is any information used by the IS auditor to determine whether the entity or data being audited follows the established audit criteria or objectives.

A **log management tool** is a product designed to aggregate events from many log files (with distinct formats and from different sources), store them and typically correlate them offline to produce many reports and to answer time-based queries.

An **ETL** is part of a business intelligence system, dedicated to extracting operational or production data, transforming that data and loading them to a central repository (data warehouse or data mart); an ETL does not correlate data or produce reports, and normally it does not have extractors to read log file formats.

**Techniques used by IS auditor to collect audit evidence:**
- Reviewing information system organization structures. Reviewing IS policies and procedures.
- Reviewing IS standards. Reviewing IS documentations. Interviewing appropriate personnel.
- Observing processes and employees performance.

**Statistical sampling –** objective method**:** In this method, IS auditor quantitatively determines the sample size.

**Non-statistical sampling –** subjective method**:** Non-statistical sampling is a sampling technique where auditor uses his judgment instead of statistical techniques for sampling.

**Attribute sampling** is generally applied in compliance testing situations and deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence.

**Frequency estimating sampling –** used to estimate the rate of occurrence of certain attribute, answers "how many". (also called fixed sized attribute sampling)

**Stop-or-go sampling -** When relatively few errors are expected to found in population, this sampling model helps prevent excessive sampling.

**Discovery sampling –** when expected occurrence of an item is extremely low, this sampling is used; for example, to detect fraud.

**Critical path diagrams** shortest possible time required for completing the project.

**PERT** diagrams are a critical path method (CPM) technique in which three estimates (as opposed to one) of time lines required to complete activities are used to determine the critical path.

**FPA** is a technique used to determine the size of a development task, based on the number of function points.

**Gantt charts** help to identify activities that have been completed early or late through comparison to a baseline. Progress of the entire project can be read from the Gantt chart to determine whether the project is behind, ahead of or on schedule

**Job rotation = Detective**

Auditors should understand artificial intelligence and expert systems, and know that these systems are used to solve complex problems. An **expert system** is a computer program that contains the knowledge base and set of rules needed to extrapolate new facts from existing knowledge and inputted data; an expert system, sometimes known as artificial intelligence, is a computer program that simulates the knowledge and judgment of humans.

In CSA **management and work teams are directly involved in judging and monitoring effectiveness of existing controls**. The objectives of CSA programs include the enhancement of audit responsibilities, not replacement of audit responsibilities.

**MOST reliable sender authentication method is DC**; Digital certificates are issued by a trusted third party. The message sender attaches the certificate and the recipient can verify authenticity with the certificate repository.

During a **CSA workshop**, instead of the IS auditor performing detailed audit procedures; they should lead and guide the clients in assessing their environment.

**Control:** The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

**IT Control Objective:** A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

**IT Governance:** A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes

**Audit Mission:**

- AUDIT Charter defining overall Authority, Scope and Responsibility of the AUDIT function approved by Top Management
- Risk Assessment
- Familiarity with Business Regulatory Environment

**Risk** The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat.

**CA** manages and issues certificates, whereas a **RA** is responsible for identifying and authenticating subscribers, but does not sign or issue certificates

Improve internal control procedures = **performing a post incident review**

**Risk Elements** = Threat + Impact + Frequency

**Automatic numerical sequencing** is the only option that accounts for completeness of transactions because any missing transactions would be identified by a gap.

**Business Risk:** Are those threats that may impact the assets, processes or objectives of a specific business organization; The natures of these threats may be : Financial – Regulatory - Operational - Or may arise as a result of the interaction of the business with its environment - Or may arise in result of the strategies, systems and particular technology, process, procedure and information system used by the business

**An Information System Audit:**

"Any Audit that encompasses review and evaluation of automated information processing, related non-automated processes and the interfaces between them."

**Audit Risk:** Risk that the information/financial report may contain material error that may go undetected during the course of Audit

The **certificate authority** manages the certificate life cycle, including certificate directory maintenance and CRL maintenance and publication

**Risk Assessment Techniques :** These techniques may be computerized; non-computerized, Scoring and Judgment

**Compliance Testing :** A compliance test determines if controls are being applied in a manner that complies with management policies and procedures.

**Substantive Testing:** A Substantive test substances the integrity of actual processing.

**Reliability of Evidences:**

- Independence of the provider
- Qualification of the provider
- Objectivity of the evidence
- Timing of the evidence

**Computer Assisted Audit techniques:** Generalized Audit Software, Utility Software, test data, application software tracing and mapping and expert systems. These tools can be used for

- Test of details of transactions and balances
- Analytical review procedures
- Compliance test of IS general controls
- Compliance Test of Application controls
- Penetration and OS vulnerabilities

**CAATs Advantages:**

- Reduced Level of Audit Risk
- Greater independence from the auditee
- Broader and more consistent audit coverage
- Faster availability of information
- Improved exception identification
- Greater flexibility of run times
- Greater opportunity to quantify internal control weakness
- Enhanced sampling
- Cost saving over time

**Hot Site:** Fully configured, ready to operate within hours

**Warm Site:** Ready to operate within days: no or low power main computer. Does contain disks, network, peripherals.

**Cold Site:** Ready to operate within weeks. Contains electrical wiring, air conditioning, flooring

**Duplicate or Redundant Info. Processing Facility**: Standby hot site within the organization

**Mobile Site:** Fully- or partially-configured trailer comes to your site, with microwave or satellite communications.

**Inherent risk** The risk that a material error could occur, assuming that there are no related internal controls to prevent or detect the error. Inherent risk is the susceptibility of an area or process to an error that could be material. An example is when an authorized program has exits (trap doors) because they provide flexibility for inserting code to modify or add functionality. Control risk The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls. **Detection risk** results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when, in fact, they do.

Authentication is typically categorized as something you know (password), something you have (token) and something you are (biometrics). **And yes I know RSA has been breached**, but there are other token vendors out there.

Web servers should have up-to-date patches because they are accessible to the Internet and are prone to attack; (**Patching is a MUST for WEB) While logging is important, lack of system patching is a more significant issue.**

Speaking of biometrics, there's palm, hand geometry, Iris, retina, fingerprint, face and voice recognition. Which one costs the most and has the highest user rejection rate? **HINT it has something to do with the eye**.

You should know some of the **disadvantages of virtualization**: Magnified physical failures; degraded performance; Complex root cause analysis; Not Supported by All Applications.

You should know some of the **advantages of virtualization:** Save energy, Reduce the data center footprint, Faster server provisioning, Increase uptime, Improve disaster recovery, Extend the life of older applications, Isolate applications, Help move things to the cloud.

**Integrated auditing** is a methodology that combines the operational audit function, the financial audit function, and the IS audit function

**The security threats and risk mitigation techniques for wireless networking**: **Change default settings** – APs purchased by home users or SMBs typically have default administrator passwords and SSIDs that are easily available on the Internet. Be sure to set these values to something that only you know. Like passwords, SSIDs shouldn't be labeled with anything that can be easily guessed by an attacker. Examples include the name of the business, spouse names, pet names, children's names, etc. **Turn off SSID broadcasting** -- Configure client workstations to connect without users having to refer to a list of available wireless networks.

**Post-incident review** examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls.

**You need to know the different types of firewall types**: Screened host firewalls, Screened subnet firewalls, Packet filer firewalls, Stateful inspection firewalls, Hybrid firewalls, Proxy server firewalls, Application level (gateway) firewalls

**Unified Threat Management (UTM)** solutions consolidate stateful inspection firewalls, antivirus, and IPS to a single appliance. They are also generally understood to include many other network security capabilities.

**Next-generation firewalls (NGFWs)** were created to respond to increasing capabilities of malware and applications. They bring together the key network security functions, including advanced firewall, IPS/IDS, URL filtering and threat protection. Our NGFW solution ensures better security than legacy firewalls, UTMs, or point threat detection products, as these functions are engineered into the product from the start and share important information across disciplines.

**Sample size** depends on the confidence interval and confidence level. The lower the confidence interval required, the higher sample size is needed.

**Continuous and measurable improvement of quality** is the primary requirement to achieve the business objective for the quality management system

**Behavioral** = signature + Voice + Keystroke

**Phishing** is a social engineering attack.

**SYN flood** attack is denial of service.

**Brute force** attacks are used to gain unauthorized access

**Lower confidence coefficient, resulting in a smaller sample size.**

**JOB TRANSFERS** a tendency to add access, but not to remove old access.

**Risk analysis** is used to determine whether the audit has any chance of representing the truth. Nothing in the realm of IS auditing is absolute because of the abstract nature of technology implementations.

**Review access logs** and make sure someone else is reviewing and acting upon unsuccessful login attempts

As auditors you should be able to do Pen Testing, just make sure you've got approval before you start this part of the audit. **HINT: PRIOR APPROVAL**

Make sure all network changes are going through **change control**, even emergency changes.

**Forensics** comes into play, so make sure you know the four major considerations in the chain of events regarding evidence (Identify, Preserve, Analyze, and Present)

**Seek competent legal advice**. It is not the auditor's job to detect potentially illegal acts; however, the auditor should seek the aid of a lawyer concerning liability and reporting requirements.

**Undue restrictions** on scope would be a major concern as would the lack of time or the inability to obtain sufficient reliable evidence.

**Fire extinguisher** stored inside a cabinet mounted to a wall

**Surge protectors** are used for power spikes.

**Risk treatment:** The decision to manage an identified risk. The available choices are mitigate risk, avoid risk, transfer the risk, or accept the risk

**High-impact events:** These events, which may be significant enough to threaten the very viability of the organization, require risk treatment that belongs in the categories of business continuity planning and disaster recovery planning.

**Physical Access Exposures and Controls: Key focus for this area is mantraps, dead-man doors, and visitor escorts.**

**Mobile Computing: Hard drive encryption; Back-ups on a regular basis; Theft response team; Special care needs to be taken to defend against malicious code.**

**It should not be possible to delete a row from a customer 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.

In order for risk management to be effective, **it is necessary to align IT risk with business objectives**. This can be done by adopting acceptable terminology that is understood by all, and the best way to achieve this is to present IT risk in business terms.

**Evidence obtained directly from the source by an IS auditor is more reliable** than information provided by a system administrator or a business owner because the IS auditor does not have a vested interest in the outcome of the audit.

**Mirroring of critical elements** is a tool that facilitates immediate recovery.

RAID 1 = **disk mirroring** = ensure availability of data

**Preparedness test** is a localized version of a full test, wherein resources are expended in **the simulation of a system crash**. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness.

**Walkthrough** is a test involving a **simulated disaster situation** that test the preparedness and understanding of management and staff rather than the actual resources.

**Paper Test (structured walk through) > Preparedness Test > Full Operational Test**

**Potential business impact i**s only one part of the cost-benefit analysis.

**Integrity of transaction process** is ensured by database commits and rollbacks.

**Recovery managers** should be rotated to ensure the experience of the recovery plan is spread among the managers.
Disaster recovery planning (DRP) is the technological aspect of business continuity planning (BCP). Business resumption planning addresses the operational part of BCP.

**Annualized rate of occurrence (ARO):** This is an estimate of the number of times that a threat will occur per year. It will vary by threat.

**Diverse Routing**: Routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing
.
**Alternate routing:** method of routing information via an alternative medium such as copper cable or fiber optics.

**Mitigation:** Schedule file and system backup

**Deterrence:** Installation of firewalls for information systems.

Review plan and compare it with standards: **adequacy of the BCP**

Database renormalizing: **increased redundancy**.

**Normalization** is optimization process for a relational database that minimizes redundancy.

**Referential integrity**: it ensures that a foreign key in one table will equal null or the value of a primary in the other table.

**Referential integrity** is provided by foreign key.

**Post-incident review** improves internal control procedures.

**Capacity management** is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively.

**Normalization:** is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and risk of not maintaining consistency of data, with the consequent loss of data integrity.

**Traditional software sizing** has been done by counting source lines of code (SLOC). This method does not work as well in modern development programs because additional factors will affect the overall cost.

**Reasonableness check**: matches input to predetermine reasonable limits or occurrence rates. Functional acknowledgements are standard electronic data interchange (EDI) transactions that tell trading partners that their electronic documents are received.

**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.

**Policy:** A statement that specifies what must be done (or not to be done) in an organization. They should not state how something must be done (or not done). It usually defines who is responsible for monitoring and enforcing it.

**Redundancy check:** detects transmission errors by appending calculated bits onto the end of each segment of data.

**Reasonableness check**: compare data to predefined reasonability limits or occurrence rates established for the data.

**Parity check**: hardware control that detects data errors when data are read from one computer to another.

**Prototype system**: provide significant time and cost savings. Also have several disadvantages like poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added.

**DSS:** emphasizes flexibility in the decision making approach of users.

**Sanitized live transaction**: test data will be representative of live processing.

**Timebox management**: by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and rapid application development (RAD) and integrates system and user acceptance testing.

**Waterfall life cycle model**: best suited to the stable conditions where requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.

**Compensating controls** are internal controls that are intended to reduce the risk of an existing opotential control weakness that may arise when duties can't be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls can't be achieved when duties can't 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.

The IT balanced scorecard (**BSC**) is a process management evaluation technique that can be applied to the IT governance process in assessing IT functions and processes. BSC provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures of evaluate customer satisfaction.

**The "V" model is a methodology** where development and testing takes place at the same time with the same kind of information available to both teams. It is good practice to write the UAT test plan immediately after the requirements have been finalized.

**Risks** are mitigated by implementing appropriate security and control practices.

**Insurance** is a mechanism for transferring risk.

Audit and certification are mechanisms of risk assurance

**Contracts and SLAs** are mechanisms of risk allocation.

**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.

**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.

**Risk management** involves identifying, analyzing, and taking steps to reduce or eliminate the exposures to loss faced by an organization or individual. The practice of risk management utilizes many tools and techniques, including insurance, to manage a wide variety of risks. Every business encounters risks, some of which are predictable and under management's control, and others which are unpredictable and uncontrollable.

**Compliance testing** determines whether controls are being applied in compliance with policy. Variable sampling is used to estimate numerical values such as dollar values. Substantive testing substantiates the integrity of actual processing such as balances of financial statements. 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.

**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 in a population and is used in compliance testing to confirm whether the quality exists.

**SLA** provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed-on service

**SOA** relies on the principles of a distributed environment in which services encapsulate business logic as a black box and might be deliberately combined to depict real-world business processes.

**Audit charter** should state management's objectives for the delegation of authority to IS audit.

**Continuous auditing techniques** can improve system security when used in time-sharing environments that process a large number of transactions.

**Audit trials** help in establishing the accountability and responsibility of processed transactions by tracing transactions through the system.

**Assessment of risk** should be made to provide reasonable assurance that material items will be adequately covered during the audit work.

**Audit risk** is the combination of detection, control and inherent risks for a given audit assignment. **Control risk** is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls. **Inherent risk** is the risk that an error exists in the absence of any compensating controls.

**Forensic software** is to preserve electronic evidence to meet the rules of evidence.

**Sampling risk** is the risk that an auditor reaches an incorrect conclusion because the sample is not representative of the population. This can be controlled by: Adjusting the sample size; Using an appropriate method of selecting sample items

**Generalized audit software** features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recompilations.

**Audit Risk** = Inherent Risk X Control Risk X Detection Risk

**Audit Risk** = Sampling Risk + Non-Sampling Risk

**Statistical Sampling:** Applies the laws of probability theory to assist the auditor in designing a sampling plan and subsequently evaluating the results of the sample.

**Non-Statistical Sampling:** Is solely based on the auditor's judgment
**Statistical sampling** provides a means of mathematically evaluating the outcome of the sampling plan by applying the laws of probability to measure the likelihood that sample results are representative of the population.

**Nonstatistical Sampling** In nonstatistical sampling, the auditor does not quantify sampling risk. Instead, those sample items that the auditor believes will provide the most useful information are selected. Since conclusions are based on a judgmental basis, nonprobabilistic sample selection is normally conducted.
The goal of the **meeting** is to confirm the factual accuracy of the audit findings and present an opportunity for management to agree on corrective action.

**CAATS vs. Traditional Audit**

- Sample 100% percent of the data
- Test for Specific Risks
- Automated Process
- Easier to Target Sample
- More precise error rate
- Less time / more productive

**What is the difference between incident management and problem management;** Problem management is trying to determine the root cause of the incident; Incident management is to focused on increasing the continuity. ..Returning

**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.

**Attribute sampling**—This type of sampling enables the auditor to estimate the rate of occurrence of certain characteristics of the population (e.g., deviations from performance of a control). It is most often used in performing tests of controls. A deviation would be the failure of a control to function properly (i.e., an error).

**Discovery sampling**—This type of sampling is designed to locate a small number of deviations or exceptions in the population. It is most often used to detect a fraudulent transaction. If there is one deviation (i.e., one fraudulent transaction) in the sample, the auditor must examine the population.

Determining the service delivery objective **(SDO)** = the minimum acceptable operational capability

**Classical variables sampling (CVS)**—This method is used to provide auditors with an estimate of a numerical quantity, such as the balance of an account. It is primarily used by auditors to perform substantive tests. It includes mean-per-unit estimation, ratio estimation and difference estimation. For example, this method would be used to confirm accounts receivable.

**Probability-proportional-to-size sampling**—This method develops an estimate of the total monetary amount of misstatement in a population. PPS uses dollar-unit sampling or monetary-unit sampling (MUS). Other methods are based on instances or occurrences, but this method is based on monetary values, where higher monetary value transactions have a higher likelihood of being chosen in a sample

**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.

**Hash totals** is an effective method to reliably detect errors in data processing.

**An Integrated test Facility (ITF)** 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.

**Audit sampling** is the application of an audit procedure (test of control or substantive testing) to less than 100% of the items within an account balance or class of transactions for the purpose of drawing a general conclusion about the account balance or the entire group of transactions based on the characteristics detected in the sample. Sampling allows an auditor to draw conclusions about transactions or balances without incurring the time and cost of examining every transaction.

Before using **ITF**; should ensure the presence of latest backup of database and application

**Eavesdropping** is one of the most common threats in a VoIP environment. Because most VoIP traffic over the Internet is unencrypted, anyone with network access can listen in on conversations. Unauthorized interception of audio streams and decoding of signaling messages can enable the eavesdropper to tap audio conversations in an unsecured VoIP environment.

**Vulnerability Analysis:** an examination of an asset in order to discover weaknesses that could lead to a higher-than-normal rate of occurrence or potency of a threat.

**Qualitative Risk Analysis:** An in-depth examination of in-scope assets with a detailed study of threats (and their probability of occurrence), vulnerabilities (and their severity), and statements of impact.

**Site classification policy**: A policy that defines sensitivity levels, security controls, and security procedures for information processing sites and work centers.

**Strategic planning:** Activities used to develop and refine long term plans and objectives. The ability to provide the capability and capacity for IT services that will match the levels on and the types of business activities that the organization expects to achieve at certain points in the future.

**ITIL**: framework process for IT service delivery

Digital signatures is to ensure data = **integrity**

**Critical** : These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.

**BSC:** management tool that is used to measure the performance and effectiveness of an organization. key measurements: financial, customer, internal process, innovation and learning

**IT steering committee:** A body of senior managers or executives that discusses high level and long-term issues in the organization. The committee's mission objectives, roles, and responsibilities should be formally defined in a written charter.

**IT steering committee:**

- Provide strategic leadership for IT through the alignment of IT strategic objectives and activities with enterprise strategic objectives and processes.
- Prioritize IT investment initiatives and deliver final approvals and recommendations on proceeding with proposed IT projects.
- Ensure open communication between the IT department and the other functional units

**Quantitative Risk Analysis:** A risk analysis approach that uses numeric methods to measure risk

**Risk acceptance**: The risk treatment option where management chooses to accept the risk as-is

**Residual risks** are REMINING RISKS and Secondary risks are introduced risks that get introduce while planning risk response.

**Quality Assurance** is also a root-cause analysis process.

**Risk mitigation** is to decrease the probability of risk.

**Elapsed time** is the time inclusive of non working days

**Complex project** will best fit in MATRIX org structure

RISK response of eliminating a threat = **RISK AVOIDANCE**

Benchmarking is a Technique used in **QUALITY PLANNING**

**Contract** LEGAL relationship

**IT STRATEGY COMMITTEE**. Ensures alignment between IT and business strategy through enterprise IT governance.

**IT STEERING COMMITTEE**. Oversees major projects – managing priorities and allocating resources with guidance from the IT Strategy Committee

**Waterfall:** requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate

**Risk analysis** is part of audit planning, and helps identify risks and vulnerabilities so the IS auditor can determine the controls needed to mitigate those risks.

**Risk audit** documents the effectiveness of the risk responses

**PERT** – Relies on Optimistic, Pessimistic and Most likely estimates (in Risk rating)

Avoid, Mitigate, Transfer, Accept – are applicable for **Negative Risks**

**Communications** are COMPLEX in Matrix organization

**ROI** = (Benefit – Cost)/Cost

**Sunk Costs**: costs incurred that cannot be reversed irrespective to future events

**Direct cost:** include dedicated labor, material, supplies, equipment, licenses, fees, training, travel, or professional service fees

**Indirect cost:** Example, if a color printer is shared by several project teams, it's difficult to definitively determine what percentage of costs each should share. [Expenses not for ONE project - these are Shared Expenses]

**Cost benefit**: Looking at how much your quality activities will cost.

**The most important critical success factor (CSF)** is the adequate involvement and support of the various quality assurance, privacy, legal, audit, regulatory affairs or compliance teams in high regulatory risk situations. Some IT system changes may, based on risk ratings, require sign-off from key stakeholders before proceeding.

**Attribute Sampling**: is binary, it either conforms to quality or it doesn't (YES or NO).

**Variable Sampling:** Measures how well something conforms to quality (RANGES).

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 RTO, there will be a discrepancy in IT strategies. **It's important to ensure that server restoration can meet the RTO**.

**Transfer**: Transference assigns all or part of risk to a third party through outsourcing, contracts, insurance, warranties, guarantees, or performance clauses

**Authentication** - Just like applying digital signatures to a message digest to identify any altering to ensure authenticity of a message and the source, a **hash function** can also be applied to Authentication.

**Force Majeure Risks**, such as Earthquakes, Floods, Acts of Terrorism, Etc., should be covered under Disaster Recovery Procedures instead of Risk Management.

**Brainstorming** = Meeting.

**Risk tolerance** is the degree, amount, or volume of risk that an organization or individual will withstand.

**Risk ranking** is direct proportional to risk tolerance

**Risk response** = many - many relationship. A single risk can have multiple risk response and vice versa.

**Business risk - Risk of a gain/loss**

**Risk audit** - Measures the effectiveness of risk response

To ensure confidentiality, authentication, and integrity of a message, the sender should encrypt the hash of the message with the sender's; **Private key and then encrypt the message with the receiver's public key**.

Provides the greatest assurance of message authenticity; **the prehash code is encrypted using the sender's private key.**

**Asymmetric Encryption** - Encryption that uses two keys; one public, one private. If data is encrypted with one of the keys, it can only be decrypted with the other key.

Public Key; The encryption key that is given to anyone in the public domain. **Normally used to encrypt data**.

Private Key; The encryption key that is kept secret and should never be shared any ware. **Normally used to decrypt data**.

**Root CA** - Basically the top dog of the certificate hierarchy. The root of the trust chain.

**Intermediate CA** - the Root CA in the trust chain and is often the CA that actually sign any CSRs for the PKI environment it is a part of.

**Digital Signature** - a mechanism in which a message can be sent to someone and they can verify it came from you due to an encrypted (using the private key) hash of the message.

**Identity** - The system/individual that owns the key pair.

**Switch** to reduce network congestion by eliminating traffic that does not involve the specific station

**Compliance tests** can be used to test the existence and effectiveness of a defined process. Understanding the objective of a compliance test is important. IS auditors want reasonable assurance that the controls they are relying on are effective. An effective control is one that meets management expectations and objectives.

**Substantive tests, not compliance tests, are associated with data integrity.**

**Orange** for multimode fibers

**Yellow** for singlemode fibers

**BIA** should emphasize system dependencies. Then, prioritization can occur.

The strongest control is a **preventive control** that is automated through the system. Developing additional access profiles would ensure that the system restricts users to privileges defined by their job responsibilities and that an audit trail exists for those user actions.

**Policy** is how you PLAN to protect.

**Guideline** is how you DO to protect.

**Standard** is a referential for getting a quality level.

**Process** is an operational document.

Preventing duplicate transactions is a **control objective**.

Having output reports locked in a safe place is an **internal accounting control system**

Backup/recovery procedures are an **operational control**

System design and development meeting user requirement is an **administrative control.**

**Parsing** is often divided into lexical analysis and semantic parsing. Lexical analysis concentrates on dividing strings into components, called tokens, based on punctuation and other keys. Semantic parsing then attempts to determine the meaning of the string.

**Disciplinary Policy:** While we talk about the "acceptable use" of assets, "privacy" or "HR policy", till the time we also mention that what disciplinary actions can be taken in case of violation, the impact of multiple policies gets diluted.

**Third Party Access Policy:** Most of the organizations, at one time or other, have to provide access to information area (physical or logical), to third party vendors or outsourced partners. If the areas are not defined & controlled properly through role based access control, it can pose a major risk

Reviewing user's activity logs is a **monitoring control**

Policy = **Preventive control**.

**System testing** = Stress testing + Performance testing + Recovery testing

**Accountability** means knowing what is being done by whom.

The best way to enforce **Accountability** is to implement a log management process that would create and store logs with pertinent information such as user name, type of transaction and hour.

To ensure message integrity, confidentiality and non-repudiation between two parties, the most effective method would be to create a message digest by applying a cryptographic hashing algorithm against: **A The entire message, encrypting the message hash using the sender's private key, encrypting the message using the receiver's public key**. SPi-RPu

**Volatile** (RAM) data refers to information in memory that will be lost when the power is shut off. Prematurely shutting off power erases the evidence of an attack, which is stored in computer chip **RAM**.

**Nonvolatile** (USB, HDD, and ROM) data is the information contained on the **hard disk and flash memory devices**. A graceful shutdown causes the operating system to clean up temporary files and clear the swap file before shutting down.

**Implementing a two-factor authentication**, and using table views to access sensitive data, are controls that would limit access to the database to authorized users but would not resolve the **accountability problem.**

**Suitable patches** from the existing developers should be selected and tested before applying them.

**Statistical sampling** method, in this method deviation rate is one of the factors that affect the population selected.

**Compliance testing:** checks for the presence of controls; **substantive testing** checks the integrity of internal contents.
A major benefit of using **open source** software is that it is free.

**The Capability Maturity Model** creates a baseline reference to chart current progress or regression. It provides a guideline for developing the maturity of systems and management procedures.

**Data retention** is a matter of business needs and requirements. No one in this forum can tell you that this or that is the best practice. It is up to you to find out from your bosses or management what should the data retention be.

Tape backup = **preventive control**

Verify the backup = **detective control**

Verification and audits = **detective controls**

An IS auditor's independence is **not impaired** by providing advice on known best practices.

**IDS** should have detected network behavior anomalies, which may have led to earlier detection.

**Authentication techniques** for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

**Vulnerability scanning** identifies software vulnerabilities, but does not detect malware.

**Reviewing the firewall** rule set is an important activity, but would not be helpful in detecting a data leak.

**Access control monitoring** may help determine access to various information assets, malware may bypass the established access control process and would thus not be detected

**Functionality** is the set of attributes that bears on the existence of a set of functions and their specified properties.

**Portability,** is the transfer software from one environment to other environment

**Reliability** is the capability of software to maintain its level of performance under stated conditions

**Audit Scope:** boundaries described by processes to be reviewed, within specific physical locations of the organization. Keep it simple by describing location, units to measure, specific activities, and a particular process with an applicable time period measured in days, weeks, or months. Compliance never happens in one giant audit. Our goal is to break down the big, complex workflow into a series of small and manageable audits executed on different days or different months.

An **independent test performed by an IS auditor** should always be considered a more reliable source of evidence than a confirmation letter from a third party since a letter does not conform to audit standards and is subjective.

**The IT BSC is a tool** that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate.

**An enterprise data model** is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments.

**The IT organizational structure** provides an overview of the functional and reporting relationships in an IT entity.

**CDP:** organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)

**Terminated Employees Credentials:** Disable the credentials rather remove them, 'cause they may be needed for future reference. You better put control over re enabling the credentials through multiple authorizations, periodically reviewing & automated monitoring mechanism.

The audit involvement decision should be based on the **project risk assessment**

**Matrix organization** consists of a project team formed with people from various functional areas within the organization. These specialists report simultaneously to the project manager and the managers of their functional departments. (**Dual reporting methodology**)

The greatest risk is that previously authenticated sessions can be hijacked and used for illegal purposes if **session time out does not working.**

**Fraud Misrepresentation** to gain an advantage is the definition of fraud. Electronic records may be subject to remote manipulation for the purpose of deceit, suppression, or unfair profit. Fraud may occur with or without the computer. Variations of fraud include using false pretenses, also known as pretexting, for any purpose of deceit or misrepresentation.

**Out-of-band authentication** means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks.

Append themselves to files as a protection against viruses = **Immunizer**

**Retina scanning** is a biometric verification technology that uses an image of an individual's retinal blood vessel pattern as a unique identifying trait for access to secure installations

**Audit planning** is developing an overall strategy for the audit. The nature, extent, and timing of planning varies with size and complexity of the entity, experience with the entity, and knowledge of the entity's business.

**Audit risk** A combination of the risk that material errors will occur in the accounting process and the risk the errors will not be discovered by audit tests. Audit risk includes uncertainties due to sampling (sampling risk) and to other factors (nonsampling risk).

**Authorize:** To give permission for. A manager authorizes a transaction by signing a voucher authorizing the disbursement.

**Eavesdropping** is the traditional method of spying with the intent to gather information. The term originated from a person spying on others while listening under the roof eaves of a house. Computer network analysis is a type of eavesdropping. Other methods include capturing a hidden copy of files or copying messages as they traverse the network.

**Fraud:** Misrepresentation to gain an advantage is the definition of fraud. Electronic records may be subject to remote manipulation for the purpose of deceit, suppression, or unfair profit. Fraud may occur with or without the computer. Variations of fraud include using false pretenses, also known as pretexting, for any purpose of deceit or misrepresentation.

Smart cards working with the users' personal identification number (PIN): **multifactor authentication**

All system access tokens, including dynamic password authentication tokens and telephone credit cards, etc. that have been lost or stolen, or are suspected of being lost or stolen, **must be reported to the service desk immediately.**

**Historical financial statements** do not provide information about planning and lack sufficient detail to enable one to fully understand management's activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

After the previous stages have been completed, the auditor can produce a draft report to be presented and discussed with management. The **draft report** uses the following standard structure: Memo; Conclusion; Background information; Scope; Objectives; Proposals; Risk template and key controls as an appendix; other appendices

**Hash** = integrity

**Hashing** = irreversible = credit card transactions

**CIAN**: confidentiality, integrity, availability, non-repudiation

**Deploying patches** without testing exposes an organization to the risk of system disruption or failure.

In case of performance issue, the appropriate recommendation is to review the results of stress tests during **UAT**.
As part of the effort to realize continuous audit management (CAM), there are cases for introducing an **automated monitoring and auditing solution**. All key controls need to be clearly aligned for systematic implementation; thus, analysts have the opportunity to come across unnecessary or overlapping key controls in existing systems.

**Waterfall** development allows for departmentalization and control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process model phases one by one

**Risk Mamanegment Process in a Project**: ID R + Evaluate R + Manage R + Monitor R + Evaluate RMP

Most EDI transactions go through a **VAN (Value Added Network)** service, which provides the proprietary networks required and translates documents between different companies' formats.

EDI documents is **X12**

**CRC** - Cyclic Redundancy Check - A technique to assure data contained within a block of data is read correctly. Check bits are added to the block of data as it is written that adjust it to make it conform to a particular formula. When the block of data is read, the formula is applied and if it fails, the contents of the block (or the read) are presumed incorrect. This failure is called a CRC Error.

**EDI** = Comm. Handler + EDI interface + Application System

**Comm. Handler** = dialup+ VAN + LL + Pubic SW network

Checking **effectiveness** can only be checked afterwards

**VAN** A privately operated network originally devoted to EDI transactions. VANs now provide other services as well, including translation of EDI transactions for Internet transmission (EDI-INT).

**Data translation** is done by EDI translator which is the other component of EDI interface!

Decision support systems **DSS** come very close to acting as artificial intelligence agents.

**DSS** = Morton (structured) + Carson (Family Tree)

**WBS** = won't help identify dependencies.

**ITF** is an audit technique to test the accuracy of the processes in the application system. It may find control flaws in the application system, but it would be difficult to find the overlap in key controls.

**Forward error control** involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors.

**Block sum check** is an extension of parity check wherein an additional set of parity bits is computed for a block of characters.

**Cyclic redundancy** check is a technique wherein a single set of check digits is generated, based on the contents of the frame, for each frame transmitted.

The process of implementing an automated auditing solution would better identify **overlapping controls**

To evaluate the security of the **client server environment**, all network access points should be identified.

**Risk assessment** is the process used to identify and evaluate risk and its potential effects = **BIA**

The process to review and approve the contract is one of the most important steps in the **software acquisition process.**

An IS auditor should verify that legal counsel reviewed and approved the contract before management **signs the contract.**

User participation is not necessarily required in the software acquisition process. Instead, users **would most likely participate in requirements definition and user acceptance testing (UAT).**

**Independent third-party audit report (External Audit Report)** such as an SSAE 16 would provide assurance of the existence and effectiveness of internal controls at the third party.

**Drive wiping** — this is the act of overwriting all information on the drive. Drive wiping allows the drive to be reused.

**Degaussing** — this process is used to permanently destroy the contents of the hard drive or magnetic media. Degaussing works by means of a powerful magnet that uses its field strength to penetrate the housing of the hard drives and reverse the polarity of the magnetic particles on the hard disk platters.

After a drive has been degaussed**, it cannot be reused.** Next to physical destruction, degaussing is the most secure way to ensure that the drive cannot be reused.

Preventive controls BEST helps secure a web application = **Developer training**

**Substantive test** can reveal whether the operational controls of transaction processing are effective or not.

**Addressing audit objectives** is the primary goal of an IS auditor during the audit planning stage.

**Passive attacks** are characterized by techniques of observation. The intention of a passive attack is to gain additional information before launching an active attack.

Three examples of passive attacks are **network analysis, traffic analysis, and eavesdropping**

**To rank the types of risk,** the auditor must first define the audit universe by considering the IT strategic plan, organizational structure and authorization matrix

**BCP and DRP,** they won't provide assurance related to internal control

All of the roles and responsibilities relating to IS security management should be defined. Documented responsibilities and accountabilities must be established and communicated to **all enterprise users**

**Parallel operation** is designed to provide assurance that a new system meets its functional requirements. This is the safest form of system conversion testing. Also is designed to test the application's effectiveness and integrity of application data, not hardware compatibility

**Hardware compatibility** relates more to the operating system level than to a particular application

Tunnel mode vs Transport mode: **Tunnel mode encapsulate** data and header, **transport mode data only**

The **data owner** holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables.

Device that translates the data between the standard format and a trading partners proprietary format is = **EDI translator**

**Dumpster diving** Most paper records and optical disks are destroyed by shredding.

Transmitting data, **a sequence number and/or time stamp built into the message** to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed.

Digital signatures = **integrity**.

**Gateway**: connects two networks at the highest level of the ISO-OSI framework

**Business risks** include risks that the new system may not meet the users' business requirements, whereas project risks are risks where the project activities exceed the limits of the project budget.

**Preparedness test** is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.

**Paper test** is a walk-through of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution.

**Paper test usually precedes the preparedness test.**

**Post-test** is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third-party systems.

**Walk-through** is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

**WORM:** transmits itself over a network

**Torjan Horse** is client/server; is used to control remote machine without system owner knowledge.

Polymorphic virus = **changes itself**

Acknowledging the receipt of electronic orders with a confirming message will **not authenticate orders from customers**

**BCP table top** exercise is an informal brainstorming session used to encourage participation from business leaders and other key employees. Typically, a business continuity consultant leads the executive team through a discussion, which is focused on the steps that the business's leaders would carry out together in order to activate the firm's BCP procedures during a disaster.

**Identification:** A claim of identity or a search process of comparing all known entries until either a match is found or the data list is exhausted. Identification is known as a one-to-many search process.

**Governance** means the right people of authority made a decision. Governance occurs at the top level of management to prevent anarchy. Decisions made at too low a level below the executives may be an indicator of lack of governance.

**Authentication:** A single match of the identity claim against reference information. If a single attempt fails, the authentication failed. Authentication is a single-try process, also known as a one-to-one process (compare only, no search)

**IT governance:** A clearly stated process of leadership to lead and control the performance expected from the IT function. The focus of IT governance is control over the technology environment.

**Audit Risk:** It is the risk that Information may contain material error that may go undetected during the course of audit.

**Virus** reproduces using a host application. It inserts or attaches itself to the file

**Worm** reproduces on its own without host application

**Logic Bomb/Code Bomb** executes when a certain event happens (like accessing a bank account) or a data/time occurs

**Trojan Horse** program disguised as a useful program/tool

**Remote Access Trojan (RAT)** remote control programs that have the malicious code and allow for unauthorized remote access Back orifice, sub seven, netbus)

An organizational **chart provides information about the responsibilities and authority of individuals in the organization**, this helps an IS auditor to know if there is a proper segregation of functions.

**Botnet** compromise thousands of systems with zombie codes can be used in DDOS attacks or spammers

**Buffer Overflow** Excessive information provided to a memory buffer without appropriate bounds checking which can result in an elevation of privilege. If executable code is loaded into the overflow, it will be run as if it were the program.

**Buffer overflows** can be detected by disassembling programs and looking at their operations.

**Buffer overflows** must be corrected by the programmer or by directly patching system memory.

**Trap Door:** An undocumented access path through a system. This typically bypasses the normal security mechanisms and is to plant any of the malicious code forms.

**Backdoor program** installed by an attacker to enable him to come back on a later date without going through the proper authorization channels

**Preservation and documentation** of evidence are primary concern when conducting an investigation.

**Substantive testing** involves obtaining audit evidence on the completeness, accuracy or existence of data at the individual transaction level. This can be achieved by comparing the data in the application to the base document. In this case, **comparison is made with the vendor invoices.**

**Compliance testing** involves testing the controls designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.

**ITF 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.**

**Qualitative analysis** is typically related to risk analysis.
**Judgment sampling** is a sample that is selected subjectively or not at random, or in which the sampling results are not evaluated mathematically

**Substantive testing** is comparing data from an accounts payable application with invoices received from vendors in the month of December (time based)

**Substantive testing** BASED ON YEARS

**Proxy** = forward internal request to outside network.

**Reverse - Proxy** = forward external request to inside network.

**Years is the base for substantive testing**

**Component-based development CBD approach**: Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic.

**Independence** may be impaired if; actively involved in the development, acquisition and implementation of the application system.

**Substantive testing involves obtaining audit evidence on the completeness, accuracy or existence of data at the individual transaction level.** This can be achieved by comparing the data in the application to the base document. In this case, comparison is made with the vendor invoices.

**Compliance tests** can be used to test the existence and effectiveness of a defined process. Understanding the objective of a compliance test is important.

Occurs when a malicious action is performed by invoking the operating system to execute a particular system call: **Interrupt Attack**

An individual **software component** is a software package, a web service, a web resource, or a module that encapsulates a set of related functions (or data).

**Mandatory access control (MAC)** = policy (enforced by reference monitor and security kernel) controls who has access. No data owner.

**Measurements of critical success factors CSF** for an e-commerce project could include: productivity, quality, economic value and customer service

**DAC** = data owner decides.

To minimize damage from security incidents and to recover and to learn from such incidents, a **formal incident response capability** should be established, and it should include the following phases: Planning and preparation - Detection - Initiation - Recording - Evaluation - Containment - Eradication - Escalation - Response - Recovery Closure - Reporting - Postincident review - Lessons learned

**Reverse proxy** would be clients outside the network (Internet) trying to access resources that are in an internal private network. IT audit and assurance standards require that an IS auditor **gather sufficient and appropriate audit evidence**. The IS auditor has found a potential problem and now needs to determine whether this is an isolated incident or a systematic control failure.

A backup failure, which has not been established at a point, will be serious if it involves critical data, IS Auditor need to **expand the sample of logs reviewed** (more investigation required).

When **business process is identified**, the IS auditor should first identify the control objectives and activities that should be validated in the audit.

To address incidents properly, it is necessary to collect evidence as soon as possible after the occurrence**. Legal advice** may be needed in the process of evidence collection and protection.

**Information security policies** must be balanced between business and security requirements

**Information security policies** cannot provide direction if they are not aligned with business requirements.

**DISA** is a feature enabling remote user's access to an outside line via a PBX with authorization codes.

**Portfolio management** includes:
. Selection of projects based on the best return on investment
. Centralized control of priorities across the projects
. Management of concurrent projects

**Four-eye principle**: business decisions and transactions need approval from two distinguished subjects prior to commitment.

Audit tools incorporates dummy transactions into the normal processing on a system: **ITF**

**SOD**: dissemination of activities and associated privileges for a specific business process among multiple subjects.

**Binding of duties;** assignment of activities and associated privileges for a specific business process to one subject.

**Conflict of interest**: subjects (and information) involved in the execution of one process should not be involved in the execution of another process.

**Need-to-know**: subjects should only obtain the information necessary to run a specific process or carry out a particular task.

**Corrective** = Reduces impact of a threat + Attempts to minimize the impact of a problem = Backup power supplies + IDS + Backup procedures

**Fail safe**—these doors fail in the locked position if power is cut. Although this means that the facility is secure, it also means that employees might not be able to get out of the facility.

**Fail soft**—Locks of this type fail open. Employees can easily leave if power is disrupted, but intruders can also easily enter.

Changes in requirements and design happen so quickly that they are seldom documented or approved **rapid pace** of modifications in requirements and design have an adverse effect on change control.

**Rapid pace** of technological innovation combined with customer demands for the latest technologies within shorter development times and limited budgets create major challenges for system designers and integrators.

**Functional acknowledgments** are standard EDI transactions that tell trading partners that their electronic documents were received.

**Attribute sampling**: The characteristic tested is a property that has only two possible values (an error exists or it does not).

**Functional acknowledgments** are used as an audit trail for electronic data interchange (EDI) transactions.

**External labels** are used to physically control the mounting of the correct tape files

**GAS** - not normally used to test terminal security.

**GAS** refers to software designed to read, process and write data with the help of functions performing specific audit routines and with self-made macros. It is a tool in applying **Computer Assisted Auditing Techniques CAAT.**

**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.

**Process owner involvement** is a critical part of the business impact analysis (BIA), which is used to create the DRP. If the IS auditor determined that process owners were not involved, this would be a significant concern. While well-documented testing procedures are important, unless process owners are involved there is no way to know whether the testing procedures are valid.

**Functions of GAS** include importing computerized data; thereafter other functions can be applied: the data can be e.g. browsed, sorted, summarized, stratified, analyzed, taken samples from, and made calculations, conversions and other operations with.

**Encryption with static keys**—using the same key for a long period of time—risks that the key would be compromised.
It is good control to change passwords periodically to ensure their **confidentiality**.

**Data security controls** are the controls that ensure **data integrity**, not accuracy.

**Computer operations controls** do not ensure data **integrity.**

Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources. **The usage of nonstandard data** definitions would lower the efficiency of the new development, and increase the risk of errors in critical business decisions

**IS auditor** should make the final decision about what to include or exclude from the audit report.

**Application controls** are not the responsibility of the data security function.

**Cost-benefit analysis** of the proposed changes to operating system software does not affect the issue of security over the system.

**Variable sampling** dollar value of inventory

**Vouch** Prove accuracy of accounting entries by tracing to supporting documents.

**Voucher** A document in support of expenditure. The signature of an appropriate official on the voucher is authorization for the treasurer to issue a check.

**Random sample:** identical probability of each population item being selected for a sample; The use of random numbers to select a random sample from a population.

In software testing, **conformance testing** verifies that a product performs according to its specified standards.

Retina scans change depending on the person's health; iris scans are stable; **because the blood vessels in the retina may change depending on certain health conditions.**

**Sniffing** is an attack that can be illegally applied to capture sensitive pieces of information (password), passing through the network.

**Encryption** is a method of scrambling information to prevent unauthorized individuals from understanding the transmission.

**Spoofing** is forging an address and inserting it into a packet to disguise the origin of the communication.

**Validation** involves comparison of the transaction against predefined criteria.

**Digital signature**: Provides the recipient with a method of testing the document received from a sender

Backup method will copy only changed files without resetting the archive bit (archive flag) = **Differential**

The best control over the distribution of data from one department to another is **transmittal document** which records the date and time transmitted.

**Race conditions**: A race is when two (or more) events happen independently, and depending on the order, different things happen. In particular, because of multi-tasking, arbitrary things may be done by other processes between any two lines of your program. For example: "create file, protect it" is not safe – attacker may open file between creation and protection. It must be created in an safe state.

**Race conditions**: interference occurs when a device or system attempts to perform two or more operations at the same time, but the nature of the device or system requires the operations to happen in proper sequence.

**Risk analysis**: analysis of the possibility of suffering loss

**Eavesdropping** can also be done over telephone lines (wiretapping), email, instant messaging, and other methods of communication considered private.

**just-in-time** An inventory system that attempts to minimize inventory costs that do not add value for the customer. It arranges for suppliers to deliver small quantities of raw materials just before those units are needed in production. Storing, insuring, and handling raw materials are costs that add no value to the product, and are minimized in a just in time system.

**A time-stamp** is used to verify that the message was not intercepted and replayed

**A time-stamp** will not necessarily guarantee data integrity.

**Eavesdropping** is secretly listening to the private conversation of others without their consent

**Risk assessment** of business applications would be the first approach to use in evaluating business processes.

**CMMI** is process improvement training

**In a private key cryptosystem**, the key is symmetric such that the encryption key is equivalent to the decryption key both parity checking and access logging are used to detect unwanted conditions.

Passwords = **preventive**

**Off-site backup** can only be used for correction purposes, **off-site backups** are not detective purpose

**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**

**Multiplexor** is an electronic device that combines data from several low speed communication lines into **a single high-speed line**

**IT governance is primarily the responsibility of the executives and shareholders** (**as represented by the board of directors**).

**Multiplexers** are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth.

**PaaS:** Run on distant computers "in the cloud" that are owned and operated by others and that connect to users' computers via the Internet and, usually, a web browser.

**PaaS** offerings typically provide and operating system or a database to the customer. The customer has little visibility into the hardware layer and shares a security control balance with the provider with the customer responsible for the application and data.

**User involvement** is necessary to obtain commitment and full benefit from the system.

Multiplexer = **data selector**.

**CA** is a trustworthy organization willing to vouch for the identities of those to whom it issues certificates. There can be hierarchies of certifying authorities, assuring the validity of the certified public keys.

**Warm site** has the basic infrastructure facilities implemented, such as power, air conditioning and networking, but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

**Switching** usually makes a peer-to-peer connection between two different nodes on the network. It is impossible (or extremely difficult) to overhear such communication from other nodes on the network.

**Multiplexer** is often used with a complementary **de-multiplexer** on the receiving end.

With **SaaS**, you no longer have to purchase, install, update and maintain the software.

**Session layer**: functions include security, recognition of names, logons and so on.

Careful programming and good administration practices help to **reduce race conditions**.

**Presentation layer** provides common communication services such as encryption, text compression and reformatting.

**Electronic data interchange (EDI)** is an electronic communication system that provides standards for exchanging data between two different companies, even in two different countries can electronically exchange documents

**EDI** reduces the costs and delays associated with handling and movement of paper documents as well as the inefficiencies of redundant entry of data

**Embedded Audit Module (EAM):** Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria. Identification of reportable items occurs as part of real-time processing.

**Reporting may be real-time online**, or may use store and forward methods. Also known as integrated test facility or continuous auditing module.

**Race conditions** occur due to interferences caused by the following conditions: Sequence or Nonatomi - Locking failure - Deadlock – LiveLock.

**Embedded audit module** = data selection technique.

**Systems analyst and programming** are two functions that need to work together and **share experiences**.

Test data and **integrated test** facility require predetermined results which will provide assurance that program procedures are working properly.

**Embedded audit modules** select only specified transactions.

**Phishing techniques include**: social engineering, link manipulation, web site forgery

The system should automatically disconnect a **logon session** if no activity has occurred for a period of time. This reduces the risk of misuse of an active logon session left unattended.

**Spear phishing** A pinpoint attack against subset of people (users of web site or product, employees of a Company, members of an organization) to undermine that company or organization

**Check digits** test for proper entry of certain fields.

**GAS** may be applied directly to data files which are the result of processing

**Data Mart** The *data mart* is a repository of the results from **data mining the warehouse**. You can consider a data mart the equivalent of a convenience store. All of the most common requests are ready for the user to grab.

A decision support system retrieves prepackaged results of **data mining** and displays them for the user in a presentation program, typically a graphical user interface (GUI).

The **data base administrator** is responsible for the organization and maintenance of the data base. Access restrictions may also be the responsibility of the data base administrator, however, normally access control is the responsibility of the data security officer.

**Data Conversion**: risk is you will not convert all the data – some will be missed. You also need to make sure that you are comparing control totals before and after conversion to avoid this.

**Certifications and accreditation** of the system take place in the implementation Phase.

**Certification** tests a system's internal controls for correct functionality against a known reference.

**Certification** is a technical review of the system. Before systems are placed into operation, they must undergo certification.

**Certification** is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meet a pre-specified set of security requirements.

**Organization's strategic plan** drive applications/software to be used -> drive the type of hardware needed.

**Audit trail** efficiency of the audit.

**Audit trail** is a visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source

**Data Mining** After the database and rules are created, the next step in the operation of a decision support system is to drill down through the data for correlations that may represent answers. **The drilling for correlations is referred to as *data mining*.** To be successful, it would be necessary to mine data from multiple areas of the organization.

**Artificial intelligence (AI)** is the subject of many technology dreams and some horror movies. The concept is that the computer has evolved to the level of being able to render its own decisions. Depending on your point of view, this may be good or bad. Artificial intelligence is useful for machines in a hostile environment. The Mars planetary rover requires a degree of artificial intelligence to ensure that it could respond to a hazard without waiting for a human to issue instructions.

**Database snapshots** can provide an excellent audit trail for an IS auditor.
Advancements in computer programming technology and databases have led to the creation of decision support systems. **DSS** is a database that can render timely information to aid the user in making a decision. There are three basic types of decision support system.

Computer operators should not have access to **source documents**.

**Atomicity** means that you can guarantee that all of a transaction happens, or none of it does; you can do complex operations as one single unit, all or nothing, and a crash, power failure, error, or anything else won't allow you to be in a state in which only some of the related changes have happened.

**Consistency** means that you guarantee that your data will be consistent; none of the constraints you have on related data will ever be violated.

**Control totals** can be used to compare batches too.

**Concurrency control** Refers to a class of controls used in a database management system (DBMS) to ensure that transactions are processed in an atomic, consistent, isolated and durable manner (ACID). This implies that only serial and recoverable schedules are permitted, and that committed transactions are not discarded when undoing aborted transactions

**Durability** means that once a transaction is complete, it is guaranteed that all of the changes have been recorded to a durable medium (such as a hard disk), and the fact that **the transaction has been completed is likewise recorded**.

**Substantive for integrity and compliance for presence of control**

**Atomicity:** Means All or None. Which means a database transaction will be either complete or NIL and never in between. If A=5 and we have to add another 5 to A. A will be 10 if transaction is complete otherwise A will remain 5, never anything else.

**Consistency**: All integrity constraints or integrity rules will be taken care by all transaction.
Deploying **patches** without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

**Non-repudiation:** It is a security service by which evidence is maintained so that the sender and the recipient of data cannot deny having participated in the communication. Individually, it is referred to as the "non-repudiation of origin" and "non-repudiation of receipt.

**Risk management** – managements risk tolerance and how to deal with each specific risk.

The most important **critical success factor** (CSF) is the adequate involvement and support of the various quality assurance, privacy, legal, audit, regulatory affairs or compliance teams in high regulatory risk situations. Some IT system changes may, based on risk ratings, require sign-off from key stakeholders before proceeding

**Screening routers:** router configured to permit or deny traffic based on a set of permission rules installed by the administrator

**Security administrator**: The person responsible for implementing, monitoring and enforcing security rules established and authorized by management

**Security incident**: A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites.

**A security incident normally includes an estimation** of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified.

**Security policy**: A high-level document representing an enterprise's information security philosophy and commitment

**Security procedures**: The formal documentation of operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved

**SoD**: A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets

**Sequence check:** Verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research

**Sequential file**: A computer file storage format in which one record follows another

The ideal humidity for a data center is **35%–45%.**

**Audit Exceptions**: errors omissions, irregularities, illegal acts.

Represents the greatest source of losses in data processing = **Errors and omissions**.

**Service bureau:** A computer facility that provides data processing services to clients on a continual basis

The purpose of **debugging programs** during system development is to ensure that all program abends (unplanned ending of a program due to programming errors) and program coding flaws are detected and corrected before the final program goes into production. A debugging tool is a program that will assist a programmer in debugging, fixing or fine-tuning the program under development.

**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.

**Fault-tolerant hardware** is the only technology that currently supports continuous, uninterrupted service.
Load balancing is used to improve the performance of the server by splitting the work between several servers based on workloads.

**HA computing** facilities provide a quick but not continuous recovery, while distributed backups require longer recovery times.

**Data edits** are implemented before processing and are considered **preventive integrity controls**.

**Packet switched** – message sent in packets and security on each packet Circuit Switched – path established to communicated

**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 integrity of the OS.

**Atomicity** refers to the transaction being "all or nothing." On the failure of a transaction; the change is backed out of the database, and the data is restored to its original state of consistency.

**IPSec** works on two basic packet components—ESP and AH. ESP encrypts the data and stores them in an encapsulated security payload packet component for data protection. Though essential, AHs manage the authentication process, not the security of the data.

**Semantic nets** are part of artificial intelligence. Semantic nets-Consist of a graph in which the nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes.

**Semantic nets** resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of data.

Unlike **product leakage**, data leakage leaves the original copy, so it may go undetected.

The effectiveness of a **BCP can best be determined through tests.** If results of tests are not documented, then there is no basis for feedback, updates, etc.

While creating **a duplicate SAN and replicating** the data to a second SAN provides some redundancy and data protection, this is not really a backup solution. If the two systems are at the same site, there is a risk that an incident such as a fire or flood in the data center could lead to data loss.

**Attenuation** is the weakening of signals during transmission. UTP faces attenuation around 100 meters.

**Top-down** approach to testing ensures that interface errors are detected early; testing of major functions is conducted early.

**Bottom-up** approach to testing begins with atomic units, such as programs and modules, and works upward until a complete system test has taken place.

**Risk assessment and business impact assessment** are tools for understanding business-for-business continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

**Sociability testing** and system tests take place at a later stage in the development process.

**Standing data** should be purged from the equipment prior to disposal. Standing data refers to information that can be recovered from a device by using any means.

**Compliance risk** is the penalty applied to current and future earnings for nonconformance to laws and regulations, and may not be impacted by the number of users and business areas affected.

**Inherent risk** is normally high due to the number of users and business areas that may be affected. Inherent risk is the risk level or exposure without taking into account the actions that management has taken or might take.

**White box** – assess effectiveness of software program logic.

**Black box** – testing of interfaces and general function – doesn't care about internal structure.

**Residual risk** is the remaining risk after management has implemented a risk response.

**Continuous auditing**: allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.

**Out sourcing**, The IS auditor should be most concerned if the strategy is to transfer an organization's legal compliance responsibility.

**Identification of the assets** to be protected is the first step in the development of a risk management program.

Based on the **observations and interviews**, the IS auditor can evaluate the segregation of duties.

**Function/validation** = similar to system testing, but often used to test the functionality of the system against requirements.

**Regression testing** – rerunning a portion of a test scenario to make sure that changes have not introduced new errors in other parts of app

**Parallel** – feed test data into two systems (new and old) and compare results

**Sociability** – confirm that the new system can operate in its target environment without affecting other systems.

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 failures (MTBF).**

**AV**: Signature based cannot detect new malware; Heuristic behavioral can detect new malware

**LiFo** "Last In First Out" inventory cost flow.

**kiting** Drawing a check on insufficient funds to take advantage of the time required for collection.

**Lapping** = A scheme to cover embezzlement by using payments made by one customer to reduce the receivables balance of another customer.

**Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

Due to its exposure to the Internet, storing customer data for six months raises concerns regarding **confidentiality** of customer data

The **risk** estimate can be presented either: Qualitatively: the evaluated risk is described in words. The estimate of risk is ranked or separated into descriptive categories. Quantitatively: the evaluated risk is estimate numerically; numerical expressions of risk are provided.

**Clean Desk Policy Explore** instituting a policy that addresses employees' housekeeping habits at work, from how to handle unattended documents and storage media to the document disposal in the waste bin.
In a risk-based approach to an IS audit, the scope is determined by the impact the devices will have on the audit. If the undocumented devices do not impact the audit scope, then they may be excluded from the current audit engagement, IS Auditor should evaluate the impact of the **undocumented devices** on the audit scope.

**Reciprocal agreements**: in which two or more parties agree to share their resources in an emergency or to achieve a common objective. In disaster if the two partnering organizations are in close geographic proximity, this could lead to both organizations being subjected to the same environmental disaster, such as an earthquake

**Naming conventions for system resources** are important for the efficient administration of security controls. The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules.

**Naming conventions** tend to be based on how each organization wants to identify its resources.

**EA** should be envisioned as a process that will help the Enterprise to improve itself and its performance in delivering services & achieving business goals. The Enterprise Architecture process will improve the current situation and every new cycle of the process will advance this progress. It is more geared towards managing strategic change initiatives rather than solving day-to-day operational problems

**Sociability testing** = it looks if the application can fit into environment

When an IS auditor uses a **source code comparison** to examine source program changes without information from IS personnel, the IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify the changes

**Infrastructure as a service** = IaaS, no need to invest in your own hardware, you rent infrastructure in IaaS

**IS Auditor** would not automatically retract or revise the finding.

**Transaction authorization** is the primary security concern for EDI environments.

**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.

IS auditor needs to be **proactive**. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risk to the organization and work with management to have these corrected.

**IS Auditor**: should stress the importance of having a **system control framework** in place

**Forensic**: fraud investigations

**Diverse Routing**: routing traffic through split cable or duplicate cable

**Digital signatures** require the signer to have a private key and receiver to have public key; are intended to verify to a recipient the integrity of the data and identify of the sender; contains a message digest to show if the message has been altered after transmission

**Diverse Routing** means one provider, but multiple routes (or paths), duplicate cables

**VPN Risk** - Malicious code could be spread across the network.

**Tuple** - Row in a database table.

**Trojan horse** - hidden malicious or damaging code within an authorized computer program

**Formal approval** is necessary before moving into the next phase. A review meeting is held with the stakeholders, project manager, and executive chairperson. All of the projections and open issues are discussed. Each item is approved, rejected, or cancelled. The project may advance to the next stage with formal approval. The auditor should look for evidence of formal approval and how the decision was made.

**Disaster**: RPO acceptable amount of data loss measured in time; RTO duration of time and a service level within which a server must be restored after a disaster

**ITSM** is the organizational implementation of a management model used to design, implement and manage quality services for business customers. This includes defining touchpoints with other management frameworks and adoptation to particular organizational capabilities and functions.

**Alternate Routing** means multiple network providers, and/or multiple mediums (fiber, cable, radio)

**Variable sampling** technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount

**Agile development** – used when don't have much in the way of requirements and things are changing frequently (iteration); Designed to flexibly handle changes to the system being developed. Use of small time boxed subprojects and greater reliance on tacit knowledge in people's heads. No real requirements baseline. Not much documentation; Less testing. Project Manager becomes more of an advocate and facilitator rather than manager; Can help detect risks early on; Lots of face to face work.

Organization must have **standard project selection framework** as per organization's IT strategy, since that is going to help steering committee in deciding the priority of project selection.

**Risk assessment** is a technique used to examine auditable units in the IS audit universe and select areas for review to include in the IS annual plan that have the greatest risk exposure**.**

**Audits** often involve resource management and deadlines similar to project management best practices.

**EA** success should be measured as factor of delivering successful change initiatives or providing tangible benefits like cost reduction, improving efficiency of business processes or reusing IT assets.

**Last-mile circuit** = from office (or home) to service provider (local ISP, microwave or cable company)

**RBAC** key feature of this model is that all access is through roles. A role is essentially a collection of permissions, and all users receive permissions only through the roles to which they are assigned (users - roles – permission).

**Privacy policy awareness training** should be performed to assist technician with understanding what should not be listed within the comments section of tickets (personal identifiable information PII)

**Quality reviews are a detective control** and will only discover exceptions after the information has been entered.

**Digital signatures** provide authentication assurance of the email sender. Digital signatures use the private key of the sender to lock (encrypt) and the sender's public key to verify the sender's identity (by unlocking). Message **hashing** provides assurance the message was not modified

**Centralized management** always provides the most control. Distributed management is also known as discretionary because the decision is made locally and is based on a variety of factors. Distributed methods provide the lowest overall control.

**DES** uses less processing power when compared with AES;

**AES** consumes too much processing power

**PKI** is primarily used to gain assurance that protected data or services originated from a legitimate source = confidentiality

**Two-factor user authentication**: A smart card addresses what the user has, not recommended magnetic card may be copied

**Direct observation of results** is better than estimations and qualitative information gained from interviews or status reports.

**Risk assessment** is a technique used to examine auditable units in the IS audit universe and select areas for review to include in the IS annual plan that have the greatest risk exposure.

**To govern IT effectively**, IT and business should be moving in the same direction

**CAAT Computer-assisted audit tools** are able to perform detailed technical tasks faster than humans and produce more accurate data during particular functions such as system scanning. Cost, training, and security of output are major considerations

**Computer logs** will record the activities of individuals during their access to a computer system or data file and will record any abnormal activities, such as the modification or deletion of financial data.

**Cipher lock** is one in which a keypad is used for entering a pin number or passwords

Provide the GREATEST assistance in developing an estimate of project duration = **PERT chart**

**Firewall systems** are the primary tool that enables an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls.

**Batch control reconciliations** is a compensatory control for mitigating risk of inadequate segregation of duties

**Run-to-run control totals** are totals of key fields - in this case the totals of the receivables balances - taken when the receivables are posted. If the totals are recalculated and compared with previous balance, this would detect alterations between postings

**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 whether it is authorized or unauthorized traffic.

**Audit trail** of only the date and time of the transaction would not be sufficient to compensate for the risk of multiple functions being performed by the same individual.

Review of the **Summary Financial Reports** would not compensate for the segregation of duties issue. Supervisor review of user account administration would be a good control; however, it may not detect inappropriate activities.

**RISK** = the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

**RTO:** indicates a point in time that the restored data should be available for the user to access.

**Backup Strategy:** Planned approach to data protection through a backup-policy that assigns the backup responsibilities to the appropriate personnel or departments, and sets the duplication time cycles.

**BCP:** A state of continued, uninterrupted operation of a business.

**BCM**: A whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption.

**Business continuity plan**: A component of business continuity management. A business continuity plan is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organization in the event of a disruption.

**Business impact analysis BIA**: A component of business continuity management. Business impact analysis is the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements, and essential staff and to help shape a BCP.

**Cold Site:** An information system (IS) backup facility that has the necessary electrical and physical components of a computer facility, **but does not have the computer equipment in place**. The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative additional functions.

**Crisis Management**: Set of procedures applied in handling, containment, and resolution of an emergency in planned and coordinated steps.

**Critical business functions:** Any activity, function, process, or service, the loss of which would be material to the continued operation of the financial industry participant, financial authority, and/or financial system concerned. Whether a particular operation or service is "critical" depends on the nature of the relevant organization or financial system.

**Confidentiality:** Assuring information will be kept secret, with access limited to appropriate persons.

**Authenticity:** The property of genuineness, where an entity is what it claims to be.

**Integrity:** Assuring information will not be accidentally or maliciously altered or destroyed.

**Non-repudiation**: Ensures that information cannot be disowned.

**Cipher:** method that encrypts or disguises text.

**Algorithm**: A procedure or formula for ciphering.

**Key clustering**: when two different keys generate the same cipher text, the same plaintext.

**Hash:** A short value calculated from digital data that serves to distinguish it from other data.

**Disaster Recovery:** Activities and programs designed to return the organization to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan **to restore an organization's critical business functions.**

**DRP**: A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.

**Automated code comparison** is the process of comparing two versions of the same program to determine whether the two correspond.

**Supervision**— IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

**Limit Check** (e.g., hours worked do not exceed 40 hours);
**Reasonableness Check** (e.g., increase in salary is reasonable compared to base salary)

**Evidence**— During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

**Documentation**— The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions.

**Duplicate (redundant) IPFs (Information processing facility):** They are dedicated, self-developed recovery sites that can backup critical applications. They can range in form a standby hot site to a reciprocal agreement with another company installation.

**Hot Sites:** They are fully configured and ready to operate within several hours. The equipment, network and systems software must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation.

**Reciprocal Agreements** with other organizations: This is a less frequently used method between two or more organizations with similar equipment or applications. Under the typical agreement, participants promise to provide computer time to each other when an emergency arises.

**Recovery Point Objective (RPO)**: The recovery point objective is determined based on **the acceptable data loss** in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data. RPO effectively quantifies permissible amount of data loss in case of interruption.

**Recovery Strategy:** A recovery strategy identifies the best way to recover a system in case of an interruption, including disaster, and provides guidance based on which detailed recovery procedures can be developed.

**Recovery Testing**: A test to check the system's ability to recovery after a software or hardware failure.

**Recovery Time Objective (RTO):** The recovery time objective is determined based on the acceptable down time in case of disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

**Warm Sites**: They are partially configured, usually with network connections and selected peripheral equipment, such as disk drives, tape drivers, and controllers, but without the main computer. Sometimes a warm site is equipped with a less-powerful CPU, than the generally used. The assumption behind the warm site concept is that the computer can usually be obtained quickly for emergency installation and, since the computer is the most expensive unit, such an arrangement is less costly than a hot site.

**Data diddling** is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.

**IRP** determines the information security responses to incidents such as cyber-attacks on systems and/or networks.
One of the main objectives of an audit is to **identify potential risk**; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization

**Risk analysis** is a process by which the likelihood and magnitude of IT risk scenarios are estimated. Risk analysis is conducted to ensure that the information assets with the greatest risk likelihood and impact are managed before addressing risk with a lower likelihood and impact. Prioritization of IT risk helps maximize return on investment for risk responses.

**Audit charter** is a general document whereas an engagement letter is specific to the audit being conducted

To do IT audit the auditor performs Understanding the **objective of company**

**COBIT** Plan and organize - Acquire and implement - Deliver and support - Monitor and evaluate

**Sampling risk** is which the auditor took a wrong conclusion from the sampled item

**Attribute sampling** is used for compliance testing

**Variable Sampling** used for substantive testing.

**Variable sampling** also called as mean estimation or dollar estimation sampling used for monetary values.

**Audit** is not implementing its checking the standards as per industry and organization.

**CAATs would enable the IS auditor to review the entire invoice file to look for those items that meet the selection criteria**; it should be used use to detect duplicate invoice records within an invoice master file

**Attribute sampling** would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates.

**Test data** are used to verify program processing, but will not identify duplicate records.

**ITF allows the IS auditor to test transactions through the production system**, but would not compare records to identify duplicates

**Expected error rate** is only applied for attribute sampling not for variance sampling.

From a control perspective **job description** establish responsibility and accountability

**GAS** refers to direct access to read and access data from different database platforms, flat file systems and ASCII formats.

**Integrated auditing** involves making a combined report based on the risks from different departments

**Types of audit:** Operational - Integrated - Administrative - Compliance – Financial; FACIO

**Audit report** should explain the restrictions placed by the management on the scope of audit

**Audit types**: system, process, product, organizational plans, general controls.

**IS controls are classified:** General + Pervasive + Detailed + Application

**Governance** helps to ensure that IT objectives help the enterprise objectives to be fulfilled. On IT governance, auditor has to check if IT objectives are aligned with the objectives of the **business needs**.

**IT balanced scorecard** is an evaluation technique used for IT governance to assess IT functions and objectives.

**The outcome of IT governance** is proper Strategic alignment - Value delivery - Resource management - Performance management - Risk management

**Enterprise Architecture (EA**) is a structured manner in which IT assets are documented for understanding, management and planning for IT investments.

**Cross training** ensures that there is no dependency on a single person and it also used as a backup if incase the first person is not available.

**Gantt** is used to identify the resource consumed and Progress

**PERT** is used for identifying the critical path, delays, probable completion time.

**Check digit** is used to identify transposition and transcription errors

**CAAT** are able to perform detailed technical tasks faster than humans and produce more-accurate data during particular functions such as system scanning. Cost, training, and security of output are major considerations

**Sensitive systems** are the one which needs controls to operate for a longer period of time manually, critical needs immediate replacement, vital can be operated for shorter period of time only

**IT BSC** ensures that IT could be aligned with business objective

If **corrective corrections** have been taken after the audit has started then during audit report the findings have to be mentioned with appropriate actions taken

**EAM (Enterprise audit module)** is also called as integrated test facility which uses some dummy transactions and runs live transactions, compares the results.

**Continuous & intermittent simulation (CIS)** audit is based on that the SW tests for a certain condition to fulfill and then the audit is performed on the identified transaction.

**Statistical sampling** is referred by the means of percentage.

Mission + Strategy + Metrics = **IT BSC**

When dealing with **outsourcing legal issues** would differ from one country to other.

**CMM** = IRDMO = Initial + Repeatable + Defined + Managed + Optimized

**Independence** could be compromised if the IS auditor advises on the adoption of specific application controls. Independence could be compromised if the IS auditor were to audit the estimate of future expenses used to support a business case for management approval of the project.

**CAAT** are able to perform detailed technical tasks faster than humans and produce more-accurate data during particular functions such as system scanning. Cost, training, and security of output are major considerations

**Digital signatures** provide authentication assurance of the email sender. Digital signatures use the private key of the sender to lock (encrypt) and the sender's public key to verify the sender's identity (by unlocking). A message hash provides assurance that the message was not modified.

**Process owner** involvement is a critical part of the business impact analysis (BIA), which is used to create the DRP. If the IS auditor determined that process owners were not involved, this would be a significant concern.

IT audit and assurance standards require that an IS auditor gather sufficient and appropriate audit evidence such as **expand the sample of logs reviewed.**

It is important that the data entered from a remote site is edited and validated prior to transmission to the **central processing site. RPO is based on the acceptable data loss in the case of a disruption**; the organization needs a short RPO. Virtual tape libraries, disk-based snapshots and disk-to-tape backup would require time to complete the backup, while **CDP continuous data backup** happens online (in real time).

**IT steering committee**: project approval and prioritization, developing the long-term IT plan, advises the board of directors on the relevance of developments in IT

**Library control software** should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized

**RPO** = acceptable amount of data loss measured in time

**RTO** = duration of time and a service level within which a server must be restored after a disaster
Periodic review of the access list by the **business owner** should determine whether errors in granting access have occurred.

**EDI translator** convert data from EDI format to propriety format,

**EDI interface** used for data movement and mapping

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
**Reasonable assurance** the audit will cover material items.
Only tests and exercises demonstrate the adequacy of the plans and provide reasonable assurance of an organization's **disaster recovery readiness**.

**Compensating Controls** – They are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated.

**Preventive Controls** - These are controls that prevent the loss or harm from occurring. For example, a control that enforces segregation of responsibilities (one person can submit a payment request, but a second person must authorize it), minimizes the chance an employee can issue fraudulent payments.

Using a **statistical sample** to inventory the tape library is an example of a substantive test.

If proper identification and authentication **are not performed during access control, no accountability** can exist for any action performed.

**ISACA audit standards** of professional ethics are intended to provide consistency. We do not want you to cast any disgrace upon our profession. We hope that by following the standards, you will not embarrass yourself or fail to understand the duties of an auditor.

**Crypto**: The sender generates a hash of the plaintext and encrypts the hash with a private key. The recipient decrypts the hash with a public key.

In planning an audit, the most critical step is identifying the **areas of high risk.**

When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which **controls are exercised as data flows through the system.**

When implementing **continuous-monitoring** systems, and IS auditor's first step is to **identify high-risk areas** within the organization.

**Inherent risk** is associated with authorized program exits (trap doors). TD is unauthorized electronic exit, or doorway, out of an authorized computer program into a set of malicious instructions or programs

**GAS** can be used to search for address field duplications.

**Lack of reporting of a successful attack** on the network is a great concern to an IS auditor.

**Integrated test facility** is considered a useful audit tool because it compares processing output with independently calculated data.

**CMM** - IRDMO - Framework to help organizations **improve their software lifecycle** processes: Initial – Repeatable – Defined – Managed – Optimized

If the **RTO is high, then the acceptable downtime is high**. **Cold site will be appropriate in such situations.**

It is true that an advantage of a **continuous audit** approach is that it can improve system security when used in **time-sharing environments that process a large number of transactions.**

**An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence.**

**Business unit management is responsible for implementing cost-effective controls in an automated system**
Reviews an organization chart is to **better understand the responsibilities and authority** of individuals.

IS auditor finds out-of-range data in some tables of a database => **Implement integrity constraints in the database.**

**Higher humidity causes condensation and corrosion.**

**Lower humidity increases the potential for static electricity.**

The ideal humidity range for computer equipment is **40% to 60%**.

When **auditing third-party service providers**, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

**IS assessment methods** allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

**Reviewing an audit client's business plan** should be performed before reviewing an organization's IT strategic plan.

**Security administrators** are usually responsible for network security operations.

**Computer logs** will record the activities of individuals during their access to a computer system or data file and will record any abnormal activities, such as the modification or deletion of financial data.

**Audit trail** of only the date and time of the transaction would not be sufficient to compensate for the risk of multiple functions being performed by the same individual.

**Review of the summary financial reports would not compensate for the segregation of duties issue**. Supervisor review of user account administration would be a good control; however, it may not detect inappropriate activities

**Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet** behind the bastion host provides a higher level of protection from external attack than all other answers.

**The directory system** of a database-management system describes the location of data and the access method.

To properly protect against **unauthorized disclosure of sensitive data**, hard disks should be demagnetized before disposal or release.

**Cryptography** does not directly provide availability

**Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL**, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality.

**WAP Gateway** was the key element of any internet system connected to the wireless network. It ensured the connection and conversion of information between WAP devices and the web server.

**Proper segregation of duties** prevents a computer operator (user) from performing security administration duties

**Modems (modulation/demodulation)** convert analog transmissions to digital and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

**Neural networks** are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem; **neural network:** A type of artificial intelligence system that approximates the function of the human nervous system.

Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. **A program could be developed to identify these conflicts.**

**Diverse routing** supports data transmission through split cable facilities, or duplicate cable facilities.

**Strategy** = adaptation of behavior or structure with an elaborate and systematic plan of action.

**Strategy** = create a fundamental change in the way the organization conducts business

**Stateful firewall** (any firewall that performs stateful packet inspection (SPI) or stateful inspection) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. **Only packets matching a known active connection will be allowed by the firewall; others will be rejected.**

Inefficient and superfluous use of network devices such as **hubs** can **degrade network performance.**

SOD = **separation of powers**

**Data mirroring** and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

**Inherent risk**: The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

**Initial program load (IPL):** The initialization procedure that causes an operating system to be loaded into storage at the beginning of a workday or after a system malfunction.

**Input control:** Techniques and procedures used to verify, validate and edit data to ensure that only correct data are entered into the computer

**Input control**: Transaction log, Reconciliation of data, documentation, Anticipation, transmittal log, cancellation of source document.

**Integrated services:** A public end-to-end digital telecommunications network with signaling, switching and transport capabilities supporting a wide range of service accessed by standardized interfaces with integrated customer control

**Integrated test facilities:** A testing methodology in which test data are processed in production systems

**Integrity**: The guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Interface testing:** A testing technique that is used to evaluate output from one application while the information is sent as input to another application

**Internal controls**: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

**Inherent risk:** The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

**XML language called SOAP is used to define APIs**. Will work with any operating system and programming language that understands XML. Easier than RPC approach because modules can be loosely coupled so a change to one component does not normally require changes to others.

The sender of a public key would be authenticated by a: **digital certificate**.

Implementing a system to provide secure email exchange with its customers; the BEST option to ensure confidentiality, integrity and nonrepudiation = **Digital Certificate**

**Spoofing** an attack using packets with the spoofed source Internet packet (IP) addresses.

**Spoofing:** Committing fraud by masquerading as a legitimate user or another system.

**SQL injection:** represent the most common method of integrating between programs, especially e-commerce across the Internet.

**Encrypted with the recipient's public key and decrypted with the recipient's private key**.

**Neural network** will monitor and learn patterns, reporting exceptions for investigation. Database management software is a method of storing and retrieving data. MIS provides management statistics but does not normally have a monitoring and detection function.

**CAAT** detect specific situations, but are not intended to learn patterns and detect abnormalities.

**Discovery sampling** is used when an auditor is trying to determine whether a type of event has occurred, **risk of fraud**

**Email spamming is a common mechanism used in phishing attacks.**

**ITAF** design recognizes that IS audit and assurance professionals are faced with different requirements and different types of audit and assurance assignments, ranging from leading an IS-focused audit to contributing to a financial or operational audit. ITAF is applicable to any formal audit or assurance engagement.

**ITAF** applies to individuals who act in the capacity of IS audit and assurance professionals and are engaged in providing assurance over some components of IT systems, applications and infrastructure.

**Compensating controls** may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

**Data mirroring and parallel processing** are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

**Outbound traffic** filtering can help prevent an organization's systems from participating in a distributed **denial-of-service (DDoS)** attack.

Nontechnical attack attempts to lure the victim into giving up financial data, credit card numbers, or other types of account information = **Phishing**

Improperly configured routers and router access lists are a common vulnerability for **DoS**.

How management controls the use of **encryption**? Is the encryption managed under a complete life cycle from creation to destruction? The management of keys should govern creation storage, proper authorization, correct use with the appropriate algorithm, tracking, archiving or reissuing, retiring, and ultimately the destruction of the encryption keys after **all legal obligations have been met**

**Traffic analysis** is a passive attack method used by intruders to determine vulnerabilities.

**CAAT**s are able to perform faster than humans and produce more-accurate data in functions such as system scanning. Cost, training, and security of output are major considerations

**Dry-pipe sprinklers** are considered to be the most environmentally friendly as fire suppression.

The ideal **humidity** for a computer room is between 35%-45% at 72 degrees. This will reduce the atmospheric conditions that would otherwise create high levels of static electricity.

**A callback system** is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

**An active IDS** (now more commonly known as an intrusion prevention system — IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator.

**A passive IDS** is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own.

**A host-based IDS** can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

**Prevent a successful brute-force** attack would be to: configure a hard-to-guess username.

**Root kits are malicious software designed to subvert the operating system security**. Software agents such as auto-update utilities are the same as root kits. Both can compromise system security and use stealth to hide their presence. After a root kit is installed, the system is completely compromised.

**Digital signatures** = The sender encrypts the hash with a private key

**Cryptography** provides authentication such as having a private key in a digital certificate. It provides integrity and confidentiality but has little to do with availability of information (e.g.. replication, clustering etc)

Internet attack = **Screened subnet firewall**

**Password guessing** attempts to log into the system, password cracking attempts to determine a password used to create a hash

**Virus scanning software application** a against the introduction of Trojan horse software into an organization

Ensure **data confidentiality** in a commercial business-to-business (B-to-B) web application = Encrypting transactions using the recipient's public key

**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.

**A knowledge-based (or signature-based) IDS** references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS. It has lower false alarm rates than behavior-based IDS.

**Dry-pipe sprinkler** system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

**Audit risk is affected by sampling risk.**
- Sample for performance of tests may not be representative of population
- Conclusions drawn may not be same as if sample was representative

**Digital signatures require** the sender to "sign" the data by encrypting the data with the sender's private key, to then be decrypted by the recipient using the sender's public key.

**Biometrics** provides only single-factor authentication, many consider it to be an excellent method for user authentication.

**Symmetrical Cryptography** = A system where the **same key** can encrypt AND decrypt data

**Asymmetrical Cryptography** = A system where one key encrypts data, and **another key** decrypts it

**Cipher** = A formula used to encrypt data

**SEED** is a block cipher, something that is "fed" to a cipher to make it more random and difficult to hack

**Certificate** = A digital "briefcase" that can hold public and/or private keys

**CRL** = a list of certificates that should not be trusted / used

**Walk-through procedures** usually include a combination of inquiry, observation, inspection of relevant documentation and performance of controls. **A walk-through of the manual log review process follows the manual log review process from start to finish to gain a thorough understanding of the overall process and identify potential control weaknesses.**

**The following are potential risks WLAN**: Insufficient policies, training and awareness; constrained access; rogue WAPs; traffic eavesdropping; insufficient network performance; hacker attacks; MAC spoofing; session hijacking; and physical security deficiencies

**Rogue WAPs are WAPs** that have been installed by end users without coordinating their implementation with the information systems team. Because they are becoming a more common occurrence due to their low cost and easy installation, users can easily and inexpensively purchase an access point and place it on the network without authorization or detection.

**Rogue Users do bad things without authorization from IT Department**: Plug a wireless access point into the Ethernet jack in his office without authorization from the IT department, Disable the anti-virus software, Use another employee's account and password Use hacker tools, Install games or other "innocent" programs without authorization, Upload data or programs brought from home, Download company data to removable media and take it home to work on.

**CAAT** are used to test the operation of software. These include test data, controlled programs, integrated test facilities, program analysis, tagging and tracing, and generalized audit software programs.

**Test data** includes one example of each type of exception and is run through the company's computer programs. The auditor compares results to expected results to evaluate the processing of the data and handling of exceptions.

In a public key infrastructure, a **registration authority**: Verifies information supplied by the subject requesting a certificate

Peer-to-Peer computing = **Data leakage**

**Integrated test facility,** fictitious and real transactions are processed simultaneously using the client's system. The auditor can review the client's processing of the data to evaluate the effectiveness of the programs.

**Program analysis techniques** involve the use of software that will allow the computer to generate flowcharts of other programs. The auditor can examine the flowcharts to evaluate the effectiveness of the client's programs.

**Generalized audit software** packages test the reliability of the client's programs. These packages are used to perform many specific audit procedures. One application is parallel simulation in which the software is designed to process data in a manner that is essentially the same as that used by the client's program

Used to gain an understanding of the Organization's business processes = **Risk assessment**

Evaluating a backup solution for sensitive data that must be retained for a long period of time due to regulatory requirements = **Media reliability**

Protects against unauthorized changes to data = **Integrity**

**Preventive control** = SOD

**Discovery sampling, sample size is very small**.
- Appropriate when expected deviation rate is extremely low or zero
- Sample large enough to detect at least one error if it exists
- Any errors in sample results in rejection

**Deviation Rate:**
Calculate the sample deviation rate = # of errors in sample ÷ # of items in sample
Calculate upper deviation limit = maximum population error rate based on sample deviation rate and acceptable risk of overreliance
Upper precision limit = Sample deviation rate + Allowance for sampling risk
- If upper precision limit ≤ tolerable rate—assessed level of control risk unchanged
- If upper precision limit > tolerable rate—assessed level of control risk increased

**GANTT charts**: aid in scheduling of activities/tasks. Charts show when activities start and end and dependencies. Used for checkpoints/milestones too.

**PERT** – network management technique Shows relationships between various tasks and shows estimates/scenarios for completing tasks – three estimates shown – optimistic, most likely and pessimistic. It doesn't talk about costs.

**Time box** – project management technique for defining and deploying software deliverables within a short and fixed period of time with pre-determined resources. Must be a software baseline

**DMZ is basically a network** which you want the outside world to be able to access.

**IS Audit plan** of the organization should be based on the business risks related to use of Information Technology

**Business risk is the most important driver of the audit program**

IS Auditor must take measures to minimize the sampling risk and base the findings on the **materiality** of findings.

IS audit involves the assessment of the IS-related controls implemented by the management to ensure achievement of **control objectives**

Understanding **control objectives and identifying the key controls** are essential for the effectiveness and efficiency of the IS audit

**Under stop or go (sequential) sampling, testing discontinues when auditor acquires sufficient data**.
- Appropriate when expected deviation rate is low
- Sample selected in steps
- Each step is based on results of previous step
- No fixed sample size and may result in lower sample if few or no errors detected

**IS auditing** is the process of ensuring that the control objectives are adequately and appropriately addressed.

**Audit** must be adequately planned to achieve audit objectives within a precise scope and budget.

IS auditor must understand the **organization environment** , external and internal factors affecting the entity , entity's selection and implementation of policies and procedures, its objectives and strategies and its performance measurement to effectively identify the enterprise's key risks

**Risk analysis** does not ensure absolute safety. The purpose of using a risk-based audit strategy is to ensure that the audit adds value with meaningful information

**Qualitative Risk Analysis?**
- Complete the Risk Analysis Matrix

**Quantitative Risk Analysis?**
- Calculate the Asset Value
- Calculate the Return on Investment
- Complete the Annualized Loss Expectancy

If a sample size objective cannot be met with the given data, the IS auditor would not be able to provide assurance regarding the testing objective. In this instance, **the IS auditor should develop (with audit management approval) an alternate testing procedure**.

**A DMZ is basically a network** which you want the outside world to be able to access.

Logging = **Detection**

**The function of re-sequencing packets (segment) r**eceived out of order is taken care of by **the transport layer**. Neither the network, session or application layers address re-sequencing.

IS Audit findings must be supported by **Objective Evidence**.

Network operating system user **features include online availability of network documentation**. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands.

**Audit information** can be gathered from auditees, reference manuals, inquiry, observation, interviews, and analysis of data using CAAT's, GAS etc.

**Authorization** should be separate from all other activities (Reprocessing, Corrective, origination). A second person should review changes before implementation. Authorization will be granted if the change is warranted and the level of risk is acceptable.

The purpose of the **audit committee** is to review and challenge assurances made, and to maintain a positive working relationship with management and the auditors.

**Audit evidence** Collection, analysis, preservation and destruction = CAPD

**Audit evidence** should include information regarding original source and date of creation

Electronic evidence is dynamic so security measures should be taken to preserve its integrity. **Hashing** can be used to confirm integrity of the original evidence

**Continuous auditing** is the process by which the effectiveness and efficiency of controls is measured primarily by automated reporting processes that enable management to be aware of emerging risks or control weaknesses without the need for "regular" audits.

**Processing Control Techniques:**
**Manual recalculations** some transactions might be recalculated to ensure that processing is operating correctly.
**Editing** This program instruction controls input or processing of data to verify its validity.
**Run-to-run totals** this ensures the validity of data through various stages of processing.
**Programming controls** these software-based controls flag problems and initiate corrective action.
**Reasonableness verification** this ensures the reasonableness of data. For example, someone might try to process a negative amount through a payment system.
**Limit checks** these checks set bounds on what are reasonable amounts. For example, order 565 flat-screen TVs.
**Reconciliation of file totals:** This refers to the act of balancing debits, credits, and totals between two systems. Reconciliation should be performed periodically to verify accuracy and completeness of data.
**Exception reports** this type of report should be generated when transactions appear to be incorrect.

**IS auditor must not rely on continuous audit process when the "BUSINESS RISK IS HIGH".** Regular audits should be carried on to support and reinforce continuous auditing.

**Application control review** involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses.

**Substantive testing** is evidence gathering to evaluate the integrity of individual transactions, data

**Extreme programming (XP)—**The XP development model requires that teams includes business managers, programmers, and end users. These teams are responsible for developing useable applications in short periods of time. Issues with XP include that teams are responsible not only for coding, but also for writing the tests used to verify the code. Lack of documentation is another concern; **XP does not scale well for large projects.**

Generally, the ordering of **biometric devices** with the best response times and lowest EERs are palm, hand, iris, retina, fingerprint and voice, respectively. (PAL-HIR-FV)

**3x primary types of database structures exist:**
- Hierarchical database-management systems (HDMS)
- Network database-management systems (NDMS)
- Relational database-management systems (RDMS)

Level of compliance to internal controls is inversely proportional to amount of **substantive testing** required.

**Embedded audit module (EAM)** processes dummy transactions during the processing of genuine transactions. The intention is to determine whether the system is functioning correctly.

**Pilot test:** is used as an evaluation to verify the application's functionality.

A mature organization will have a complete suite of policies and standards, and inconsistent risk treatment is most likely to be inconsistent **compliance with standards**; very important to review compliance with standards.

Wherever possible it is advisable not to allocate **default port number** for the default application. This will make hacker's job a little more difficult. An IS Auditor must see the port allocation and feasibility.

**Confidentiality**, encrypt with receiver's public key and decrypt with receiver's private key

**Authenticity**, encrypt with sender's private key and decrypt with sender's public key

**White-box:** test Verifies inner program logic; is cost-prohibitive on a large application or system.

**Black-box:** test Integrity-based testing; looks at inputs and outputs.

**Function test** validates the program against a checklist of requirements.

**Regression test** Used after a system or software change to verify that inputs and outputs are correct.

**Sociability test** Verifies that the system can operate in its target environment

**Sampling** is done to minimize the time and cost for verification of compliance of all controls in a predefined population

**Scrum** is an iterative development method in which repetitions are referred to as sprints and typically last 30 days.

**Scrum is typically used with object-oriented technology, requires strong leadership, and requires the team to meet each day for a short time**. The idea is to move planning and directing tasks from the project manager to the team. The project manager's main task is to work on removing any obstacles from the team's path.

Sample represents a set of population members which have same characteristics as that of the population; **Sampling** may not be required if an audit software may allow testing of certain attributes across whole population.

**In a WAP gateway, the encrypted messages from customers must be decrypted to transmit to 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.

**3DES** is suitable for bulk data encryption

**Certification**: Technical testing of the system

**Accreditation**: Formal approval from the Management!

**TLS** uses the following cryptographic techniques: Asymmetric-key cryptography + Symmetric-key cryptography + Cryptographic hash functions + PKI certificates +Nonces.

**Emergency Power-off Switch** should be: clearly labeled , easily accessible, secure from unauthorized people, shielded to prevent accidental activation

Prevent dangling tuples in a database = **Relational integrity**

**Audit findings should be reported to the stakeholders** with appropriate buy-in from the auditees for the audit to be successful

**Successful resolution of the audit findings with the** auditees is essential to ensure that auditees accept the audit report recommendations and implement the corrective action.

**Token and pin** = two-factor authentication.

**Class B** = flammable or combustible liquids

The lower the **EER**, the more accurate the biometric system

**data-classification process** = Identifying the custodian

Key performance metrics = meet **SLA**

Capability Maturity Model (CMM): contains the essential elements of effective processes for one or more disciplines. It also describes an **evolutionary improvement path from ad hoc**, immature processes, to disciplined, mature processes, with improved quality and effectiveness.

The **objective of concurrency control** in a database system is to: **prevent integrity problems**, when two processes attempt to update the same data at the same time.

**CSA - Control self-assessment can be facilitated by the IS auditor to help and guide the business process owners in defining and assessing appropriate controls**.

**Process owners** are the best people to select controls as they are more knowledgeable of the process objective.

**Process and business owners evaluate and implement controls based on the risk appetite of the entity**. IS Auditor check their compliance level and risk impact.

**Management approved audit charter outlines the auditor's responsibility**, authority and accountability for the audit (internal as well as external).

**Audit charter** defines the management responsibility, objectives for and delegation of authority to the IS Audit function and outlines the entire scope of the audit activities

Approved audit charter should be changed only if it can be thoroughly justified and approved by the **senior management/BOD**.

**Audit Engagement letter** is focused on a particular audit exercise and has a specific objective. It is not as comprehensive as **Audit charter.**

**Outsourced IS audit function**, the scope and objectives should be documented in the contract or statement of work between the auditees and the auditing organization

**System administration review**: This includes security review of the operating systems, database management systems, all system administration procedures and compliance.

**Application software review**: The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed.

**Network security review**: Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.

**Business continuity review**: This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.

**Legal and regulatory requirements** will define the audit criteria and should therefore be reviewed first. The other choices support the organization's approach to adhering to the requirements

**Three authentication methods exist:**
Authentication by knowledge—what a user knows
Authentication by ownership—what a user has
Authentication by characteristic—what a person is and does

**OVERLAPPING** controls are two controls addressing the same control objective or exposure.

**Attribute sampling** is used to test compliance of transactions to controls—in this instance, the existence of appropriate approval.

**Variable sampling** is used in substantive testing situations and deals with population characteristics that vary, such as monetary values and weights.

**Stop-or-go sampling** is used when the expected occurrence rate is extremely low.

**Judgment sampling** is not relevant here. It refers to a subjective approach of determining sample size and selection criteria of elements of the sample.

Before implementing **IT BS**, an organization must define key performance indicators.

To assist an organization in planning for IT investments, the IS auditor should recommend the use of **enterprise architecture.**

**Controls** are basically to mitigate the risk.

**Ping of death**—uses an oversized IP packet.

Results in a denial-of-service attack = **Ping of death**

**Smurf**—sends a message to the broadcast of a subnet or network so that every node on the network produces one or more response packets.

**Inference engine** uses rules, also known as heuristics, to sort through the knowledge base in search of possible answers. The meaning of information in the knowledge base can be recorded in objects and symbols known as semantic networks.

**Syn flood**—manipulates the standard three-way handshake used by TCP.

**Trinoo**—Launches UDP flood attacks from various channels on a network.

**Botnets**—Botnets are another tool used for DDoS attacks. A botnet is a collection of computers hijacked during virus and worm attacks that are now under the control of a remote attacker. Botnets can be used to launch a variety of TCP and UDP flood attacks.

**IS audit services** can be provided externally or internally; the role of IS internal audit function should be established by an audit charter approved by senior management. If IS audit services are provided externally, then it should be documented in a formal contract or statement of work between the contracting organization and the service provider.

**Audit charter:** Establish the internal audit function's position within the enterprise - Authorize access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements - Define the scope of the audit function's activities

**Logical controls** are controls are technical tools used for identification, authentication, authorization, and accountability. They are software components that enforce access control measures for systems, programs, processes, and information. This would be your ACLs (Access Control Lists), Mandatory and Discretionary and Role base controls and the like.

**Engagement letter** is specifically for external parties

**Audit charter** provides guidance both to an external as well as internal party.

**AR** = IR x CR x DR

**AR** = Allowable audit risk that a material misstatement might remain undetected for the account balance and related assertions.

**IR** = Inherent risk, the risk of a material misstatement in an assertion, assuming there were no related controls.

**CR** = Control risk, the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by internal control.

**DR** = Detection risk, the risk that the auditors' procedures will fail to detect a material misstatement if it exists.

**Audit charter** is required for covering entire SDLC project say for example 'Data Warehousing project'. **Engagement letter** is required for covering **'Data Masking sensitive information'** in lower environment so that developer won't see 'the critical' information (separate activities).

**Engagement letter** is a supplementary document provided to external parties like external auditor for putting specific terms of the contract and stating independence of an auditor.

**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.

An IS auditor should expect References from other customers (an item) to be included in the **RFP** when IS is procuring services from an independent service provider (ISP).

**IT governance** ensures that an organization aligns its IT strategy with enterprise objectives.

**Legal issues** also impact organization business operations in terms of compliance with ergonomic (intended to provide optimum comfort and to avoid stress and injury, human factor) regulations, the US Health Insurance Portability and Accountability Act (HIPAA), etc.

Two-factor authentication can be circumvented through = **Man-in-the-middle**

**Audit Risk** is that material errors or fraud exists resulting in an inappropriate audit report

**Audit Risk** = Risk of material misstatement * Risk Auditor Fails to Detect Misstatements

**Audit Risk** = Inherent Risk * Control Risk * Detection Risk

**Data mining** uses rules to drill down through the data in the data warehouse for correlations. The results of data mining are stored in the data mart. The DSS presentation program may display data from the data mart in a graphical format.

**COSO: Committee of Sponsoring Organization, they provide internal Control framework**.

**An IS auditor should ensure that IT governance performance measures evaluate the activities of IT oversight committees.**

**IS strategic plans would include analysis of future business objectives.**

**Scope creep** refers to uncontrolled changes or continuous growth in a project's scope. This phenomenon can occur when the scope of a project is not properly defined, documented, or controlled. It is generally considered a negative occurrence, to be avoided.

**Firewall systems are the primary tool that enables 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 whether it is authorized or unauthorized traffic.

**A 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.**

**Scope creep** can result in a project team overrunning its original budget and schedule.

**HW Configuration Analysis is critical to the selection and acquisition of the correct operating system SW**

When conducting a review of business process reengineering, an IS auditor found that a **key preventive control had been removed.** The IS auditor **should inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.**

**STOP-OR-GO SAMPLING** is taking a sample from a population and checking after each sample item is drawn whether the sample supports a desired conclusion. Sampling ceases as soon as that conclusion is supported.

Applicable **Privacy requirements** may be a matter of law or policy and will require consideration when outsourcing processes that involve personal information.

**Data sanitization** is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data and even advanced **forensic tools** should not ever be able recover erased data.

Purchase a package instead of developing it. In this case, the design and development phases of a traditional software development life cycle (SDLC) would be replaced with **selection and configuration phases.**

**Not reporting an intrusion is equivalent to 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.

**Capacity Management** is a process used to manage information technology (IT). Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner.

**Extensive sampling** involves enough existing background data to formulate a comprehensive research design. Extensive sampling provides generalizations about large areas. For example, extensive sampling of vegetation might reveal regional patterns (e.g., pine forests, grasslands).

**Intensive sampling** provides more detail about small areas. Using vegetation as an example once again, intensive sampling would reveal individual site variations in numerous locales (e.g., details about the forest-prarie ecotone).

**Data redundancy** leads to data anomalies and corruption and generally should be avoided by design.

**Substantive testing** seeks to verify the content and integrity of evidence. Substantive tests may include complex calculations to verify account balances, perform physical inventory counts, or execute sample transactions to verify the accuracy of supporting documentation.

**Variable sampling**: Used to designate dollar value or weights (effectiveness) of an entire subject population by prorating from a smaller sample.

**Unstratified mean estimation**: Used in an attempt to project an estimated total for the whole subject population. (VAR-Sampling)

**Stratified mean estimation:** Used to calculate an average by group, similar to demographics, whereby the entire population is divided (stratified) into smaller groups based on similar characteristics. (VAR-Sampling)

**Difference estimation**: Used to determine the difference between audited and unaudited claims of value. (VAR-Sampling)

Each organization should have an **audit committee** composed of business executives. Each audit committee member is required to be financially literate, with the ability to read and understand financial statements. The purpose of the audit committee is to provide advice to the executive accounting officer concerning internal control strategies, priorities, and assurances.

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 redundancy of data.**

**Resilience** - The ability to recover quickly from illness, change, or misfortune; buoyancy.

An IS auditor evaluating the **resilience** of a high-availability network should be MOST concerned if the network servers are clustered

A **service-level agreement (SLA)** is a part of a service contract where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service or performance).

When **archive bit** is set to zero, it indicates that the files have been backed up, while an archive bit set to one means it has not been backed up. Remember that both incremental and full backup set the achieve bit to zero when the backup completes, which means when you take a full or incremental backup, your files will have archive bits set to zero.

**Differential backup** keep the archive bit unchanged after taking a backup.

When reviewing a **service level agreement SLA** for an outsourced computer center, an IS auditor should FIRST determine that the services in the agreement are based on an analysis of business needs.

An IS auditor should recommend the use of **library control software** to provide reasonable assurance that program changes have been authorized.

**Integrity** ensures that transactions are accurate but does not provide the identification of the customer.

**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 2 or below.
**Digital signatures** = validates the source of a message.

**ITF: there is a need to isolate test data from production data.** An IS auditor is not required to use production data or a test data generator**. Production master files should not be updated with test data.**

**Blackout - Generator**

**Brownout - Uninterrupted power supply (UPS)**

**Surge - Surge protector**

**Spike - Surge protector**

**Noise = Power conditioner**

**The recovery point objective (RPO)** defines how current the data must be or how much data an organization can afford to lose. The greater the RPO, the more tolerant the process is to interruption.

**The recovery time objective (RTO)** specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored.

**Three-factor authentication,** which involves possession of a physical token and a password, used in conjunction with biometric data, such as finger scanning or a voiceprint.

**Social engineering**, in the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information, this is a type of confidence trick for the purpose of information gathering, fraud, or gaining computer system access.

**Security awareness training** is the most effective way to reduce social engineering incidents.

Ensure that the databases are appropriately secured: **Look for Database Initialization Parameters**

In order to effectively audit a database implementation, the IS auditor must examine the database **initialization parameters**.

**Digital signatures** are used for authentication and non-repudiation, and are not commonly used in databases.

**PKI**= control for an Internet business looking for confidentiality, reliability and integrity of data

**Nonce** is defined as a "parameter that changes over time" and is similar to a number generated to authenticate one specific user session.

**Nonce**s are not related to database security; they are commonly used in encryption schemes.

**Challenge response-based authentication** is prone to **session hijacking** or man-in-the-middle attacks.

**CA** is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with an RA to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

**Sniffing**: to gather information without actually touching it (or being detected or in hiding), e.g., network packet sniffing. Sniffing is "listening" to network traffic to collect information. A common usage of sniffing is to listen to network traffic to look for patterns of a worm spreading itself.

**Spoofing**: mimic mirroring something and create an illusion of the presence of the original, e.g., email spoofing. Spoofing is sending network traffic that's pretending to come from someone else, a common usage for spoofing is sending an email message.

**IT steering committee** provides open communication of business objectives for IT to support. The steering committee builds awareness and facilitates user cooperation. Focus is placed on fulfillment of the business objectives.

**Network security reviews** include reviewing router access control lists, port scanning, internal and external connections

**Public key encryption**, asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

**Symmetric key encryption requires that the keys be distributed**. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore**, use less processing power** than asymmetric techniques, thus making it ideal for **encrypting a large volume of data.**

Nontechnical attack attempts to lure the victim into giving up financial data, credit card numbers, or other types of account information = **Phishing**

**A digital signature** contains a message digest to show if the message has been altered after transmission.

The use of **hash totals** is an effective method to reliably detect errors in data processing. A hash total would indicate an error in data integrity.

The best control to mitigate the risk of **pharming** attacks to an Internet banking application is **Domain name system (DNS) server** security hardening.

**Pharming** is an attacker's attack intended to redirect a website's traffic to another, bogus site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

**Application-level gateway** is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is or is not permitted.

The role of the **board of directors** is to provide strategic direction and impetus as well as to monitor the risk profile of the company.

**Proxy servers** can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program.

If **cloud vendor** is providing development platform it comes under PAAS; if vendor is giving you storage server it comes under IAAS infrastructure as a service; if cloud vendor is giving you access or services of one or more application software it comes under SAAS software as a service

An **information security policy must be holistic**. It is not just a technical document requiring input mainly from information security professionals. Business and other units need to contribute to its development and maintenance. In this role the board ensures that management has the authority to address, and is addressing, risk.

**A system downtime log** provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

**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.

**VPN is a mature technology**; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network.

The first thing an IS auditor should do after detecting the **virus** is to alert the organization to its presence, then wait for their response.

**Measuring IT performance** is a dynamic process

DB **normalization** minimizes duplication of data through standardization of the database table layout = Increased Speed

**Encapsulation, or tunneling**, is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly (VPNs)

**An IS auditor's role** is to detect and document findings and control deficiencies. Part of the audit report is to explain the reasoning behind the findings.

**The use of shared IDs is not recommended because it does not allow for accountability of transactions**. An IS auditor has no proof that a privacy breach has occurred as a result of the shared IDs.

**False Acceptance Rate** or false match rate **(FAR or FMR)**: the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

**False Rejection Rate or false non-match rate (FRR or FNMR**): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

**A low EER is the measure of the more effective biometrics control device.**

**Session hijacking Attack**: method that allows an attacker to overtake and control a communication session between two systems.

**The BEST overall quantitative measure of the performance of biometric control devices is EER.**

**ITAF** = **General, Performance and Reporting.**

**SBC:** Provide security features for VoIP traffic similar to that provided by firewalls. Scope Notes: SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.

**Honey-pot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. Honey-pots acts as a decoy to detect active internet attack.

**Inherent risk:** it is a probability of risk because of an existing situation, considering that there is no compensation controls. For instance, money is more likely to be stolen than power generators. These types of risks are independent of audit.

**Cost performance** of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected.

**Remember that audit risks are not the same as statistical sampling risks. Sampling risk is selecting the incorrect samples.**

**A background screening is the primary method for assuring the integrity of a prospective staff member.**

**Traffic analysis** is the process of intercepting and examining messages in order to deduce information from patterns in communication.

**Social Engineering** Criminals can trick an individual into cooperating by using a technique known as social engineering. The social engineer will fraudulently present themselves as a person of authority or someone in need of assistance.

Not knowing how much **disk space is in use and therefore how much is needed at the disaster recovery** site could create major issues in the case of a disaster.

In the absence of adequate segregation of duties, good **audit trails** may be an acceptable compensating control

**The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted** before the disruption threatens the achievement of organizational objectives.

**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.

**Client-server environment**: most serious is Password controls are not administered over the client-server environment.

**Substantive testing** obtains audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.

**Direct observation of results is better than estimations and qualitative information gained from interviews or status reports**. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

**White box testing assesses the effectiveness of software program logic**.

**Compliance testing** is evidence gathering for the purpose of testing an enterprise's compliance with control procedures. This differs from substantive testing in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.

**Analytical testing** evaluates the relationship of two sets of data and discerns inconsistencies in the relationship.

**Control testing** is the same as compliance testing.

**System's risk ranking** = Critical + Vital + Sensitive + Non-sensitive

**Software for centralized tracking and monitoring would allow a USB usage policy** to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management.

A validity check helps to **evaluate the password verification process** because it checks if the required format is being used in the password.

**Controls** to detect threats to equipment include: Temperature sensors, humidity sensors, water detectors, and smoke detectors

**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.

**Identification of the priority for recovering critical business processes** should be addressed first in **BCP process**.

During an audit, an auditor discovers that the same person is responsible for both IT and accounting. The review of computer log showing individual transaction would work as the **best compensating control** in this situation.

**Tracing** involves following the transaction from the original source through to its final destination.

**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; **could prevent out-of-range data.**

**Logging all table update transactions and implementing before-and-after image reporting are detective controls** that would not avoid the situation.

**SaaS** refers to a business application delivered over the Internet in which users interact with the application through a web browser. SaaS applications are designed with a significant degree of network and device independence. SaaS is most commonly used by individuals, small- to mid-sized businesses and departments within larger enterprises.

**Tracing and tagging** are used to test application systems and controls and **could not prevent out-of-range data.**

The main objective of an auditor discussing the audit findings with the auditee is to confirm the accuracy of the findings, and to decide on the **corrective actions required to fix the vulnerabilities.**

During an audit, if an auditor finds out **that user account ID of a website is being shared**, he should **document the finding** in his report, explaining the risk of using shared IDs.

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and **include additional substantive tests**.

**A reboot in the system can destroy all the evidence** of a compromised computer.

**The main purpose of forensic audit is to systematically collect digital evidence to use in judicial proceedings.**

When an IS auditor evaluate data mining and audit software that he want to utilize in his audit, he should **ensure that this audit software tool maintains data integrity and do not modify the system or its source code.**

**Different BIA approaches**: Questionnaire + Interview key users + Work group

The benefits of using **Data Dictionary/Directory System** include:

- Enhancing documentation
- Providing common validation criteria
- Facilitating programming by reducing needs for data definition
- Standardizing programming methods

The BEST control to mitigate the risk of unauthorized manipulation of data is to provide access to the utility on a **need-to-use basis**.

**Secure Shell (SSH)** is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively

**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.

MOST appropriate to ensure the confidentiality of transactions initiated via the Internet is **PKI.**

In the event of a data center disaster, the MOST appropriate strategy **to enable complete recovery of a critical database** is Real-time replication to a remote site.

**Defining a security policy for information and related technology is the first step toward building security architecture**. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization.

Testing (BCP) = **identify limitations of the BCP**.

**Reconciliation**: Supervisor should review that *all* data was properly recorded and processed

| | | |
|---|---|---|
| Data Sanitization = **Erasing/Over-Writing** | (Re-Use) Yes | No (Media Destroyed) |
| Data Sanitization = **Degaussing** | (Re-Use) Probably Not | Yes (Media Destroyed) |
| Data Sanitization = **Physical Destruction** | (Re-Use) No | Yes (Media Destroyed) |

**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

**Cross-training**, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations

**Traditional EDI** include: 1. Communications handler 2. EDI interface 3. Application system

**If the changes are reviewed by the authors of the application there are less likely to be unwanted errors** or side effects caused by improper or incomplete modifications. The analysts have a better understanding of the application they developed.

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.

**Digital signatures** are enabled by using the sender's private key. The CA binds the identity of the public key with the sender's private key to enable the identification of the sender.

**CSA:** can identify high-risk areas that might need a detailed review later.

**Outsourcing:** different countries if a service provider outsources part of its services to another service provider, there is **a potential risk that the confidentiality of the information will be compromised.**

**CSA** does not allow management to relinquish its responsibility for control

**Walk-through costs** are not a part of disaster recovery.

The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a **substantive test** that directly addresses the risk of unauthorized code changes.

The **backup device** and media must be chosen based on a variety of factors: Standardization, Capacity, Speed and Price

**To prevent software license violations**: Centralizing control and automated distribution and installation of software, Regularly scanning user PCs, either from the LAN or directly, Installing metering software on the LAN and requiring that all PCs to access applications through the metered software

**SOD**: is the concept of having more than one person required to complete a task, in business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

**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, while the security plan should be at a corporate level.

**Prototype systems** can provide significant time and cost savings; however, they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated, and it often leads to functions or extras being added to the system that were not originally intended.

**SOD:** Custody, Authorization, Record keeping, Reconciliation

**Compensating Controls** for Lack of Segregation of Duties would include: Audit trails, Reconciliation, Exception reporting, Transaction logs, Supervisory reviews, Independent reviews.

**Reconciliation**: is used to ensure that the money leaving an account matches the actual money spent, this is done by making sure the balances match at the end of particular accounting period.

**Hybrid sourcing agreement** with most help center staffing located overseas.

**An independent third-party audit report** such as an SSAE 16 would provide assurance of the existence and effectiveness of internal controls at the third party.

**Audit risk: the risk that an auditor will accept**

**Control Risk:** the risk that might not be detected by a system of internal controls

**Business risk:** the risk that will affect the business's functional goals

**Continuity risk: the risk the business faces that it might not be able to recover from a disaster**

**Detection risk: the risk that an improper test is performed that will not detect a material error**

**Material risk:** an unacceptable risk

**Network administrator cannot be combined** with: control group, application programmer, help desk/support manager, end user, data entry, computer operator, database

**Inherent risk**: the risk of a material misstatement in the unaudited information assumed in the **absence of internal control** procedures

**Data Control Group** Responsible for: Checking all data, Validity of input, Accuracy of output, Control Manual

**Due care** can be equated to doing the right thing and **due diligence** to ensuring that due care actions are effective

**Security risk** — the risk that unauthorized access to data will result in the exposure or loss of integrity of the data

**Attribute sampling**: Attribute sampling is used primarily for compliance testing. It records deviations by measuring the rate of occurrence that a sample has a certain attribute.

**Variable sampling**: Variable sampling is used primarily for substantive testing. It measures characteristics of the sample population, such as dollar amounts or other units of measurement.

**Capacity management** is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. **Business criticality** must be considered before recommending a disk mirroring solution and offsite storage is unrelated to the problem. Though data compression may save disk space, it could affect system performance.

**Audit charter**: A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity. The charter should: Establish the internal audit function's position within the enterprise; Authorize access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements; define the scope of audit function's activities.

**Digital signatures provide integrity** because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

In **top-down policy** development, policies are pushed down from the top of the company. The advantage of a top-down policy development approach is that it ensures that policy is aligned with the strategy of the company. What it lacks is speed; this process requires a substantial amount of time to implement.

**Bottom-up policy** development addresses the concerns of operational employees: It starts with their input and concerns, and builds on known risk. This is faster than a top-down approach, but it does not always map well with high-level strategy.

**Capability Maturity Model CMM** – Initial this is an ad-hoc process with no assurance of repeatability. - Repeatable Change control and quality assurance are in place and controlled by management, although a formal process is not defined. - Defined process and procedures are in place and used. Qualitative process improvement is in place. - Managed Qualitative data is collected and analyzed. A process-improvement program is used. - Optimized Continuous process improvement is in place and has been budgeted for.

**Emergency changes**; because management cannot always be available when a system failure occurs, it is acceptable for changes to be reviewed and approved within a reasonable time period after they occur.

**Data flow diagrams** are used as aids to graph or chart data flow and storage. They trace the data from its origination to estination, 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.

Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. **Data mapping** deals with automatic integration of data in the receiving company.

**The best control would** be provided by having the production control group copy the source program to the production libraries and then compile the program.

The design of a **honeypot** is such that it lures the hacker and provides clues as to the hacker's methods and strategies and the resources required to address such attacks. A bastion host does not provide information about an attack. IDSs and intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.

**SCARF** works using predetermined exceptions. The constituents of "exceptions" have to be defined for the software to trap. GAS is a data analytic tool that does not require preset information. The integrated test facility tests the processing of the data and cannot be used to monitor real-time transactions. Snapshots take pictures of information observed in the execution of program logic.

**Audit charter** outlines the overall authority, scope and responsibilities of the IS audit function.

**Detailed Staff training plan** should be drawn for the year and should be reviewed semi-annually to ensure that training needs are aligned to the direction that the audit organization is taking.

**Short term audit planning** takes into account audit issues that will be covered during the year

**Long term audit planning** relates to plans that take into account risk related issues regarding changes in the organization's IT strategic direction that will affect the organization's IT environment

**Analysis of short and long term issues** should occur annually and the results of this analysis to be reviewed by senior management approved by the audit committee

**Risk assessment by management**, privacy issues and regulatory requirements may impact overall approach to audit.
IS auditor must gain an understanding of the **business's mission**, objectives, purpose and process to perform audit planning. Steps to gain understanding of the business include touring key organization facilities

**Risk analysis** is a part of audit planning and it helps identify risks and vulnerabilities so the auditor can determine the controls needed to mitigate those risks

**IS auditor** is most focused toward high risk issues associated with the confidentiality, availability or integrity of sensitive and critical information and the underlying information systems and processes that generate, store and manipulate such information.

**Risk management process** is an iterative cycle beginning with identifying business objectives, information assets, and the underlying systems or information resources that generate/store use or manipulate the assets critical to achieving these objectives Once critical assets are identified, **risk assessment** is performed to identify risks and determine the probability of occurrence and the resulting impact and additional safeguards that would mitigate this impact to a level acceptable to management.

**Internal controls** are developed to provide reasonable assurance that an organization's business objectives will be achieved and undesired risk events will be prevented, detected and corrected.

**Internal accounting controls** – primarily directed at accounting operations-safeguarding assets and reliability of financial records

**Operational controls** – directed at day-to-day operations, functions and activities to ensure operation is meeting business objectives

ID Info Assets -> **Risk Assessment** -> identify vulnerability and threats and determine the probability of occurrence.

**Payment Card Industry (PCI) Data Security Standard (DSS)** is a mandatory compliance standard for all acquiring organizations; e-commerce sites; retailers; and any organization that collects processes or stores credit card information.

Granting database administrator access to business owners is a blatant violation of **SOD**.

**Administrative controls** – concerned with operational efficiency in a functional area and adherence to management policies including operational controls. They support operational controls

**Preventive Control**: Detect problem before they arise. Monitor inputs; prevent an error, omission etc.

**Operational audit** – evaluate internal control structure in a given process or area

**Integrated audits** – combines financial and operational audit steps

IS Auditor should review the following **documents**: IT strategies, plans and budgets- Security policy documentation Organization/functional charts - Job descriptions - Steering committee reports - System development and program change procedures - Operations procedures - HR manual - QA procedures

**Utility programs** can be categorized by use, into functional areas: Understanding application systems - Assessing or testing data quality - Testing a program's ability to function correctly - Assisting in faster program development - Improving operational efficiency

**Utilities** should be well controlled and restricted

**Forensic audit**: Audit specializing in discovering, disclosing and following up on frauds and crimes; Electronic evidence is vulnerable to changes. Hence Chain of custody for evidence should be established to meet legal requirements. The most important consideration for forensic auditor is to make a bit stream image of the target drive and examine that image without altering date stamps or other information attributable to the examined files.

Acting as an **audit trail** for electronic data interchange (EDI) transactions, **functional acknowledgments** are one of the **main controls used in data mapping.**

**Audit Risks**: Inherent risk – Risk that an error exists that could be material which when combined with other errors assuming that there are no compensating controls. E. g. complex calculations are more likely to be misstated than simple ones and cash is more likely to be stolen than inventory of coal. They exist independent of audit and can occur because of the nature of the business.

**Control Risk**: Risk that a material error exists that cannot be prevented or detected in a timely manner by the internal control system. E.g. Control risk with manual reviews of computer logs are high whereas computerized validation procedures are low.

**Detection risk**: The risk that an IS auditor uses inadequate test procedure and concludes that errors do not exist when in fact they do.

**Triggers** will record logon activities of specified users and their attempts to make changes to database objects in an audit trail.

The Risk assessment of counter measures should be performed through **cost-benefit analysis** where controls to mitigate risks are selected to reduce risks to a level acceptable to management.

**Monetary policy** is the process by which the monetary authority of a currency controls the supply of money

**Compliance test** Evidence gathering for the purpose of testing organization's compliance with control procedures. It tests the existence and effectiveness of a defined process which may include a trail of documentary and/or automated evidence.

**Substantive tests**: Evidence gathering to evaluate the integrity of individual transactions, data or other information. It substantiates integrity of actual processing. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support these balances.

**Substantive test** tests for monetary errors directly affecting financial statement balance

**Compliance test** – test a sample of programs to determine if the source and object versions are the same,

**Substantive test** – using a thorough inventory or a statistical sample to determine if the tape library inventory records

Performing **a walk-through** of the process/procedure allows the IS auditor to gain evidence of compliance and observe deviations, if any. Reporting relationships should be observed to ensure that assigned responsibilities and segregation of duties are being practiced.

**After reviewing the disaster recovery planning (DRP) process of an organization**, the goal of the meeting is to confirm the **factual accuracy** of the audit findings and present an opportunity for management to agree on corrective action.

**Statistical sampling** – Objective method – quantitatively decides how closely the sample should represent the population (assessing sample precision) and the number of times in 100 the sample should represent the population (reliability of confidence level). Permits IS auditor to quantify the probability of error (Confidence co-efficient)

**Non statistical or Judgmental sampling** – Depends on sample size and sample selection. These are subjective judgment as to which items/transactions are the most material and most risky.

The MOST important consideration would be to ensure that the contract contains: a **right-to-audit clause**.

**Trapdoor**: usually a hidden access technique left in the software by the developer for future use by their technical support staff.

**Document the finding and explain the risk of using shared IDs.**

**Statistical sampling** – Attribute Sampling (Used in Compliance testing)

**Attribute sampling** (Fixed size attribute sampling or frequency estimating sampling) Used to estimate the rate of occurrence of a specific quality in a population. E.g. testing approval signatures of computer access request forms

**Statistical sampling** – Stop-or-go sampling – (Compliance test) Helps prevent excessive sampling by allowing an audit test to be stopped at the earliest possible moment. It is used when the auditor believes that relatively few errors will be found in a population

**Statistical sampling:** Discovery sampling – (Compliance test) used when the expected **occurrence rate is extremely low**. Often used to seek out => Discover fraud

**Variable sampling** (Dollar estimation or mean estimation sampling) used for **substantive test**. This is a technique used to estimate the monetary value or some other unit of measure such as weight of a population from a sample. E.g. review of **balance sheet for material transactions** and an application review of program that produced the balance sheet

**Cycle** = Risk Assessment + Risk Mitigation + Risk reevaluation

**Capacity management** is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively.

**Risk in IT Projects** = Market Risk - Financial Risk - Technology Risk - People Risk - Structure Risk

**Difference estimation** – estimate the total difference between audited values and book values based on differences obtained from sample observations.

**Sample mean**: measures the average size of sample.

**Sample standard deviation** – variance of sample values from the mean. Measures the spread or dispersion of the sample values

**Tolerable error rate:** Maximum number of Misstatements or errors that can exist without an account being materially misstated. It is used for planned upper limit of the precision range for compliance testing. Expressed as a %

**Population standard deviation:** Mathematical concept that measures the relationship to the normal distribution; greater the standard deviation, the larger the sample. This is applied to variable sampling and not attributes sampling.

A check file of a fixed length created by a source file of any length; the purpose is to indicate whether the source file may have been changed **(Message hash)**

**CAATs** provide a means to gain access and analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system.

**2x authentication** = SMART CARD = ATM Card

**Example of two-factor authentication**; however, a magnetic card is **much easier to copy than** a smart card so the use of a smart card with a PIN is better.

**GAS Generalized audit software supports** File access – enables reading of different formats and file structure // File reorganization –enables indexing, sorting, merging and linking with another file Data selection – enable global filtration conditions and selection criteria // Statistical functions – enables sampling, stratification and frequency analysis
Arithmetical functions – enables arithmetic operations and functions.

**Expert system** – query based system built on the knowledge of senior auditors.

**The scope of an IS audit is defined by its objectives**. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them.

Traditional perimeter protection and access control are **NOT** as effective at blocking attacks from inside organizations as they are at blocking external hackers

**CAATs** are used for tests of detailed transactions and balances, analytical procedures, compliance tests of IS general controls, compliance tests of IS application controls and penetration and OS vulnerability assessment testing.

**Audit universe** is all auditable areas within the company, after risk assessment, choose the one with high risks depending on resources.

With **real-time replication** to a remote site, data are updated simultaneously in two separate locations; therefore, a disaster in one site would not damage the information located in the remote site. This assumes that both sites were not affected by the same disaster.

Monitoring audits and initiating cost controls will **not necessarily ensure the effective use of audit resources**.

A SaaS provider does not normally have onsite support for the organization. **Therefore, incident handling procedures between the organization and its provider are critical for the detection**, communication and resolution of incidents, including effective lines of communication and escalation processes.

It is a generally agreed upon standard in the computer industry that expensive IT equipment should not be operated in a computer room or data center where the ambient room temperature has exceeded **85°F (30°C)**.

**Compensating control** – A detailed manual balancing process over all transaction is a compensating control over weakness in a system transaction error report. Strong staging and job set up procedures are compensating controls for a weakness in a tape management system where some parameters are set to bypass or ignore labels written on tape header records.

**Change management** can't Change the design

**Acknowledgments** indicate the status of EDI message transmission.

**Big-bang** is where the new or changed service is deployed to all user areas in one operation

**Phased** is where the service is deployed to a part of the user base initially and this operation is repeated for subsequent parts of the user base,

**Pull** is where the software is available in a central location but users are free to download the software at a time of their choosing.

**Typical type of metrics**: Technology metrics, Service metrics, Process metrics

The goal **of Problem Management** is: To prevent Problems and resulting incidents from happening.

In the **Service Level Management process**: Collate, measure and improve customer satisfaction

**CSA** helps process owners assess the control environment and educates them on control design and monitoring. The sampling of transaction logs is a valid audit technique; however, risk may exist that is not captured in the transaction log and there may be a potential time lag in the analysis. (**Continuous auditing with large volume**)

**Flow Chart**: Shows HOW PROCESSES INTERRELATE.

**Governance** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; monitoring performance and compliance against agreed-n direction and objectives.

**COBIT** = separating governance from management + Enable holistic approach + applying single integrated Framework, covering enterprise end-to-end, meeting stakeholder needs

**Significant indicators** of potential problems include: Unfavorable end-user attitudes - Excessive costs - Budget overruns - Late projects - High staff mover - Inexperienced staff - Frequent HW /SW errors - An excessive backlog of user requests - Slow computer response time - Numerous aborted or suspended development projects - Unsupported or unauthorized HW /SW purchases - Frequent HW /SW upgrades - Extensive exception reports - Exception reports that were not followed up - Poor motivation - Lack of succession plans - A reliance on one or two key personnel - Lack of adequate training -

Line capacity; **A peak traffic load of 96 percent is approaching a critical level**, and the auditor should not assume that capacity is adequate at this time or for the foreseeable future**; Further investigation is required**.

**Attribute sampling is the method used for compliance testing**. In this scenario, the operation of a control is being evaluated, and therefore the attribute of whether each purchase order was correctly authorized would be used to determine compliance with the control.

**Unstratified mean per unit** is used in variable sampling.

**Performing an exhaustive** review of the recovery tasks would be appropriate to identify the way these tasks were performed, identify the time allocated to each of the steps required to accomplish recovery, and **determine where adjustments can be made**.

Assurance of achieving **confidentiality, message integrity and nonrepudiation** by either sender or recipient, the recipient uses the sender's public key, verified with a certificate authority, to decrypt the pre hash code.

**Risk assessment** should be performed to determine how internal audit resources should be allocated in order to ensure that all material items will be addressed.

**Risk assessments** form the basis of audit department management and are used to determine potential areas on which to focus audit efforts and resources**. A risk assessment is the process used to identify and evaluate risk and its potential effects**.
**Histogram (Column Chart):** It shows HOW OFTEN something occurs, or it's FREQUENCY (no Ranking).

**CSAs** require employees to assess the control stature of their own function. CSAs help increase the understanding of business risk and internal controls. Because they are conducted more frequently than audits, **CSAs help identify risk in a more timely manner.**

**An IS audit charter establishes the role of the information systems audit function**. The charter should describe the overall authority, scope and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee.

**The audit committee** is a subgroup of the board of directors. The audit department should report to the audit committee and the **audit charter** should be approved by the committee.

**Balance scorecard** in a simple example If I want to check the performance of any organization I should check the: financial statement and operations, because if the financial revenue is high while operation is bad, so there is something wrong. The two factors financial and not financial measures the elements of performance
The IS auditor should develop an **audit plan** that takes into consideration the objectives of the auditee relevant to the audit area and its technology infrastructure.

**CONTROLS** = what should be achieved + what should be avoided

A **Technical Acknowledgment** generated as a result of header validation. The technical acknowledgment reports the status of the processing of an interchange header and trailer by the address receiver.

A **Functional Acknowledgment** generated as a result of body validation. The functional acknowledgment reports each error encountered while processing the received document.

**Risk Analysis help IS Auditor** = identify risk + evaluate of controls + support risk based audit decisions

**IS strategy** is that it must support the business objectives of the organization

**Tape Library:** This is an example of substantive sampling which confirms the integrity of a process. This test will determine whether tape library records are stated in a correct manner.

**The objective of risk based audit** approach is focus on areas where risk is high. Various scheduling methods are used to prepare audit schedules and it does not come under risk based approach. It also does not relate to budget requirements met by staff and number of audits performed in a given year.

Ensure integrity of new staff = **Background screening**

Assessment through **configuration management tools** is insufficient as they tend to assess the configuration of an individual device in isolation from other devices

**Require supervision of audit staff** to accomplish audit objectives and comply with competence, professional proficiency and documentation requirements, and more.

**The extent to which data** will be collected during an IS audit is related directly to the purpose, objective and scope of the audit.

An IS auditor should **expect References from other customers** to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP).

To sharpen the details of an average population by using a stratified mean (such as demographics) to further define the data into small units **(Defuzzification)**

For large organizations with officers in various location it is not practical to **organize workshops**, In this case a hybrid approach is needed. A questionnaire is issued which is analyzed, evaluated and readjustment of questionnaire **is performed using life cycle approach**.

**Participating in the design of the risk management framework involves designing controls, which will compromise the independence of the IS auditor to audit the risk management process**. Advising on different implementation techniques will not compromise the auditor's independence because the IS auditor will not be involved in the decision-making process. Facilitating awareness training will not hamper the IS auditor's independence because the auditor will not be involved in the decision-making process. Due diligence reviews is a type of audit

**Integrated auditing**: typically involves identification of relevant key controls. Focused on risk Benefit is that this approach assists in staff development and retention by providing greater variety and the ability to see how all the elements mesh together to form a complete picture.

CV = EV – AC If Cost Variance is positive, this means you are **under budget**.
CV = EV – AC If Cost Variance is negative, this means you are **over budget**.
CV = EV – AC If Cost Variance is zero, this means you are **on budget**.

The use of **continuous auditing techniques** can improve system security when used in time-sharing environments that process a large number of transactions.

**Continuous auditing**: Distinctive character of continuous auditing is the short time lapse between the facts to be audited and the collection of evidence and audit reporting; requires a high degree of automation.

**Continuous monitoring:** IDS, real-time, anti-virus etc.

The **Pareto Principle** states that, for many phenomena, 80 percent of effects or consequences come from 20 percent of the causes. (80 co / 20 ca)

When both continuous monitoring and auditing take place**, continuous assurance can be established**

**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

**Generalized audit software GAS** will facilitate reviewing the entire inventory file to look for those items that meet the selection criteria. GAS provides direct access to data and provides for features of computation, stratification, etc.

**ITF integrated test** facility allows the IS auditor to test transactions through the production system.

**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.

**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.

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.**

**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**.

**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.

Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve **confidentiality, message integrity and nonrepudiation** by either sender or recipient.

**RBAC** = this is a normal process to allow the application to communicate with the database. Therefore, the best control is to control access to the application and procedures to ensure that access to data is granted based on a user's role

**Encryption**: the recipient uses the sender's public key to decrypt the digital signature and obtain the hash of the message, which would prove message source and integrity. A single, secret key is used to encrypt the message because secret key encryption requires less processing power than using public and private keys.

**Preventive** = Qualified personal, SOD, ACL, Procedures, Complete program edit checks, encryption

**Detective** = Hash totals, Check points, Echo Control, Error messages, Duplicate checking, Past-due, Review logs

**Corrective** = BCP, Backup, Rerun Procedures

**WBS does not help identify dependencies**

**Detective** = use controls that detect and report the occurrence of an error, omission or malicious act

**Corrective** = Minimize the impact of threat, identify cause of problem

**IT governance** is about effectiveness

**A digital certificate,** signed by a certificate authority, validates senders' and recipients' public keys.

The recipient uses the sender's public key, verified with a certificate authority, to **decrypt the hash code**.

**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.

**Generalized audit software** involves the use of auditor programs, client data, and auditor hardware. The primary advantage of GAS is that the client data can be down-loaded into the auditor's system and manipulated in a variety of ways

**Authentication systems** may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

Inadequate software baseline = **Scope creep**.

**Control objectives relate to** = Effectiveness Efficiency Confidentiality Integrity Availability Compliance Reliability

**HIGHEST risk SSL Self-signed digital certificates** are not signed by a certificate authority (CA) and can be created by anyone. Thus, they can be used by attackers to impersonate a web site, which may lead to data theft or perpetrate a man-in-the-middle attack.

**BCP**: is a system or methodology used to create a plan on how an organization will resume its partially or completely interrupted critical functions within a predetermined time after the occurrence of a disaster or disruption. The aim is to keep critical functions operational.

**COBIT** is the leading framework for governance, control and assurance for information and related technology

**Masking** preserves the type and length of structured data, replacing it with an inert, worthless value. Because the masked data look and act like the original, they can be read by users and processes.

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address = **Address Resolution Protocol**

**Continuous monitoring is a responsibility of IT management and cannot be handed over to the internal audit team.**

**Continuous auditing** is a function of the audit team and is not a substitute for continuous monitoring. Moreover, the internal audit team cannot assume that their scripts are being used appropriately by IT management or that their scripts have not been modified, which then could give erroneous results. **Simply reducing the audit scope** and frequency in areas where continuous monitoring is used does not imply risk-based auditing and is inappropriate.

A key factor in a **successful outsourcing** environment is the capability of the vendor to face a contingency and continue to support the organization's processing requirements.

**BIA** goal is to distinguish which are the most crucial and require to continue operations if a disaster occurs

**Standards** set the allowable boundaries for technologies, procedures and practices and thus are the appropriate documentation to define compliance requirements.

**RPO:** The RPO defines how current the data must be or how much data an organization can afford to lose. The greater the RPO, the more tolerant the process is to interruption.

**RTO:** The RTO specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored

**Dumpster diving**: The process of digging through trash to recover evidence or improperly disposed-of records. The same process is frequently used by government agents and law enforcement to gather evidence; therefore, it's completely legal unless the person is trespassing.

**Non statistical sampling** = does not provide a quantitative measure/expression, sample may not be effective.

**Statistical sampling** = expensive time consuming, requires software

**Bit-stream backups**, also referred to as **mirror image backups**, involve the backup of all areas of a computer hard disk drive or other type of storage media. Such backups exactly replicate all sectors on a given storage device including all files and ambient data storage areas.

A standardized reference listing of all the programmer's data descriptions and files used in a computer program, **Data dictionary**

**Accountability**: the ability to map a given activity or event back to the responsible party.

**Decision trees** use questionnaires to lead a user through a series of choices until a conclusion is reached.

**Cross certification enables entities in one public key infrastructure (PKI) to trust entities in another PKI**. This mutual trust relationship is typically supported by a cross-certification agreement between the certification authorities (CAs) in each PKI.

**AES** replaced 3DES.

**Multiplexing Data** include: TDM ATDM FDM Statistical

MPLS is independent of any routing protocol and can be used for **unicast packets**

A formal statement of policy signed by management and acknowledged by the user with their signature. Normally this policy is enforced by the HR department. This policy should state that computer use is for company business only and that non-company activities, including those related to religion or topics of questionable use, are prohibited; **Acceptable use policy (AUP)**

**Accreditation**, formal approval by management to accept all the responsibilities and consequences for a system to be used in production for a **period of 90 days, 180 days, or 365 days** (annual)

**Engagement Letter**: addresses the independence of the auditor.

Low voltage for an extended period of time = **Brownout**

Network firewall is usually the simplest to configure but has the worst logging capabilities **= A packet-filtering network firewall (gen 1)**

A new generation of software or a design change resulting in a new version. Releases tend to occur in 12- to 24-month intervals, **Major software release**

**Version usage:** helps in assurance that correct file is being used, **Version control helps in controlling unauthorized changes** to the document.

**UPS** is a backup power system that utilizes batteries to provide short-term power when a power losses such as a black out or a brownout is detected.

**UPS** protection from Black + Broun OUT

The IT steering committee provides open communication of business objectives for IT to support. The steering committee builds awareness and facilitates user cooperation. **Focus is placed on fulfillment of the business objectives**.

**Power conditioner** devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.

**Surge protectors** are passive devices that are used to **protect electrical components from spikes in the power line.** Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground

**Generator** is used when a continuous power supply is needed in power loss situations and is activated when a loss in power is detected. It does not protect electrical components from spikes in the power line.

**An engagement letter** states the scope and objectives, which has been agreed by both the auditor and the auditee.

**Compliance test** on change management process will reveal that whether any unauthorized modification was made to data or programs.

**Control risk** can be high, but it would be due to internal controls not being identified, evaluated or tested, and would not be due to the number of users or business areas affected.

**Compliance risk** is the penalty applied to current and future earnings for nonconformance to laws and regulations, and may not be impacted by the number of users and business areas affected.

**Inherent risk** is normally high due to the number of users and business areas that may be affected. Inherent risk is the risk level or exposure without taking into account the actions that management has taken or might take.

**Residual risk** is the remaining risk after management has implemented a risk response, and is not based on the number of user or business areas affected.

**Continuous monitoring** IDS, AV

**Data federation technology**, also called data virtualization technology or data federation services, is software that provides an organization with the ability to collect data from disparate sources and aggregate it in a virtual database where it can be used for business intelligence (BI) or other analysis.

**Continuous auditing** It is a methodology that an IS auditor uses to give written assurance, which may be a series of reports, on a specific subject. The IS auditor provides these reports either when a specific event occurs or after a short time of the occurrence of that event.

**Continuous assurance** = CM + CA

**Tokenization** is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. Tokenization, which seeks to minimize the amount of data a business needs to keep on hand, has become a popular way for small and mid-sized businesses to bolster the security of credit card and e-commerce transactions while minimizing the cost and complexity of compliance with industry standards and government regulations.

**The prerequisites for the success of continuous auditing depends** on the presence of automation and reliable automated process, alarms to notify control failures, automated audit tools for IS auditors, informing the IS auditor about system anomalies or errors, quick issuance of audit report, technical competency of auditors, reliable evidence, strictly following materiality guidelines, evaluation of cost factors.

The **mandatory examination procedures** to be executed during an audit to ensure consistency of findings; any deviations must be well documented, with justification as to why the procedures were not followed **(Auditing standard)**

**Assymetric encryption**: cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.

**Audit charter** describes the role of IS audit function. It also must specify the authority, responsibilities and scope of the audit function.

**Audit charter** need to be approved by the top management and the audit committee.

**Attack Signature**: Specific sequence of events indicative of an unauthorized access attempt; typically a characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities.

**Before formally closing a review**, an IS auditor needs to meet the auditee to get agreement on his findings.

The list of objectives, tasks in sequence, skills matrix, written procedures, written test procedures, and forecast illustrating scope, time, and cost estimates = **Audit plan**

**CPS** is a formal document outlining the issuer's certificate policy and enforcement policy.

**Timebox management**, by its nature, sets specific time and cost boundaries. It is effective in controlling costs and delivery time lines by ensuring that each segment of the project is divided into small controllable time frames.

**Timebox management** integrates system and user acceptance testing.

An encryption system using two different keys; Both keys are mathematically related. This type of encryption is not time sensitive. The private key is kept totally secret by the sender, and their public key is freely distributed to anyone who desires to communicate with the owner**. (Asymmetric encryption, also known as public-key cryptography)**

Matching the combined security of subject (user or program), object (data), and context of usage (need or purpose) to determine whether the request should be approved or denied **(Attribute-based access control (ABAC))**

An affirmation by the signer that all statements are true and correct; the purpose is to certify that a declaration is genuine (**Attestation**)

An access control system based on rules that require the user to have an explicit level of access that matches the appropriate security label. The only way to increase access is by a formal promotion of the user ID to the next security level **(Mandatory access control (MAC))**

This occurs in biometrics when the system is calibrated to favor either speed or increased accuracy => **Crossover error rate (CER)**

A fire-suppression system with water stored in the pipes at all times; this type of system is susceptible to corrosion and freezing **(Wet pipe system)**

**Throughput** is the quantity of useful work made by the system per unit of time. In telecommunications, it is the number of bytes per second that are passing through a channel.

The process of physically marking insecure wireless access points to the Internet **War chalking.**

**Capability Maturity Model (CMM):** Developed by the Software Engineering Institute to benchmark the maturity of systems and management processes. Maturity levels range from 0 to 5. Level 5 removes any authority from the workers, completely documented and optimized for continuous improvement.

**Data federation** (also known as data virtualization) is a process whereby data is collected from distinct databases without ever copying or transferring the original data itself.

**If a password is displayed on a monitor**, any person or camera nearby could look over the shoulder of the user to obtain the password. (**shoulder Surfing**)

**Digital signature** is represented in a computer as a string of bits.

**The effect of applicable statutory requirements must be factored in while planning an IS audit**—the IS auditor has no options in this respect because there can be no limitation of scope in respect to statutory requirements.

**Statutory requirements always take priority over corporate standards**.

**Industry best practices** help plan an audit; however, best practices are not mandatory and can be deviated from to meet organization objectives.

The most critical requirement is that the **audit tool does not compromise data integrity** or make changes to the systems being audited

**Data sanitization method** is the specific way in which a data destruction program or file shredder overwrites the data on a hard drive or other storage device.

**Organizational policies and procedures are important, but statutory requirements always take priority.**

**Qualitative Risk Analysis**: use of subjectivity in describing likelihood and impact of risk

**Owner of the information asset** should be the person with the decision making power in the department deriving the most benefit from the asset.

**Protocol analyzer:** is typically hardware-based and operate at the data link and/or network level

**ISO** as part of its communications modeling effort has defined basic tasks related to network management (5x):

When an IS auditor uses a source code comparison to examine source program changes without information from IS personnel, the IS auditor has an objective, independent and relatively complete assurance of program changes because the **source code comparison will identify the changes.**

**Digital signature** is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified

**Digital signatures** may be generated on both stored and transmitted data.

**Signature generation uses a private key to generate a digital signature**; signature verification uses a public key that corresponds to, but is not the same as, the private key.

**The RPO is the earliest point in time to which it is acceptable to recover the data.** If backups are not performed frequently enough to meet the new RPO, a risk is created that the company will not have adequate backup data in the event of a disaster. This is the most significant risk because, **without availability of the necessary data, all other DR considerations are not useful.**

**Problem management** is trying to determine the root cause of the incident; **Incident management** is focused on increasing the continuity, returning the business to its normal operation as quickly as possible.

**Post implementation review**; review of the system after it is placed in operation to determine whether it fulfilled its original objectives.

**If the BCP is tested regularly**, the BCP and disaster recovery plan (DRP) team is adequately aware of the process and that helps in structured disaster recovery.

**A digital signature is an electronic identification of a person or entity**. It is created by using asymmetric encryption. To verify integrity of data, the sender uses a cryptographic hashing algorithm against the entire message to create a message digest to be sent along with the message. **Upon receipt of the message, the receiver will recomputed the hash using the same algorithm.**

**CA** issues certificates that link the public key with its owner. The CA does not compute digests of the messages to be communicated between the sender and receiver.

The purpose of the **Post Project Review (PPR)** is to review the completed project and find lessons learnt on what went well and what could be done better.

The purpose of the **Post Implementation Review (PIR)** is to ensure that the project meets the intended business requirements. PIR should be scheduled some time after the solution has been deployed; Typical periods (6 weeks - 6 months) depending on the type of solution and its environment.

**Substantive test** includes gathering evidence to evaluate the integrity

**Outsourcing environment** provider's performance should be monitored to ensure that services are delivered as required.

**Digital signature**, the message digest is computed: by both the sender and the receiver.

**Transferring risk** insurance policy is a way to share risk.

**Tolerating risk** means that the risk is accepted, but not shared.

During a post implementation review of an enterprise resource management system, an IS auditor would MOST likely: **review access control configuration.**

In circumstances in which the IS auditor's independence is **impaired and the IS auditor continues to be associated with the audit**, the facts surrounding the issue of the IS auditor's independence should be disclosed to the appropriate management and in the report.

The predecessor to SSL is Transport Layer Security **TLS**

**Collusion between employees** is an active attack where users collaborate to bypass controls such as separation of duties. Such breaches may be difficult to identify because even well-thought-out application controls may be circumvented.

**Agile**= Post iteration reviews that identify lessons learned for future use in the project.

**Preventive:** IPS

**Detective:** hash, checkpoints, echo, error messages, internal audit, performance log etc.

**Corrective:** contingency, planning, backup, rerun procedures etc.

**Compliance tests**: user access right to the system, change control procedures of programs, documentation procedures, reviewing logs, checking software license etc.

**Substantive tests**: performance of interest calculation in a sample account.

**Sampling**: is used when the verification of all data is not possible or feasible due to time and cost constraints. Sampling helps to infer characteristics of the total data in a population, based on sample analysis.

**Statistical sampling** uses law of probabilities to determine the sample size, to select samples, to evaluate sample results.

**Non-statistical sampling** uses subjective judgment to determine sample size

**Detection risk** the risk audit procedures will lead to a conclusion that material error does not exist when in fact such error does exist.

**Detective control** a control designed to discover an unintended event or result.

**Deviation** is departure from prescribed internal control. Often expressed as a rate at which the departure occurs.

**Attribute sampling** used in compliance testing; expressed in rates

**Variable sampling** used in substantive testing; expressed in deviation from the normal value

**Integrated Auditing** is a process that combine multiple audit disciplines (IS controls, financial control etc.) to assess or evaluate primary controls of a process, an operation or an organization. **Risk is the primary focus on integrated audit** approach.

**Attribute sampling**: this is also called fixed-sample size attribute sampling. They express the percent of occurrence of a specific attribute in a population. It figures out the occurrence of an attribute or quality in numbers (e.g. how many times).For instance, you can use sampling to check the **presence of signatures or approval on database access** request forms.

**Stop or go-sampling**: when an auditor assumes the presence of relatively few errors in a population, he uses this sampling method. An auditor takes a sample and checks it to find his expected value. The audit stops whenever a desired value is found in the sample. It saves auditor's time by not taking too many samples of a given attribute.

**Discovery sampling**: it is used when the expected occurrence of a particular attribute or incident is very rare → **discover frauds** r

Attack attempts that could not be recognized by the firewall will be detected if a network-based intrusion detection system (**IDS) is placed between the firewall and the organization's network.**

**CRL:** list of revoked and expired certificates issued by the certificate authority (CA).

**Embezzlement** to take assets in violation of trust.

Plan Audit -> Obtain Understanding of Client and Its Environment Including Internal Control -> Assess Risks of Misstatement and Design Further Tests -> Perform Substantive Procedures -> Complete the Audit ->**Issue Audit Report**

A database of information derived from the knowledge of individuals who perform the related tasks. Used in decision support systems **(Knowledge base)**

A type of audit that reviews the internal control used in daily operation = **Operational audit**

**4GL** provides screen-authoring and report-writing utilities that automate database access.

**4GL tools** do not create the business logic necessary for data transformation.

Type of test, the data used for rerunning the test scenario is the same as the original data => **Regression testing**

**Caveat** = warning or caution.

**Check digit** = redundant digit added to a code to check accuracy of other characters in the code.

**Limit test/check**: A computer program step that compares data with predetermined limits as a reasonableness test (hours worked over 60 per week).

**Enterprise Risk Management** (ERM) identifies risks and opportunities, assesses them for likelihood and magnitude, determines responses strategy, and monitors progress. ERM integrates strategic planning, operations management, and internal control. Monitoring ERM is part of internal control activities.

**IPsec** = Transport mode + Tunnel mode

**Time-sharing**: A technique that allows more than one individual to use a computer at the same time.

**Required vacations/holidays** of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place.

**Recovery managers should be rotated** to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

Errors in data processing can be effectively detected with **hash totals**.

**ITF integrated test facility** can create fictitious data in the database to test the transaction process capability while the database in the production mode. Therefore, if you use integrated testing facility you do not have to setup separate test process. However, **you have to be careful that the test data do not mix up with the production data.**

An IS auditor should **report all his reportable findings** in his final report including those that have been corrected by the auditee immediately after the identification during the audit period. If the finding is corrected before the audit ends, the auditor should mention about the corrective action in his report.

**Neural networks can be used to attack problems that require consideration of numerous input variables**; they are capable of capturing relationships and patterns often missed by other statistical methods. Neural networks will not discover new trends. They are inherently non-linear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

**Risk assessment** always expects to identify the vulnerabilities and the threats.

**CMM** creates a baseline reference to chart current progress or regression. It provides a guideline for developing the maturity of systems and management procedures.

If there is **any disagreement about the impact of an audit finding between the auditor and the auditee**, then the auditor should explain the risks and the potential exposures to the auditee. An auditee may lack the required knowledge and understanding to realize the seriousness of a threat or risk.

**If the auditee disagrees with the impact of a finding**, it is important for an IS auditor to elaborate and clarify the risks and exposure since the auditee may not fully appreciate the magnitude of the exposure. When the auditee expresses an alternative view, the auditor should not agree with him, but he should communicate maintaining his professional code of conduct.

**CSA** transferring some control monitoring responsibilities to the line managers.

**Success of CSA depends much on how the line managers handle their control monitoring responsibility**.

**The audit hook is the most effective online audit monitoring** technique used for early detection of irregularities and errors.

**Addressing the audit objectives** is the primary goal of an IS auditor during the planning phase of an audit.

**Substantive test** always verifies the integrity of the system or application. Checking the balances of a financial statement is an example of substantive test.

**DRM** prevents users from converting purchased products to alternate formats that might be more convenient for playback.

**Digital Rights Management**: system for authorizing the viewing or playback of copyrighted material on a user's computer or digital music player. DRM has centered around copyrighted music, with Apple's FairPlay and Microsoft's Windows Digital Rights Manager being the two predominant DRM systems. As broadband Internet and more highly compressed video formats take hold, the focus of DRM broadens to video content.

The selection of audit procedures **affects the detection risk**. A faulty audit procedure may not identify the detection risk. That is why an IS auditor's decision can directly affect the detection risk.

When an IS auditor discover the presence of authorized access requests that has not been authorized by the proper authority such as managers, he needs to conduct further analysis and **substantive test** to determine why the normal authorization process did not work. Before making any decision, an auditor should understand the context of the incident and collect sufficient evidence to support his action.

**Concurrent use license**: software license that is based on the number of simultaneous users accessing the program. It typically deals with software running in the server where users connect via the network. For example, in a five-user concurrent use license, after five users are logged on to the program, the sixth user is prohibited. When any one of the first five log out, the next person can log in. Concurrent licensing can be managed by the application itself or via independent software metering tools.

The main reason for applying **data masking** to a data field is to protect data from external exposure.

It identifies the source and verifies the integrity of data = **DS**

Establish accountability and responsibility of the processing of information or transaction = **audit trail**.

Identifying the high-risk areas is the most critical steps in **audit planning**.

**The threats and vulnerabilities affecting the IT resources** should be reviewed first when an IS auditor evaluate management's risk assessment of information system.

**During the audit phase**, if an IS auditor discover that there is no documented security procedures in the organization, then he should try to identify and evaluate the security practices that the organization follow.

Audit's scope and purpose determines to what extent data will be collected as **audit evidence**.

The main objective of forensic software is to **preserve digital evidence**.

**Attribute sampling** can estimate the rate of occurrence of a specific attribute of quality in a population. That is why **attribute sampling is used in compliance testing**.

When there is not enough sample or data to draw from the population to make any assurance about the test objective, an IS auditor need to find an **alternative approach of testing.**

**Observing and taking interviews** IS auditor can get the best evidence about the SOD in organization

After review of any plan such **as business continuity plan**, an IS auditor need to call a meeting with the management to agree on the facts of his findings and to give them an opportunity to agree on the correction action.

An IS auditor considers a report from an **external auditor more reliable** than a confirmation letter to a third party. A confirmation letter does not follow any audit standards and is likely to be subjective.

**Reporting the suspected incident** to management will help initiate the incident response process, which is the most appropriate action. **Management is responsible for making decisions regarding the appropriate response.**

The best way to determine the accuracy of a computing system is to make some simulated transaction and test the **result with pre-determined results.**

**Developing audit plan based on risk assessment** is the first step to ensure that audit resources deliver the highest value to the organization. That is why a risk assessment is performed during the planning phase of an audit to give reasonable assurance that the audit will cover all the material items.

**Conducting a physical count of tape inventory** = substantive test.

Acceptance sampling is sampling to determine whether internal control compliance is greater than or less than the **tolerable deviation rate.**

When the probability of errors need to be identified objectively, an IS auditor should **use statistical sampling, not the judgmental/non-statistical sampling**

If an IS auditor finds that the interview answers of a financial personal do not match with the job description for the role, then he should conduct **further testing with substantive test.**

At the pre-audit phase, an IS auditor performs functional **walkthrough in order understand the business processes**.

**Automated code comparison** will reveal the presence of unauthorized changes in program since the last authorized program changes and update.

**Test data** runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program.

**Script kiddies** are hackers who do not necessarily have the skill to carry out specific attacks without the tools provided for them on the Internet and through friends. Since these people do not necessarily understand how the attacks are actually carried out, they most likely do not understand the extent of damage they can cause

**Code review** is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

**"Due care"** implies reasonable care and competence, not infallibility or extraordinary performance.

- The conduct of examinations and verifications to a reasonable extent
- The reasonable assurance that compliance does exist
- The consideration of the possibility of material irregularities

If the IS auditor executes the data extraction, there is **greater assurance that the extraction criteria** will not interfere with the required completeness and therefore all required data will be collected. Asking IT to extract the data may expose the risk of filtering out exceptions that should be seen by the auditor. (**Auditor is extracting the data**)

An IS auditor always need to gather appropriate and **sufficient evidence** in order to provide a strong base for his conclusion on the audit findings.

**Conversation and interviews** provides the best evidence that segregation of duties SOD exist in an organization.

**Testing of users rights provides incomplete information** about the function they perform in their job role

Determining that only authorized modifications are made to production programs would require the **change management process** be reviewed to evaluate the existence of a trail of documentary evidence.

**Compliance testing** would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs.

**Forensic analysis** is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

In a meeting that takes place after conducting an audit on disaster recovery plan, the **IS auditor should confirm the accuracy of his findings with the management.**

**Before submitting the audit report**, an auditor should ensure if the audit has sufficient evidence to support the findings.

**Generalized audit software(GAS)** is best suited to conduct overpayment audits because GAS has the ability to run statistical analysis, duplicate checking, sequencing, computation and various types of mathematical computation.

When an IS auditor needs to run further testing before gaining enough assurance in his audit, but cannot run the test due to limited time frame of the audit, he should highlight this in his report. Besides, a **follow-up testing date should be scheduled and mentioned in the report.**

**Replacing a manual monitoring process with automated monitoring system** can reveal the presence of overlapping key controls in application systems

**Assessing the risk of the information systems**, the key factor that an IS auditor should, at first, review vulnerabilities and threats that may affect the IS assets.

**Compliance testing** determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized.

**Assertion** is a statement that enables you to test your assumptions about your program. For example, if you write a method that calculates the speed of a particle, you might assert that the calculated speed is less than the speed of light.

**Detective Control:** IDS, SEIM, honeypots, Pen testing, Virus detection, vulnerability scanning, Log review, audits, compliance review, CCTV

**Corrective Control:** Backup/restore, Load-balancing, DRP, BCP, Incidence response plans Security guard.

**Preventive Control:** Firewalls, Access controls, user access rights, IPS, PKI, PGP, encryption, security baselines, info security architecture, content filtering, data encryption, restricted drive allocation, antivirus, VPN, Logon banner warnings, security awareness tuning, policies, procedures, contracts, Locks

**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.

**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.

**Two-factor authentication** is a method of user authentication that uses something you know (your account and password), and something that you have (physical token, or hardware with virtual token).

**Wire transfer procedures** include segregation of duties controls. This helps prevent internal fraud by not allowing one person to initiate, approve and send a wire. Therefore, the IS auditor should review the procedures as they relate to the wire system.

**Fraud monitoring** is a detective control; does not prevent financial loss.

**SOD** = preventive control

**Attribute sampling** is the method used for compliance testing. In this scenario, the operation of control is being evaluated, and therefore attribute sampling should be used to determine whether the purchase orders have been approved.

**Variable sampling** is the method used for substantive testing, which involves testing transactions for quantitative aspects such as monetary values.

**The lack of adequate controls represents vulnerability**, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information, financial loss, legal penalties or other losses.

A registration authority (RA) is an entity that is trusted by the certificate authority (CA) to register or vouch for the identity of users to a CA and is a **component of PKI**.

**Trend/variance detection tools** look for anomalies in user or system behavior, such as invoices with increasing invoice numbers. CASE tools are used to assist in software development. Embedded (audit) data collection software, such as systems control audit review file (SCARF) or systems audit review file (SARF), is used to provide sampling and production statistics, but not to conduct an audit log analysis. **Heuristic scanning tools are a type of virus scanning used to indicate possible infected codes.**

**Stratified mean per unit and unratified mean per unit are used in variable sampling**.

**Protecting life always takes precedence above all else.**

**Locks and keys are the most inexpensive access-controls devices**. Preset locks (padlock), Chipper locks (Programmable combination locks) and Device locks (Cable locks).

**Discovery sampling** is used when an auditor is trying to determine whether a type of event has occurred, and therefore it is suited to **assess the risk of fraud**

**Deadman Doors = prevent piggybacking**.

**Dead-man door** is a double door that requires an individual to pass through a secured area before entering the facility.

The **approved audit charter** outlines the auditor's responsibility, authority and accountability

Authenticates an individual's identity by a unique personal attribute; **Biometric** is quite advanced and is very sensitive. This sensitivity can make biometrics prone to error.

**False Rejection Rate (FRR) Type I Error**: Biometric system rejects an authorized individual.

**False Acceptance Rate (FAR) Type II Error**: Biometric system accepts imposter who should be rejected. An accuracy measure for a biometric system is FAR.

**FAR** is the most important consideration when evaluating biometric access control effectives.

**Iris Scan**- Reads the unique characteristics of the iris (colored portion).

**Fingerprint scanner** provides the highest degree of physical access control in terms of authentication.

During the review of a biometrics system operation, the IS auditor should first review the stage of **ENROLLMENT**.

The use of residual biometric information to gain unauthorized access is an example of a **REPLAY ATTACK**.

The information security policy should state "each individual must have their badge read at every controlled door" to address the threat of **PIGGYBACKING**.

**Facilitated workshops** work well within business units
**Data scrubbing** is an activity in which faulty data is removed from a database. Data can be described as faulty if it is imprecise, unfinished, incorrectly structured, or is a duplicate. Companies who frequently work with digital information will scrub or cleanse their data periodically, using data scrubbing software that verifies data and then corrects flaws by altering or deleting certain elements of faulty data.

The **CSA program** can be implemented by various methods. For small business units within organizations, it can be implemented by facilitated workshops

**Memory Card**: no processing capability (ATM cards); **Smart Card**: includes processing capability.

**Discovery sampling** is used when an auditor is trying to determine whether a type of event has occurred, assess risk of Fraud

**Provides two factor authentication** since user must enter a PIN to get a token.

**Escorting visitors** is the most EFFECTIVE control over visitor access to a data center.

**Input authorization verifies** that all transactions have been authorized and approved by management.

The **executive steering committee** should be involved in software decisions to provide guidance toward fulfillment of the organizational objectives.

In **smaller organizations**, it generally is not appropriate to hire additional staff to achieve a strict segregation of duties. Therefore, IS auditor must look at alternatives

Detects suspicious traffic or users, and generates alarms accordingly: **Security management**

**HASH TOTALS**: Verification that the total in a batch agrees with the total calculated by the system.

**Batch balancing** can be performed through manual or automated reconciliation.

**Revalidate the supporting evidence for the finding**.

**Preventive controls** that are used in a program before data are processed.

**Procedures** should be established to ensure that input data are validated and edited as close to the time and point of origination as possible.

**Batch Totals** To compare input against actual processing.

**Run-to-Run Totals:** To provide verification of the data values during the different stages of processing. This helps ensure the completeness of all transactions.

**Request for information (RFI)** is used when the client wants input to see what is available and does not want to give vendors the expectation of any commitment to purchase.

**RFP** indicates that the buyer intends to purchase something from a vendor. Eligible vendors can expect an opportunity to make a sale.

**Limit Checks:** To prevent processing of any amount in excess of the expected average. Overly large transactions will not be processed. For example, no employee should receive a paycheck for $50,000. That amount would obviously be excessive outside of executive positions.

**Encrypting the pre-hash code using the sender's private key** provides assurance of the authenticity of the message. Mathematically deriving the pre-hash code provides integrity to the message. Encrypting the pre-hash code and the message using the secret key provides confidentiality.

**ITF**: Periodic testing does not require separate test processes.

**User Management**: should review and approve system deliverables as they are defined and accomplished to ensure the successful completion and implementation of a new business system application.

**User management** should review and approve system deliverables as they are defined and implemented.

Greatest assurance of achieving confidentiality, message integrity and non-repudiation by either the sender or recipient; **The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.**

To ensure confidentiality, authentication, and integrity of a message, the sender should encrypt the hash of the message with the: **sender's Private key and then encrypt the message with the receiver's public key.**

**Exception Reporting:** To identify errors. The exception may hold the batch in suspension until the errors are corrected, or reject individual transactions containing errors, or reject the entire batch of transactions.

**A validity check** would be the most useful for the verification of passwords because it would verify that the required format has been used—for example, not using a dictionary word, including non-alphabetical characters, etc. An effective password must have several different types of characters.

**Sequence check:** The control number follows sequentially and ANY SEQUENCE (out of order o range)OR DUPLICATED controls numbers ARE REJECTED OR NOTED ON AN EXCEPTION REPORT for follow-up purposes. A sequence number and time stamp will help verify that the instruction was not duplicated when transmitting a payment instruction.

**Limit check:** Data should not exceed a predetermined amount. If it exceeds the predetermined amount, the data would be REJECTED for further verification/authorization.

**Range check:** Data should be within a predetermined range of values. Example: Range from 1 - 100. Any code outside this range should be REJECTED as an invalid product type.

**Validity check:** Programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for marital status and the **acceptable status codes are M or S**. If any other code is entered, the record should be REJECTED.

**Reasonableness check:** Input data are matched to predetermined reasonable limits or occurrence rates. If the limit is different, then computer program should be designed**; TO PRINT THE RECORD WITH A WARNING INDICATING THAT THE ORDER APPEARS UNREASONABLE.**

**Table lookups:** Input data comply with predetermined criteria maintained in a computerized table of possible values.

**Existence check:** Data are entered correctly and agree with **valid predetermined criteria**. For example, a valid transaction code must be entered in the transaction code field.

**Key verification:** The keying process is repeated by a separate individual using a machine that compares the original keystrokes to the repeated keyed input. Helps assure quality of input trying to reduce errors.

**Check digit**: A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect, but valid, substituted. This control is effective in detecting TRANSPOSITION AND TRANSCRIPTION.

**Completeness check:** A field should always contain data rather than zeros or blank. A check of each byte of that field should be performed to determine that some form of data not blanks or zeros, is present.

**Logical relationship check**: If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid.

**Sending and reconciling transaction** counts and totals helps ensure that all orders transmitted to production are received and processed.

**Run to run totals:** Provide the ability to verify data values through the stages of application processing.

**Automated systems balancing**: Helps ensure that transactions are not lost during processing.

**Exception reports:** An exception report is generated by a program that identifies transactions or data that appear to be incorrect. These items may be outside a predetermined range or may not conform to specified criteria.

The greatest **risk when end users have to access to a database at its system level**, instead of through the application, is that the users can make unauthorized changes to the database directly, without an audit trail. Lack of synchronization between interrelated databases poses a great risk to data completeness.

**Atomicity:** Evaluating data integrity in a transaction-driven system environment; determine whether a transaction is completed or a database is updated. If 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, the auditor know that the processing feature of ATOMICITY has been violated.

**Consistency** - Ensures that all integrity conditions in the database be maintained with each transaction.

**Isolation** - Ensures that each transaction is isolated from other transactions, 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.

**Data Integrity Testing:** Examines the accuracy, completeness consistency and authorization of data.

**Data integrity tests will indicate failures in input or processing controls.**

**Redundancy check**: detects transmission errors by appending calculated bits onto the end of each segment of data.

**Domain integrity**: test can be used to bear out the effectiveness of edit and validation routines.

**Relational integrity testing**: detects modification to sensitive data by the use of CONTROL TOTALS.

**Foreign key** Data in the database is stored in separate tables to improve speed. A foreign key is the link between data in different database tables. When the links are valid, the database has referential integrity.

**Referential integrity** CHECK DATABASE INTEGREITY

**Referential integrity** constraint ensures that data are updated through triggers.

An IS auditor should review the FOREIGN KEYS to evaluate the **referential integrity of a database**.
**Corruption of the foreign keys** in a relational database can cause errors when transactions are processed since critical associations with master data may have been lost.

**Referential integrity:** means a valid link exists between data in different tables.

The new product should have **quality assurance**, and a formal **certification process**. Only then will it go through **accreditation** and **acceptance.**

Firewalls are an example of rule-based access. Active Directory user profiles are a form of role-based access. These controls are called **Non-Discretionary controls**.

**RPO** is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

Quite simply, **non-discretionary access controls** are ones that are not at the discretion of the user. They are global rules, they apply to mostly everyone, so don't feel bad : )

The **service delivery objective (SDO)** is directly related to the business needs. The SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.

**The Audit Program:** Includes: Scope, audit objectives, audit procedures, Administrative details such as planning and reporting Preliminary Review of Audit Area/Subject, Evaluating Audit Area/Subject, Gather Evidence.

The audit report contains the audit findings. The content and structure of the report are defined according to the type of audit. **The IS auditor must ensure that sufficient evidence is collected before concluding on the findings.**

**Sufficiency of evidence is a subjective decision** based upon on auditor's professional judgment. The extent to which data will be collected during an IS audit should be determined based on the purpose and scope of the audit being done. **Techniques**: Review IS organization structures, interview appropriate personnel, Observe processes and employee performance, Review IS policies, procedures, and standards

**Updated and flawless access list** is a significant challenge in Firewall and, therefore, has the greatest chance for errors at the time of the initial installation.

**Attribute Sampling:** used by IT auditors; is the primary sampling method used for compliance testing.

**Variable sampling**: used by financial auditors

**Statistical sampling**: Objective quantification of errors and risk

**Non-statistical sampling**: Relies on subjective judgment.

**Sampling Risk**: The risk that incorrect assumptions are made about a population a sample is selected from.

**Substantive testing** substantiates the integrity of actual processing, which provides evidence of the validity of the final outcome; sampling the statistical details of a control, rather the control's ability to fully satisfy a control objective.

**Asymmetric Key**: RSA / GAMAl / ECC

**Public key ensures**: Authentication / Confidentiality and Non-repudiation (Accountability); **Much higher overhead than symmetric** encryption;

**Asymmetric encryption** key is a cryptography option that would increase overhead/cost; Intensive calculation

**PKI:** Provides access control, authentication, confidentiality, non-repudiation, and integrity for exchange of messages

**Prior to implementing new technology**, an organization should perform a risk assessment, which would then be presented to business unit management for review and acceptance.

The **change management process**, which would include procedures regarding implementing changes during production hours, helps to ensure that this type of event does not recur. An IS auditor should review the change management process, including patch management procedures, to verify that the process has adequate controls and to make suggestions accordingly.

**The PKI element:** that manages the certificate life cycle, including certificate directory maintenance and certificate revocation list (CRL) maintenance and publication.

The role of **certificate authority (CA)** as a third party is to confirm the identity of the entity owning a certificate issued by that CA.

**Digital Certificates**: Associates a public key with a collection of components that can be used to authenticate the owner of the public key. **The purpose is to associate the public key with the individual's identity**.

**Certification Revocation list (CRL)**: Checks the continued validity of the certificates for which the CA has responsibility. The CRL details Digital Certificates that are no longer valid because they were revoked by the CA.

**Certification practice statement** - is a PKI element that provides detailed descriptions for dealing with a compromised private key.

**Registration Authority** (Sometimes separate from the CA): Managers the certificate life cycle, including the certificate directory maintenance and certification revocation list.

**Digital Signatures:** It is an encrypted hash value of a message.

**Hashing:** One-Way Function - The most important difference between hashing and encryption is that hashing is irreversible. Output of the hash function is called a message digest; Hash is computed over the entire message;

**Types of hash**: MD4 / MD5 / MD2 / SHA / SHA-1 / HAVAL

**Web of trust** is a key distribution method suitable for communication in a small group. It is used by tools such as pretty good privacy (PGP) and distributes the public keys of users within a group.

**Kerberos Authentication System** extends the function of a key distribution center by generating "tickets" to define the facilities on networked machines, which are accessible to each user.

**RAID 0** = Striping with no parity = this is no truly a fault tolerance solution. This is primarily for high performance of read / writes operations.

**RAID 1** = Mirroring = this provides fault tolerance

**RAID 3** = Striping of Data with parity on one drive**.**

**RAID 5** = Striping with Parity striped across all drivers.

**The PRIMARY purpose of implementing RAID level 1 in a file server is to ensure availability of data.**

**Implementing data mirroring as a recovery strategy is appropriate if the recovery point objective (RPO) is low.**

**Installing a level 1 RAID system in all servers do not compensate for the elimination of offsite backups.**

**Network Attached Storage (NAS)**

- ✓ Integrates one or more storage devices, (NAS appliances) into the local area network (LAN).
- ✓ Comprised of one or more disk drives and an internal controller.
- ✓ Employs Raid technology to ensure hardware redundancy.
- ✓ Can be shared by multiple users on the network.
- ✓ Network Data Management Protocol (NDMP) technology should be used for backup if a NAS appliance is required.

**Storage Area Network (SAN)**

- ✓ Expands SAN to wide area networks (WAN). SAN replication
- ✓ SAN is a dedicated network.
- ✓ Multiple SANs can be simultaneously utilized.
- ✓ SAN can be expensive and technically complicated.
- ✓ Capable of handling very high volumes.
- ✓ SAN is a great solution for large companies.
- ✓ SAN is designed to be very fault tolerant.

**Identification and classification of information resource**: How important are these assets? How much are they worth? What damage could be caused if they were inappropriately accessed?

**Assess risks and vulnerabilities** associated with the information resource and the likelihood of their occurrence.

**Key components for performing risk analysis** are vulnerabilities and threats.

Vulnerabilities result from inadequate security controls; when evaluating management's risk assessment of information systems, the IS auditor should first review the **threats/vulnerabilities affecting the assets.**

A poor choice of passwords and data transmission over unprotected communications lines are examples of vulnerabilities

**Assessing IT risks** is best achieved by evaluating threats associated with existing IT assets and IT projects.

**Qualitative analysis methods:**

- ✓ Use word or descriptive rankings to describe the impacts or likelihood.
- ✓ They are the simplest and most frequently used methods.
- ✓ Based on checklists and subjective risk ratings such as high, medium or low.
- ✓ If the impact of a risk cannot be effectively projected in quantifiable terms, management should apply qualitative risk assessment.

**Semi quantitative Analysis methods:** Descriptive rankings are associated with a numeric scale; such methods are frequently used when it is not possible to utilize a quantitative method or to reduce subjectivity in qualitative methods.

**Quantitative analysis methods**: Uses numeric values to describe the likelihood and impacts of risks, using data from several types of sources such as historic records past experiences, industry practices and records, statistical theories, testing, and experiments. **Reduce risk** to a tolerable level through implementation of controls (countermeasures to threats).

Look at existing controls can be evaluated or new controls designed to reduce the vulnerabilities to an acceptable level of risk. Controls that should be considered are: **Preventive, detective or corrective, manual or automated and formal** (i.e., documented in a procedure manuals and evidence of their operation is maintained).

**The basis for an expert system** is the capture and recording of the knowledge and experience of individuals in an organization. This will allow other users to access information formerly held only by experts.

**Risk can be:** Avoid, Mitigate, Transfer, Accept

**An organization may choose to REJECT risk by ignoring it**, which can be dangerous and should be considered a red flag by the IS auditor.

**Protecting human life is the primary objective of BCP and DRP.**

Following the identification of and classification of informational assets, **the next step in preparing a BCP is to prepare a BIA.**

**The primary purpose of a BIA** is to identify the events that could impact the continuity of organizations operations.

**BIA Collection Methods**: Critical Success Factor Analysis, KPI, business and information process flows, business and information process flows, activity categorization, desk review of documentation, questionnaires, interview and workshops.

**IT governance** is primarily the responsibility of the executives and shareholders (as represented by the board of directors).

**Critical**: Functions are those that cannot be performed unless they are REPLACED BY IDENTICAL CAPABILITIES and CANNOT BE REPLACED BY MANUAL METHODS.

**Vital**: Functions refer to those that CAN BE PERFORMED MANUALLY but only for a brief period of time; this is associated with lower costs of disruption than critical functions.

**Sensitive:** These functions CAN BE PERFORMED MANUALLY, AT A TOLARABLE COST and FOR AN EXTENDED PERIOD OF TIME. While they can be performed manually, it usually is a difficult process and requires additional staff to perform.

**Nonsensitive/Non critical :** Functions may be interrupted for an extended period of time at little or no cost to the company, and require little or no catching up when restored.

**IT BSC** represents the translation of the business objectives into what IT needs to do to achieve these objectives.

**Preventative - "stops":** Administrative Hiring procedures, background checks, segregation of duties, training, change control process, acceptable use policy (AUP), organizational charts, job descriptions, written procedures, business contracts, laws and regulations, risk management, project management, service-level agreements (SLAs), system documentation Technical Data backups, virus scanners, designated redundant high-availability system ready for failover (HA standby), encryption, access control lists (ACLs), system certification process Physical Access control, locked doors, fences, property tags, security guards, live monitoring of CCTV, human readable labels, warning signs.

**Corrective - "fixes":** Termination procedures (friendly/unfriendly), business continuity and disaster recovery plans, outsourcing, insourcing, implementing recommendations of prior audit, lessons learned, property and casualty insurance, Data restoration from backup, high-availability system failover to redundant system (HA failover occurs), redundant network routing, file repair utilities, Hot-warm-cold sites for disaster recovery, fire-control, sprinklers, heating and AC, humidity control

**Detective "finds":** Auditing, system logs, mandatory vacation periods, exception reporting, run-to-run totals, check numbers, control self-assessment (CSA), risk assessment, oral, testimony, Intrusion detection system (IDS), high-availability systems detecting or signaling system failover condition, (HA failure detection), automated log readers, (CAAT), checksum, verification of digital signatures, biometrics for identification (many search), CCTV, used for logging, network scanners, computer forensics, diagnostic utilities, Broken glass, physical inventory count, alarm system, (burglar, smoke, water, temperature, fire), tamper, seals, fingerprints, receipts, invoices

**Governance is the set of responsibilities and practices exercised** by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly.

**RPO:** is determined based on the acceptable data lost in case of disruption of operations. It indicates the earliest point in time in which it is acceptable to recover the data.

**RTO:** is determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume AFTER DISASTER; **The lower the RTO, the lower the disaster tolerance**.

**Buffer**: Memory reserved to temporarily hold data to offset differences between the operating speeds of different devices, such as a printer and a computer Scope Note: In a program, buffers are reserved areas of random access memory (RAM) that hold data while they are being processed.

**DSS**: An interactive system that provides the user with easy access to decision models and data, to support semi structured decision-making tasks

Responsible for network security operations = **Security administrators**

Ensuring that security and control policies support business and IT objectives is a primary objective of **IT security policies audit**

**Escrow Agent**: A person, agency or enterprise that is authorized to act on behalf of another to create a legal relationship with a third party in regard to an escrow agreement; the custodian of an asset according to an escrow agreement Scope Note: As it relates

to a cryptographic key, an escrow agent is the agency or enterprise charged with the responsibility for safeguarding the key components of the unique key.

**XML**: Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and enterprises.

Risk-based Audit Approach: Gather Information and Plan; Obtain Understanding of Internal Control; Perform Compliance Tests; Perform Substantive Tests; Conclude the Audit

**Fiber**: Glass fibers that transmit binary signals over a telecommunications network Scope Note: Fiber-optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.

**Decision support system** Interactive system that provides the user with easy access to decision models and data from a wide range of sources – supports managers in decision making tasks for business purposes; Concentrates less on efficiency than on effectiveness (performing the right task). Improves managers decision making ability, but hard to measure.

**Implementation risk is inability to specify purpose and usage.**

**Foreign key**: A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value Scope Note: The problem of ensuring that the database does not include any invalid foreign key values is known as the referential integrity problem. The constraint that values of a given foreign key must match values of the corresponding candidate key is known as a referential constraint. The relation (table) that contains the foreign key is referred to as the referencing relation and the relation that contains the corresponding candidate key as the referenced relation or target relation. (In the relational theory it would be a candidate key, but in real database management systems (DBMSs) implementations it is always the primary key)

Because the data are directly collected by the IS auditor, the audit findings can be reported with an emphasis on the reliability of the records that are produced and maintained in the system. **The reliability of the source of information used provides reassurance on the findings generated.**

**Limit Check:** Tests specified amount fields against stipulated high or low limits of acceptability Scope Note: When both high and low values are used, the test may be called a range check.

The auditor must never take ownership of the problems found. The auditor may provide general advice to the auditee and demonstrate what they are looking for during the audit. The auditee needs to design their own remediation plan. **Auditors who participate in detailed remediation planning are no longer objective nor independent**

**BSC** is a way to measure performance, a definition of key performance indicators is required before implementing an IT BSC; will measure the value of IT to business, not the other way around; also will measure the performance of IT, but the control over IT expenses is not a key requirement for implementing a BSC.

**Maximum Allowed Outage (MAO):** The amount of time that the organization can sustain loss without going out of business.

**Maximum TOLAREABLE Outage (MTO)**: Maximum time the organization can support processing in ALTERNATE MODE; Acceptable downtime.

**Interruption window:** The time the organization can wait from the point of failure to the critical services/applications restoration.

**Service delivery objective (SDO):** Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the BUSINESS NEEDS.

**Computer evidence** is secondary evidence, not primary/best evidence.

**Benchmark** = Plan, research, observe, analyze, adapt, improve = PRO-AAI

**CASE TOOLS** (Data Flow Diagrams and data elements) = source code

large organizations and complex systems= **phased approach**

BC and DR plans must be aligned with **Change Management**

**Benchmarking**
plan-critical processes are identified
research-collect data,partners are identified
observer-visit partner
analyze-intercepting collected data
adopt-translate finding
improve-links each process

**BASE CASE SYSTEM EVALUATION**-in this technique, an auditee will prepare test data for an application system in cooperation with the auditor.The objective is to prepare a comprehensive 'base case' that can be used to test the application system BEFORE it is released into production

**Independent reviews** are carried out to compensate for mistakes or intentional failures in following prescribed procedures; Such reviews will help detect errors or irregularities.

**Time box management**: Project management technique for defining and deploying software deliverable within a relatively short and fixed period of time and with predetermined specific resources

**Extended records** .... A modification of the snapshot technique is the EXTENDED RECORD TECHNIQUE. Instead of having the software write one record for each snapshot point, auditors can have it construct a single record that is built up from the images captured at each snapshot point.

**INTEGRATED TEST FACILITY**-this involves creating a fictitious file or dummy entity in the database and processing audit test data against the entity as a means of verifying processing, authenticity, accuracy, and completeness

**Snapshot** can be used to track transactions in a financial institution that alter the terms of major loans

**SNAPSHOT**-records flow of designated transactions through logic paths within programs.It is used to verify program logic.The snapshot technique involves having software take 'pictures' of a transaction as it flows through an application system

Data center should be positive pressure – **air flows out.**

The digital certificate contains a public key that is used to encrypt messages and verify digital signatures

**Humidity** – too much and get corrosion/condensation, too little and get static electricity.

**Feedback error control** – only enough additional information is transmitted so the receiver can identify that an error has occurred – error detection only

**Digital certificates** are better than digital signatures because digital certificates are issued by trusted third parties.

**SHTTP** – similar to ssl, but not session oriented – does it based on message

**Configuration management** ensures that the setup and management of the network is done properly, including managing changes to the configuration, removal of default passwords and possibly hardening the network by disabling unneeded services.

**The selection of a recovery strategy would depend on:** Criticality of the Business Process / Cost / Time required recovering/ Security

The following meets the description "the primary objective is to leverage the internal audit function by placing responsibility of control and monitoring onto the functional areas" = Control self-assessment = **CSA**

**Governance** means the right people of authority made a decision. Governance occurs at the top level of management to prevent anarchy. Decisions made at too low a level below the executives may be an indicator of lack of governance.

**Recovery alternatives:** Cold sites, Mobile sites, Warm sites, hot sites, Mirrored sites, Reciprocal agreements

**Telecommunication Networks Disaster Recovery Methods:** Redundancy, alternative routing, diverse routing, long-haul network diversity, last-mile circuit protection and voice recovery.

**Based on the inputs received from the BIA**, criticality analysis and recovery strategy selected by management, a detailed BCP and DRP should be developed or reviewed.

**Implement the Business Continuity Plan**: Getting the final SENIOR-MANAGEMENT SING-OFF, creating enterprise-wide awareness for the plan, and implementing a plan and maintenance procedure.

**Beta testing** is the final stage of testing and typically includes users outside the development area. **Beta testing is a form of user acceptance testing (UAT)**, and generally involves a limited number of users who are external to the development effort.

**Providing security awareness training** is the best method to mitigate the risk of disclosing confidential information on social networking sites. It is important to remember that users may access these services through other means such as mobile phones and home computers; therefore, **awareness training is most critical.**
IS auditor should recommend reviewing the process of access control management. **Emergency system administration-level access should only be granted on an as-needed basis and configured to a predefined expiration date.** Accounts with temporary privileges require strong controls to limit the lifetime of the privileges and use of these accounts should be closely monitored.

**Verifying the decision with the business units**; it is not the IT function's responsibility to decide whether a new application modifies business processes.

**The overriding of computer processing jobs by computer operators** could lead to unauthorized changes to data or programs. This is a control concern; thus, it is always critical.

**BCP should be reviewed and updated on a scheduled basis** to reflect continuing recognition of changing requirements. The responsibility for maintaining the BCP often falls on the BCP coordinator.

**DRP part of BCP process**, IT DRP follows the same path. After conducting a BIA and risk assessment (determine the risks and effectiveness of mitigation controls otherwise), the IT DR strategy is developed. Implementing this strategy means making change to: IT systems, networks, IT processing sites, Organization structure, IT processes and procedures. The plan should be documented and written in simple language that is understandable to all.

An IS auditor should first evaluate the definition of the **minimum baseline** level by ensuring the sufficiency of the control baseline to meet security requirements.

**Configuration management** ensures that the setup and management of the network is done properly, including managing changes to the configuration, removal of default passwords and possibly hardening the network by disabling unneeded services.

**Topological mappings** provide outlines of the components of the network and its connectivity. This is important to address issues such as single points of failure and proper network isolation, but is not the most critical component of network management.

**Application monitoring** is not a critical part of network management.

**Thin client** is computer that does the work of presentation only and relies completely on server for computation... As opposed to FAT client; which does both processing as well as computation

**CA** can delegate the processes of: establishing a link between the requesting entity and its public key.

**ADVANTAGES OF JOB SCHEDULING SOFTWARES:**
• Job information is set up only once, reducing the probability of an error.
• Job dependencies are defined so that if job fails, subsequent jobs relying on its output will not be processed.
• Records are maintained of all job successes and failures.
• Reliance on operators is reduced.

**Assets** are anything of value. **Threats** are negative events that cause a loss if they occur. **Vulnerabilities** are paths that allow a threat to occur.

**Assessment** is less formal than an audit. The purpose of an assessment is to determine value based on relevance. Assessments have a lower value because they are not independent or a regimented independent audit

**Application stacking** is simply terminology used to discuss server virtualization; For running multiple applications on one or more virtual machines. Consolidating applications on a few large servers known as application stacking

Which of the following is in the BEST position to approve changes to the audit charter? **Audit committee**

**DISA:**
- Change default codes after installation of new equipment
- Never publish DISA telephone numbers
- Change your DISA access telephone number periodically
- Block or restrict overseas access;
- Program your system to answer with silence after five or six rings

**UPS**: is an intelligent power monitor coupled with a string of electrical batteries. The UPS constantly monitors electrical power. A UPS can supplement low-voltage conditions by using power stored in the batteries. During a power outage, the UPS will provide a limited amount of battery power

**UPS** are capable of signaling the computer to automatically shut down before the batteries are completely drained. Larger commercial UPS systems have the ability to signal the electrical standby generator to start.

**The service delivery objective (SDO)** illustrates the expected level of service during recovery. The organization may have several SDO targets based on the different phases of recovery.

**Contract personnel** should not be given job duties that provide them with power user or other administrative roles that they could then use to grant themselves access to sensitive files.

**Scorecard Disadvantages** The scorecard requires a careful selection of initiatives by the CEO or CFO. It is reported in executive trade journals that metrics derived from a committee will consistently fail. Interestingly, observations indicate that executives unwilling to adapt to the scorecard methodology may lack a genuine interest in being a team player or may possess more interest in building their own empire within the organization. Politics can kill the BSC unless the sponsor eliminates the people creating political conflict. Strong sponsors will not hesitate to remove obstacles.

**Normalization:** The process of removing duplicate, redundant data from a database.

**Emergency action team**: They are the first responders, whose function is to deal with fires or other emergency response scenarios.

**ONE OF THEIR PRIMARY FUNCTIONS IS THE ORDERLY EVACUATION OF PERSONNEL AND THE SECURING OF HUMAN LIFE.**

**Damage Assessment team:** Assesses the extent of damage following the disaster. The team should be comprised of individuals who have the ability to assess damage and estimate the time required to recover operations at the affected site.

**To ensure that the IT governance framework is effectively in place,** senior management must be involved and aware of roles and responsibilities. Therefore, it is most essential to ensure the role of senior management when evaluating the soundness of IT governance.

**Offsite storage team**: Responsible for obtaining, packaging and shipping media and records to the recovery facilities.

**Transportation team:** Serves as a facilities team to locate a recovery site, if one has not been predetermined, and is responsible for coordinating the transport of the company employees to a distant recovery site.

**Salvage team:** Manages the relocation project. This team also makes a more detailed assessment of the damage to the facilities and equipment than was performed initially; provides the emergency management team with the information required to determine whether planning should be directed toward reconstruction or relocation**. Provide information necessary for filing INSURANCE CLAIMS (INSURANCE CLAIMS IS THE PRIMARY SOURCE OF FUNDING FOR THE RECOVERY EFFORTS).**

**Relocation team:** Coordinates the process of moving from the hot site to a new location or to the restored original location.

Use of **a software baseline** provides a cutoff point for the design of the system and allows the project to proceed as scheduled without being delayed by scope creep.

**Balanced scorecard (BSC)** is a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives; **it does not prevent scope creep.**

**Centralized logging also provides security for log integrity.**

**Any systems performing event logging on a network should be synchronized with a central time server in order to cross-reference disparate logs.**

**Time-stamping:** Prevents falsifying date and time of access or modification.

**Identification**: Early incident detection is a key to minimizing loss; Detection through human observation, vulnerability assessments and IDS are forms of identifying an incident.

**Preservation and documentation of evidence** for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the admissibility of the evidence in legal proceedings.

Test data should be **sanitized** to prevent sensitive data from leaking to unauthorized persons.

The main change when using **thin client architecture** is making the servers critical to the operation; therefore, the probability that one of them fails is increased and, as a result, the availability risk is increased

**Digital signatures** provide authentication assurance of the email sender. Digital signatures use the private key of the sender to lock (encrypt) and the sender's public key to verify the sender's identity (by unlocking). Message hashing provides assurance the message was not modified.

**Verifying the existence of a security incident MUST BE ACHIEVED PRIOR TO FURTHER INVESTIGATION, CONTAINMENT, OR COMMUNICATION OF THE INCIDENT.**

**Upon detection of a significant security breach**, the information security manager should first notify the data owners who may be impacted by the breach.

**Containment:** Containing an incident to prevent further damage should be the first priority of incident response procedures. Assessing current system status should be the first response after suffering a denial-of-service attack. An information security manager's first response to a security-related incident is to contain the incident and minimize costs of impact.

**Eradication:** Periodic file backup can actually make total eradication of malicious code more difficult; especially if the malicious code is not detected through sever backup cycles; when containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network. Scope Notes: Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.

**Key logger**; sometimes called a keystroke logger, key logger, or system monitor, is a small program that monitors each keystroke a user types on a specific computer's keyboard. Using a key logger is the easiest way to hack an email account. A key logger program can be installed just in a few seconds and once installed you are only a step away from getting the victim's password.

**Bottom-up testing** begins by testing of atomic units such as programs or modules. The testing works upward until the complete system has been tested. The advantages to bottom-up testing are: No need for stubs or drivers, Can be started before all programs are complete, Provides early detection of errors in critical modules

**Damage assessment** should begin immediately following incident containment and recovery. Damage assessment should not limit its scope to a single system; **Damage Assessment Team** Works with structural engineers to assess damage to the facility. This team is trained to provide accurate analysis and estimates of the impact. This team works with the safety team for matters of safe reentry to the facility.

**Sampling Risks:** These are the risks that an auditor will falsely accept or erroneously reject an audit sample (evidence).

**Nonsampling Risks:** These are the risks that an auditor will fail to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objective (detection fault).

**Risk assessment:** Identify risk, vulnerabilities and threats => evaluate controls => determine audit objectives => supports risk based audit decision.

**Physically destroying the hard disk** is the most effective way to ensure that the data cannot be recovered

**The primary incident response objective of a post-event review is to improve the incident response process itself.**

**CMM provides five process maturity levels** (IRDMO) to guide organizations in selecting process improvement strategies to identify the most critical issues for software quality and process improvement.

- ✓ Initial - Ad hoc individual effort
- ✓ Repeatable - Processes are established to plan and track cost, schedule and functionality. These defined processes can be repeated on similar projects.
- ✓ Defined - Repeatable process are standardized across the organization.
- ✓ Managed - Quantitative managed control is applied to well-defined processes.
- ✓ Optimized - Managed processes are further refined for higher quality.

**Benchmarking Process** - a continuous, systematic process for evaluating and improving products, services, and work processes by comparing the organizations practices against leaders.

**Degaussing** is a bulk erasing process using a strong electromagnet. Degaussing equipment is relatively inexpensive. To operate, the degaussing unit is turned on and placed next to a box of magnetic media. The electromagnet erases magnetic media by changing its electrical alignment. Erasure occurs within minutes or hours, depending on the strength of the device.

**Physical Destruction** Just remembers the risk of standing data until you are certain that media is destroyed.

**SDLC models:** Waterfall Model - Iterative Model - Spiral Model - V-Model - Big Bang Model - Agile Model - RAD Model

**V-Model**, the corresponding testing phase of the development phase is planned in parallel. So there are Verification phases on one side of the 'V' and Validation phases on the other side. Coding phase joins the two sides of the V-Model.

**Big Bang Model** is SDLC model where there is no formal development followed and very little planning is required. Even the customer is not sure about what exactly he wants and the requirements are implemented on the fly without much analysis. Usually this model is followed for small projects where the development teams are very small.

**Accountability** individuals must be identifiable and must be held responsible for their actions.

**Accredited** A computer system or network that has received official authorization and approval to process sensitive data in a specific operational environment. There must be a security evaluation of the system's hardware, software, configurations, and controls by technical personnel.

**Annualized loss expectancy (ALE):** Dollar amount that estimates the loss potential from a risk in a span of a year; single loss expectancy (SLE) × annualized rate of occurrence (ARO) = ALE

**Annualized rate of occurrence (ARO):** The value that represents the estimated possibility of a specific threat taking place within a one-year timeframe.

**Audit trail:** chronological set of logs and records used to provide evidence of a system's performance or activity that took place on the system. These logs and records can be used to attempt to reconstruct past events and track the activities that took place, and possibly detect and identify intruders.

**Authenticate** = verify the identity

**Authorization** = Granting access to an object after the subject has been properly identified and authenticated.

**Automated information system (AIS)** computer system that is used to process and transmit data. It is a collection of hardware, software, and firmware that works together to accept, compute, communicate, store, process, transmit, and control data processing functions.

**Availability** The reliability and accessibility of data and resources to authorized individuals in a timely manner.

**Back up** Copy and move data to a medium so that it may be restored if the original data is corrupted or destroyed. A full backup copies all the data from the system to the backup medium. An incremental backup copies only the files that have been modified since the previous backup. A differential backup backs up all files since the last full backup.

**Backdoor** An undocumented way of gaining access to a computer system. After a system is compromised, an attacker may load a program that listens on a port (backdoor) so that the attacker can enter the system at any time. A backdoor is also referred to as a trapdoor.

**Confidentiality** A security principle that works to ensure that information is not disclosed to unauthorized subjects.

**Configuration management** The identification, control, accounting, and documentation of all changes that take place to system hardware, software, firmware, supporting documentation, and test results throughout the lifespan of the system.

**Contingency plan:** A plan put in place before any potential emergencies, with the mission of dealing with possible future emergencies. It pertains to training personnel, performing backups, preparing critical facilities, and recovering from an emergency or disaster so that business operations can continue.

**Control zone:** The space within a facility that is used to protect sensitive processing equipment. Controls are in place to protect equipment from physical or technical unauthorized entry or compromise. The zone can also be used to prevent electrical waves carrying sensitive data from leaving the area.
**Cost/benefit analysis** An assessment that is performed to ensure that the cost of a safeguard does not outweigh the benefit of the safeguard. Spending more to protect an asset than the asset is actually worth does not make good business sense.

**Data classification** Assignments to data that indicate the level of availability, integrity, and confidentiality that is required for each type of information.

**Data custodian:** an individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department (usually the network administrator). The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the company's security policy, standards, and guidelines that pertain to information security and data protection.

**Database shadowing Mirroring technology:** is used in databases, in which information is written to at least two hard drives for the purpose of redundancy.

**Degauss** Process that demagnetizes magnetic media so that a very low residue of magnetic induction is left on the media; used to effectively erase data from media.

**Delphi technique:** group decision method used to ensure that each member of a group gives an honest and anonymous opinion pertaining to the company's risks.

**Denial of service (DoS)** any action, or series of actions, that prevents a system, or its resources, from functioning in accordance with its intended purpose.

**Dictionary attack a** form of attack in which an attacker uses a large set of likely combinations to guess a secret, usually a password.

**Digital signature** An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

**Discretionary access control (DAC)** An access control model and policy that restricts access to objects based on the identity of the subjects and the groups to which those subjects belong. The data owner has the discretion of allowing or denying others access to the resources it owns.

**Due care** Steps taken to show that a company has taken responsibility for the activities that occur within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.
**Due diligence:** the process of systematically evaluating information to identify vulnerabilities, threats, and issues relating to an organization's overall risk.
**Electronic vaulting:** the transfer of backup data to an offsite location; through communications lines to a server at an alternative location.

**Emanations** Electrical and electromagnetic signals emitted from electrical equipment that can transmit through the airwaves. These signals carry information that can be captured and deciphered, which can cause a security breach. These are also called emissions.

**Exposure factor** The percentage of loss a realized threat could have on a certain asset.

**Gateway** A system or device that connects two unlike environments or systems. The gateway is usually required to translate between different types of applications or protocols.

**Guidelines** Recommended actions and operational guides for users, IT staff, operations staff, and others when a specific standard does not apply.

**Executive management**: Responsible for the overall protection of information assets, and for issuing and maintaining the policy

framework.

**Honeypot** A computer set up as a sacrificial lamb on the network in the hope that attackers will attack this system instead of actual production systems.

**Integrity** A security principle that makes sure that information and systems are not modified maliciously or accidentally.

**Intrusion detection system (IDS)** Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms.

**Isolation** The containment of processes in a system in such a way that they are separated from one another to ensure integrity and confidentiality.

**Keystroke monitoring** A type of auditing that can review or record keystrokes entered by a user during an active session.

**Lattice-based access control model** mathematical model that allows a system to easily represent the different security levels and control access attempts based on those levels. Every pair of elements has a highest lower bound and a lowest upper bound of access rights. The classes stemmed from military designations.

**Link encryption:** type of encryption technology that encrypts packets' headers, trailers, and the data payload. Each network communications node, or hop, must decrypt the packets to read its address and routing information and then re-encrypt the packets. This is different from end-to-end encryption.

**Audit Report:** Findings are based on appropriate, relevant and sufficient audit evidence. That is all recorded initially in the work papers. The actual report starts as a preliminary report that would be shared with IS management for comments and their proposed corrective action. Once the auditors and IS management are satisfied with the final product, the final report is released to the Audit Committee/Board or Upper Management. **So the report needs to be supported by statements from IS management.**
**CSA**: nothing to do with an audit report.

**Out-of-band connectivity** is something that is not in the same channel of communication. Common example is the OTP that you receive on your mobile, for authorization of any payment that you make online.

**Logic bomb** A malicious program that is triggered by a specific event or condition.

**Maintenance hook** Instructions within a program's code that enable the developer or maintainer to enter the program without having to go through the usual access control and authentication processes. Maintenance hooks should be removed from the code before it is released to production; otherwise, they can cause serious security risks. Also called trapdoor or backdoor.

**Malware:** Code written to perform activities that circumvent the security policy of a system. Examples are viruses, malicious applets, Trojan horses, logical bombs, and worms.

**Mandatory access control (MAC)** An access policy that restricts subjects' access to objects based on the security clearance of the subject and the classification of the object. The system enforces the security policy, and users cannot share their files with other users.

**Masquerading** Impersonating another user, usually with the intention of gaining unauthorized access to a system.

**Message authentication code (MAC)** in cryptography, a message authentication code (MAC) is a generated value used to authenticate a message.

**Piggyback** Unauthorized access to a system by using another user's legitimate credentials.

**Playback attack** Capturing data and resending the data at a later time in the hope of tricking the receiving system. This is usually carried out to obtain unauthorized access to specific resources.

**Privacy** A security principle that protects an individual's information and employs controls to ensure that this information is not disseminated or accessed in an unauthorized manner.

**Public key encryption** A type of encryption that uses two mathematically related keys to encrypt and decrypt messages. The private key is known only to the owner, and the public key is available to anyone.

**Purge** The removal of sensitive data from a system, storage device, or peripheral device with storage capacity at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data cannot be reconstructed.

**Qualitative risk analysis:** a risk analysis method that uses intuition and experience to judge an organization's exposure to risks. It uses scenarios and ratings systems. Compare to quantitative risk analysis.

**Quantitative risk analysis:** a risk analysis method that attempts to use percentages in damage estimations and assigns real numbers to the costs of countermeasures for particular risks and the amount of damage that could result from the risk. Compare to qualitative risk analysis.

**RADIUS (Remote Authentication Dial-in User Service)** A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism.

**Recovery planning**: The advance planning and preparations that is necessary to minimize loss and to ensure the availability of the critical information systems of an organization after a disruption in service or a disaster.

**Reference monitor concept:** an access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. The security kernel enforces the reference monitor concept.

**Reliability:** The assurance of a given system, or individual component, performing its mission adequately for a specified period of time under the expected operating conditions.

**Repudiation** When the sender of a message denies sending the message. The countermeasure to this is to implement digital signatures.

**Residual risk:** The remaining risk after the security controls has been applied. The conceptual formulas that explain the difference between total and residual risk are threats × vulnerability × asset value = total risk (threats × vulnerability × asset value) × controls gap = residual risk

**Risk** The likelihood of a threat agent taking advantage of vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit vulnerability.

**Risk analysis:** a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards.

**Risk management:** the process of identifying, assessing, and reducing the risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

**RBAC** Type of model that provides access to resources based on the role the user holds within the company or the tasks that the user has been assigned.

**SOD** A security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

**Shoulder surfing:** When a person looks over another person's shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.

**Single loss expectancy (SLE):** a dollar amount that is assigned to a single event that represents the company's potential loss amount if a specific threat were to take place. asset value × exposure factor = SLE

**Social engineering:** the act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

**Spoofing** Presenting false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

**Standards** Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies,

**TACACS (Terminal Access Controller Access Control System)** A client/ server authentication protocol that provides the same type of functionality as RADIUS and is used as a central access control mechanism mainly for remote users.

**Trojan horse** A computer program that has an apparently or actually useful function, but that also contains additional hidden malicious capabilities to exploit a vulnerability and/or provide unauthorized access into a system.

**Validation:** the act of performing tests and evaluations to test a system's security level to see if it complies with security specifications and requirements.

**Virus:** small application, or string of code, that infects applications. The main function of a virus is to reproduce, and it requires a host application to do this. It can damage data directly or degrade system performance.

**Worm** An independent program that can reproduce by copying itself from one system to another. It may damage data directly or degrade system performance by tying up resources.

**Authentication:** Assuring that a message has not been modified in transit or while stored on a computer. It is one of the objectives of cryptography. (This is referred to as message authentication or message integrity.)

**Certificate:** A certificate is a data file that identifies an individual, organization, or business. Certificates are obtained from specialized certificate-issuing companies and can be used to encrypt data and/or confirm the certificate owner's identity.

**Certificate authority (CA):** is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Depending

on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

**Confidentiality:** assurance that only owners of a shared secret key can decrypt a computer file that has been encrypted with the shared secret key.

**Digital Certificate**: a specialized document signed by a trusted third party which is the preferred way to securely deliver public keys. The top part of a digital certificate contains plaintext identifying the issuer (signer), subject (whose public key is attached), the subject's public key and the expiration date of the certificate. The bottom part of a digital certificate contains the issuer's signed hash of the top part.

**Digital Signature:** a small piece of code that is used to authenticate the sender of data. Digital signatures are created with encryption software for verification purposes. A private key is used to create a digital signature, and a corresponding public key can be used to verify that the signature was really generated by the holder of the private key.

**Hashing:** is used to encrypt and decrypt digital signatures. The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received. (They should be the same.)

**Integrity:** assurance that a file was not changed during transit; also called message authentication.

**Key:** is simply a special piece of data used for encryption and/or decryption. Keys are not human readable and typically look like alphanumeric gibberish.

**Risk assessment** is used to gather data.

**Risk analysis** examines the gathered data to produce results that can be acted upon.

**Non-repudiation** - assurance that the sender cannot deny a file was sent. This cannot be done with secret key alone.

**Private Key:** a concealed key held by only one person in public key cryptography. It is never shared.

**Public Key:** used in asymmetric cryptography. One of their primary purposes is to enable someone to encrypt messages intended for the owner of the public key. Public keys are meant for distribution, so anyone who wants to send an encrypted message to the owner of the public key can do so, but only the owner of the corresponding private key can decrypt the message.

**Eradication**: When containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network..

**Scope Notes**: Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.

**Allowance for sampling risk**: An interval around the sample results in which the true population characteristic is expected to lie.

**Attributes sampling:** A sampling plan enabling the auditors to estimate the rate of deviation (occurrence) in a population.

**Deviation rate:** A defined rate of departure from prescribed controls. Also referred to as occurrence rate or exception rate.

**Difference estimation:** A sampling plan that uses the difference between the audited (correct) values and book values of items in a sample to calculate the estimated total audited value of the population. Difference estimation is used in lieu of ratio estimation when the differences are not nearly proportional to book values.

**Discovery sampling:** A sampling plan for locating at least 1 deviation, providing that the deviation occurs in the population with a specified frequency.

**Dual-purpose test:** A test designed to test a control and to substantiate the dollar amount of an account using the same sample.

**Estimated total audited value:** Based on the variables sampling method used (e.g., mean-per-unit, ratio, difference) and the sample selected, the most likely point estimate of the account audited value.

**Expected population deviation rate:** An advance estimate of a deviation rate. This estimate is necessary for determining the required sample size in an attributes sampling plan.

The ability of two or more objects to interpret a message differently at execution, depending on the superclass of • the calling object, is termed **polymorphism**

The most secure firewall system is: The **screened-subnet firewall**

**Mean:** The average item value, computed by dividing total value by the number of items composing total value.

**Mean-per-unit estimation** A classical variables sampling plan enabling the auditors to estimate the average dollar value (or other variable) of items in a population by determining the average value of items in a sample.

**Nonsampling risk:** The aspects of audit risk not due to sampling. This risk normally relates to "human" rather than "statistical" errors.

**Physical representation of the population:** The population from which the auditors sample. The physical representation of the population differs from the actual population when it does not include items that exist in the actual population. For example, the auditors sample from a trial balance of receivables which may or may not include all actual receivables.

**Population:** The entire field of items from which a sample might be drawn.

**Precision**: See allowance for sampling risk.

**Probability-proportional-to-size sampling:** A variables estimation procedure that uses attributes theory to express a conclusion in monetary (dollar) amounts.

**Projected misstatement:** An estimate of the most likely amount of monetary misstatement in a population.

**Random selection:** Selecting items from a population in a manner in which every item has an equal chance of being included in the sample.

**Ratio estimation:** A sampling plan that uses the ratio of audited (correct) values to book values of items in the sample to calculate the estimated total audited value of the population. Ratio estimation is used in lieu of difference estimation when the differences are nearly proportional to book values.

**Reliability:** The complement of the risk of incorrect acceptance.

**Representative sample** A sample possessing essentially the same characteristics as the population from which it was drawn.

**Risk of assessing control risk too high:** This risk is the possibility that the assessed level of control risk based on the sample is greater than the true operating effectiveness of the control.

**Risk of assessing control risk too low:** This most important risk is the possibility that the assessed level of control risk based on the sample is less than the true operating effectiveness of the controls.

**Risk of incorrect acceptance:** The risk that sample results will indicate that a population is not materially misstated when, in fact, it is materially misstated.

**Risk of incorrect rejection:** The risk that sample results will indicate that a population is materially misstated when, in fact, it is not.

**Sampling error:** The difference between the actual rate or amount in the population and that of the sample. For example, if an actual (but unknown) deviation rate of 3 percent exists in the population, and the sample's deviation rate is 2 percent, the sampling error is 1 percent.

**Sampling risk:** The risk that the auditors' conclusion based on a sample might be different from the conclusion they would reach if the test were applied to the entire population. For tests of controls, sampling risks include the risks of assessing control risk too high and too low; for substantive testing, sampling risks include the risks of incorrect acceptance and rejection.

**Sequential (stop-or-go) sampling**: A sampling plan in which the sample is selected in stages, with the need for each subsequent stage being conditional on the results of the previous stage.

**Standard deviation:** A measure of the variability or dispersion of item values within a population; in a normal distribution, 68.3 percent of all item values fall within 1 standard deviation of the mean, 95.4 percent fall within 2 standard deviations, and 99.7 percent fall within 3 standard deviations.

**Stratification:** Dividing a population into two or more relatively homogeneous subgroups (strata). Stratification increases the efficiency of most sampling plans by reducing the variability of items in each stratum. The sample size necessary to evaluate the strata separately is smaller than would be needed to evaluate the total population.

**Systematic selection:** The technique of selecting a sample by drawing every nth item in the population, following one or more random starting points.

**Tolerable deviation rates:** The maximum population rate of deviations from a prescribed control that the auditor will tolerate without modifying the planned assessment of control risk.

**Tolerable misstatement:** An estimate of the maximum monetary misstatement that may exist in an account balance without causing the financial statements to be materially misstated.

**Variables sampling:** Sampling plans designed to estimate a numerical measurement of a population, such as a dollar value.

**Voucher:** A document authorizing a cash disbursement. A voucher usually provides space for the initials of employees performing various approval functions. The term voucher may also be applied to the group of supporting documents used as a basis for recording liabilities or for making cash disbursements.

**Information risk:** The risk that the information used by investors, creditors, and others to assess business risk is not accurate.

**Integrated audit:** As required by the Sarbanes-Oxley Act and the Public Company Accounting Oversight Board, an audit that includes providing assurance on both the financial statements and internal control over financial reporting. Integrated audits are required of publicly traded companies in the United States.

**Operational audit:** An analysis of a department or other unit of a business or governmental organization to measure the effectiveness and efficiency of operations.

**Adequate disclosure:** All essential information as required by generally accepted accounting principles (or some other appropriate basis of accounting) is included in the financial statements.

**Audit risk:** The risk that the auditors may unknowingly fail to appropriately modify their opinion on financial statements that are materially misstated.

**Auditors' report:** A very precise document designed to communicate exactly the character and limitations of the responsibility being assumed by the auditors; in standard form, the report consists of an introductory paragraph, a scope paragraph, and an opinion paragraph.
**Consistency:** The concept of using the same accounting principles from year to year so that the successive financial statements issued by a business entity will be comparable.

**Error:** An unintentional misstatement of financial statements or omission of an amount or a disclosure.

**Fraud**: For financial statement audits, "fraud" includes two types of intentional misstatements of financial statements—misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets. Legally, fraud is the misrepresentation by a person of a material fact, known by that person to be untrue or made with reckless indifference as to whether the fact is true, with intent to deceive and with the result that another party is injured.

**Independence** A most important auditing standard, which prohibits CPAs from expressing an opinion on financial statements of an enterprise unless they are independent with respect to such enterprise; independence is impaired by a direct financial interest, service as an officer or trustee, certain loans to or from the enterprise, and various other relationships.

**Inspection** (conducted by the Public Company Accounting Oversight Board) A process that leads to an assessment of the degree of compliance of each registered public accounting firm and associated persons of that firm with the Sarbanes-Oxley Act of 2002 and the board's requirements in connection with its performance of audits, issuance of audit reports, and related matters.

**Internal control:** A process, effected by the entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (1) reliability of financial reporting; (2) effectiveness and efficiency of operations; and (3) compliance with applicable laws and regulations.

**Defendant:**The party against which damages and suit are brought against by the defendant.

**Due diligence:** A public accounting firm's contention that its audit work was adequate to support its opinion on financial statements included in a registration statement filed with the SEC under the Securities Act of 1933.

**vLAN** is only a logical segregation and can't be accepted as a high security principle in a risky environment.

**Fraud:** Misrepresentation by a person of a material fact, known by that person to be untrue or made with reckless indifference as to whether the fact is true, with intent to deceive and with the result that another party is injured.

**Control risk:** The risk that a material misstatement that could occur in an account will not be prevented or detected on a timely basis by internal control.

**Detection risk:** The risk that the auditors' procedures will lead them to conclude that a financial statement assertion is not materially misstated when in fact such misstatement does exist.

**Inherent risk:** The risk of material misstatement of a financial statement assertion, assuming there were no related controls.

**Substantive tests:** Tests of account balances and transactions designed to detect any material misstatements in the financial statements. Substantive tests directly affect detection risk

Which of the following would be an indicator of the effectiveness of a computer security incident response team? **Financial impact per security incident**

**Analysis:** A working paper showing all changes in an asset, liability, equity, revenue, or expense account during the period covered by the audit.

**Audit evidence:** Any information that corroborates or refutes the auditors' premise that the financial statements present fairly the client's financial position and operating results.

**Audit file:** The unit of storage for a specific audit engagement. The audit documentation for each year's audit of a company is included in its audit file.

**Audit risk:** The risk that the auditors may unknowingly fail to appropriately modify their opinion on financial statements that are materially misstated.

**IT steering Committee** - The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives

**IS steering committee** = MoM

**Segregation of Duties** = Compensating Controls

**Bottom Up:** Are more likely to be derived as a result of a risk assessment

**Bollards:** implement barriers that will block the passage of vehicles but freely allow foot traffic

**Top-Down:** Are developed for the organization as a whole , Will not conflict with overall corporate policy, Ensure consistency across the organization.

**Security Baseline** – Sufficiency of control, doc , Implementation, Compliance

**Strategic alignment**, - Strategic alignment provides input for security requirements driven by enterprise requirements

**Value delivery** - Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. aligning the IT strategy with the enterprise strategy.

**Risk management provides an understanding of risk exposure**

**SOD – COMPENSATIONG CONTROLS**

- Reviewing transaction and application logs
- Restricting LOGICAL access to computing equipment

**Difference Between Symmetric and Asymmetric Encryption**; Essentially, symmetric has to have pre-chosen passwords, and asymmetric can generate its own password.

**Board of Directors (Sr. Mgmt)** - determining business goals

**STEERING Committee ---** More Connected to Sr. Managnemt (MoM) – Approve the projects

**Strategy Committee**

- Aligning IT to business objectives
- Advising on IT compliance risk
- Promoting IT governance practices

**Too Much Power**
Spike → High amount of voltage for a short time.
Surge → High amount voltage for a long time.

**Decline of Power**
Sag/Dip → Low amount of voltage for a short time.
Brownout → Low amount of voltage for a long time.

**No Power**
Fault → No power for a short time.
Blackout → No power for a long time.

**UPS** Serves as a backup power source in the event of a short power outage or times of voltage fluctuations - Protects against surges, spikes, blackout, brownout, faults…

**Surge Protectors** Protects hardware and equipment from power fluctuations, such as changes in voltage - Protects against spikes, surges

**Power Generators:** Serves as a backup power source in the event of a long power outage - Protects against blackouts

**These are the elements of a fire**: Oxygen, heat, and a fueling agent.

**Halon** prevents fires by stopping their chemical reaction.

**Waterfall Model:** The process is linear - It does not allow programmers to go back a step - It is does not work for complicated and detailed projects, maybe smaller projects

**Dual-Password** Two different types of authentication for a single user - multi-factor authentication, or more specifically two-factor authentication.

**Dual-Control** 1xoperation is split between two people. Suppose the same database with the encryption keys is locked away in separate technology room which must be opened first. The entrance to this room has a door that is about 3 meters wide. Both sides of the door has a biometric fingerprint scan machine. Two people with the same authorization has to scan their fingerprints at the same time in order for the door to open.

**CMM** provides developers a way to make sure the software they are developing is done properly and with due care. Without proper care, software can crash, error out, or worse, fail to meet the expectations of the customer.

**Risk tolerance** tells you how sensitive the organization or people are to risks. High tolerance means people are willing to take a high risk, and low tolerance means people are not willing to take much risk. It is the willingness of a group of people or organization to accept or avoid risk. It shows the risk attitude of stakeholders or an organization in measurable units.

**Cryptography** – Study of encrypting messages

**Cryptanalysis** – Study of decrypting messages

**Cryptology** – Study of the mathematics behind encryption/decryption

**Referential Integrity**: issues occur when a foreign key does not reference a primary key. If you create another table from the original table, the foreign key in the second table must reference the primary key in the first table. (RDBMS)

**Entity Integrity**: Databases must have a unique primary key! Primary keys uniquely identify something in a database. If you have two exact primary keys, it's like having two people in a database with matching fingerprints. Doesn't make sense!

**Semantic Integrity:** Maintaining semantic integrity means the value of the data in a cell corresponds with the correct data type.

**Exploit** is a piece of malware code that takes advantage of a newly-announced or otherwise unpatched vulnerability in a software application, usually the operating system, a web browser or a program that routinely activates through a web browser (PDF reader, media player, or other 'plug-in').

**Risk appetite** can be considered as a tendency of an individual or group of people towards risks.

**Risk tolerance** is an acceptable variance; e.g. +5% to -5%. Tolerance is a limit.

**Zero-day exploit** is an exploit that takes advantage of a vulnerability on the same day that the vulnerability is announced.

**Vulnerability** Software applications, such as the Microsoft operating system or your web browser are complex feats of engineering, often with millions of lines of programming code. Inevitably, errors creep into the code, and some of these errors create security vulnerabilities that malefactors can take advantage of with exploits and other malware.

**Social engineering** is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face.

**Trojan horse** is also a type of virus which is used to control remote machine without system owner knowledge. Trojan has two parts: 1. server 2. Client, Server handles all infected remote computers' connections and client is used to infect victim computer system. Every Trojan has its associated port number for communication over internet or LAN.

**Root kit** is also a virus like Trojan for remote access of any system. Root kit is very powerful as compared to Trojan because root kit implements on kernel level of any operating system, which is hard to detect and delete. Root kit is invisible in task manager as it hides itself.

**Spyware** is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent.

**Elements encryption systems:** • Encryption algorithm • Encryption key • Key length

**Symmetric Key:**

- Use the same (shared) key to both encrypt and decrypt a message
- Fast, Confidentiality, good for bulk message and streaming media encryption
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

**Asymmetric Key:**

- Private key kept private by owner
- Public key can be distributed freely
- May use certificates to distribute public keys (PKI to be seen later)
- Confidentiality, access control, non-repudiation, authenticity, integrity
- Disadvantages – slow
- Examples – RSA, Diffie-Hellman, Elliptic Curve ECC

**Hashing Algorithms**
• Used for message integrity
• Calculates a digest of the message
• Can be validated by the receiver to ensure the message was not changed in transit or storage
• Examples: MD5, SHA-1, SHA256

**Digital signatures: Created by signing a hash of a message with the private key of the sender**
• Data integrity
• Authentication
• Nonrepudiation
• Replay protection

**Digital envelope:** Used to send encrypted information and the relevant key along with it. The message to be sent, can be encrypted by using either: Asymmetric key; Symmetric key

**Risk-based Auditing**
- Gather Information and Plan;
- Knowledge of business and industry
- Prior year's audit results
- Recent financial information
- Regulatory statutes
- Inherent risk assessments

**Perform Compliance Tests;**
• Identify key controls to be tested
• Perform tests on reliability, risk prevention, and adherence to organizational policies and procedures

**Perform Substantive Tests;**
• Analytical procedures
• Detailed tests of account balances
• Other substantive audit procedures

**Audit planning steps**
• Gain an understanding of the business's mission, objectives, purpose and processes
• Identify stated contents (policies, standards, guidelines, procedures, and organization structure)
• Evaluate risk assessment and privacy impact analysis
• Perform a risk analysis
• Conduct an internal control review
• Set the audit scope and audit objectives
• Develop the audit approach or audit strategy
• Assign personnel resources to audit and address engagement logistics
• Write audit report

The IS auditor should apply their own **Professional Judgment** to the specific circumstances

**Standards:** Must be followed by IS auditors Guidelines

**Guidelines:** Provide assistance on how to implement the standards Tools and Techniques

**Tools and Techniques:** Provide examples for implementing the standards

**Compliance test** Determines whether controls are in compliance with management policies and procedures

**Substantive test:** Tests the integrity of actual processing

**CAATs enable IS auditors to gather information independently**

**CAATs include:**
• Generalized audit software (GAS)
• Utility software
• Debugging and scanning software
• Test data
• Application software tracing and mapping
• Expert systems

**Features of generalized audit software (GAS):** Mathematical computations; Stratification; Statistical analysis; Sequence checking

**Functions supported by GAS:** File access; File reorganization; Data selection; Statistical functions; Arithmetical functions

The FIRST step in managing the risk of a cyber-attack is to: **Identify critical information assets**

To check compliance with a service level agreements (SLA) requirement for uptime = **Availability reports**

Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is: **Encrypted using dynamic keys**

FIRST step in managing the risk of a Cyber Attack is to: **Identify critical information assets**

When using a **digital signature**, the message digest is computed: by both the sender and the receiver

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the: **certificate authority (CA**).

**Security administration** read-only access security log files.

**Audit trail** is not effective if the details in it can be amended

**Characteristic of timebox management**: Prevents cost overruns and delivery delays

Online auditing techniques is most effective for the early detection of errors or irregularities = **Audit hooks**

Data validation edits is effective in detecting transposition and transcription errors = **Check digit**

White box testing is that it: **Determines procedural accuracy or conditions of a program's specific logic paths.**

**Not backing up the servers** on a regular basis is the most serious threat to the integrity and availability of informational assets

**MD5** is a hashing algorithm. (Verify integrity)

**RSA** is an asymmetric algorithm that generally offers confidentiality, authentication, and nonrepudiation.

The most important step of the pen test process is to obtain **written authorization** and approval. No testing should occur until this step is completed.

**A digital signature** contains a message digest to: show if the message has been altered after transmission.

Digital signatures = **data integrity**

**Retina** scans are invasive—they can relay user health information. Iris scans remain (comparatively) stable regarding the general health of the user attempting access.

**Retina** scans change depending on the person's health, iris scans are stable

BEST information source to obtain evidence when a server has been compromised by malware = **Volatile data held in computer resources**

**Application programmers or system development programmers** should not have access to production data or programs.
The worst condition for an IDS = **False negative**

**Chain of custody** is the critical item that must be maintained during any forensic activity. Chain of custody concerns who collected the information and how it was documented, processed, stored, and handled.

**Risk analysis** is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected information held by a covered entity, and the likelihood of occurrence. The risk analysis may include taking inventory of all systems and applications that are used to access and house data, and classifying them by level of risk.

**Risk assessment** is the process of analyzing potential losses from a given hazard using a combination of known information about the situation, knowledge about the underlying process, and judgment about the information that is not known or well understood

Ensure **CIA** of a message, the sender should encrypt the hash of the message with the sender's: private key and then encrypt the message with the receiver's public key.

To ensure that internal application interface errors are identified as soon as possible = **Top-down**

Organizational policies is often driven by risk assessment = **Top-down**

**Audit trails** = establish accountability and responsibility for processed transactions.

RFID tags are subject to **Eavesdropping**

**Digital signature**: Create a hash of the entire message, encrypts that hash with sender's private key. Provides integrity, authentication, non-repudiation, but not confidentiality (INTEGRITY)

**Digital envelope** - Sender encrypts the message with a symmetric key (session key). The session key is encrypted with the receiver's public key and sent. (CONFIDENTIALITY)

**Preventive (strongest)** – prevents threat from exploiting vulnerability

**Detective** – detects that a control has failed

**Corrective** – corrects situation and mitigates risk

**Compensating controls** – if another control fails or not possible, can mitigate risk through

**Format-preserving encryption** preserves the ability of users and applications to read the protected data and is one of the fastest performing encryption processes.

**SDM** is utilized in test/development environments in which data that look and act like real data are needed for testing, but sensitive data are not exposed to developers or systems administrators.

**DDM** provides security to data at rest or in transit and from privileged users.

**Tokenization**, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token that has no extrinsic or exploitable meaning or value.

**Projects** are unique, temporary and are developed progressively.

**Business case** – shows benefits to be achieved for the business and must be kept for lifecycle of project

**Influence** – Project Manager has no formal authority

**Pure project** – Project Manager has formal authority over those taking part in project.

**Matrix project** – Project Manager share authority with functional managers (Dual Reporting)

**Engagement letter** - It acts as a CONTRACT between CLIENT AND AUDITOR.

**SMART:** Specific – Measurable – Achievable - Relevant - Time bound

**Senior Mgmt** - approves the resources for the project

**User Mgmt** – assumes ownership of project and resulting system

**Project steering committee** – overall direction and ensures stakeholders represented. Responsible for deliverables, costs and schedules

**Project sponsor** – provides funding and works with Project Manager to define critical success factors and metrics. Data and application ownership assigned to sponsor

**Project manager** – provides day to day management of project.

**Three critical elements to projects**: Time + Cost + Scope

**Software size estimation:** Lines of code – SLOC (# of lines of source code), KLOC (kilo lines of source code), KDSI – thousand delivered source instruction – better for basic or cobol.

**Function Point analysis** – used to estimate complexity in developing large apps. Size measured based on number and complexity of inputs, outputs, files, interfaces and queries. Software Cost estimates directly related to software size estimates.

**GANTT charts:** aid in scheduling of activities/tasks. Charts show when activities start and end and dependencies. Used for checkpoints/milestones too.

**PERT** – network management technique Shows relationships between various tasks and shows estimates/scenarios for completing tasks – three estimates shown – optimistic, most likely and pessimistic. It doesn't talk about costs.

**Time box** – project management technique for defining and deploying software deliverables within a short and fixed period of time with pre-determined resources; must be a software baseline.

**Data Conversion**: risk is you will not convert all the data – some will be missed. You also need to make sure that you are comparing control totals before and after conversion to avoid this.

**XML** document is case-sensitive which is different from HTML code

**XML** is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and enterprises.

**Output Controls**: logging storage of negotiable + computer generation + report distribution

**Control totals** can be used to compare batches too.

**Configuration management** – interrelationships between assets

**QA** is responsible for ensuring that programs and program changes and documentation adhere to established standards.

**Project steering committee** approves the RFPs for software acquisitions. It is responsible for all costs and timetables.

**IT asset management** is more concerned towards the ownership of physical assets rather than the maintaining the baseline for configuration. Some controls are required to check that procured IT asset conformed to EA (enterprise architecture) set standards.

**IT Asset Management** is to manage the lifecycle of physical IT assets (PC, Desktop, Physical Servers) starting from procurement, delivery to end-user, installation, disposal etc.

**Configuration management** is to manage and create a baseline for CIs which can be tangible (physical assets) and intangible (VMs, Applications, Services).

**Bottom up** – Finds critical errors earlier because can start before system done – sort of white box testing.

**Top down** – start at interfaces of entire system and work your way down to each function/component – like black box testing – functional

**TQM** purpose is end user satisfaction

**Unit testing** – testing of individual programs or modules – usually white box testing.

**System testing** – making sure that all modules function together properly

**Integration testing** – evaluates connection of components that pass info to each other.

**Final acceptance testing** – done during implementation phase by QA and then UAT.

**White box** – assess effectiveness of software program logic.

**Black box** – testing of interfaces and general function – doesn't care about internal structure.

**Function/validation** – similar to system testing, but often used to test the functionality of the system against requirements

**Regression testing** – rerunning a portion of a test scenario to make sure that changes have not introduced new errors in other parts of app

**Sociability** – confirm that the new system can operate in its target environment without affecting other systems.

**Prototyping** – creating system through controlled trial and error. Can lead to poor controls in finished system because focused on what user wants and what user sees. Change control complicated also – changes happen so quickly, they are rarely documented or approved. Also called evolutionary development. Reduces risk associated with not understanding user requirements. Just include screens, interactive edits and reports (no real process programs)

**RAD** – methodology to develop important systems quickly, while reducing costs but maintaining quality. – small dev teams, evolutionary prototypes, Automates large portions of the SDLC via CASE and imposes rigid time frames. Prototyping is core to this. Skip documentation, less emphasis on requirements.

**Object Oriented** – data and software together to form object – sort of a blackbox – other objects talk to the object's interface and don't care what's inside. Encapsulation provides high degree of security over the data.

**Component based** – outgrowth of object oriented – assembling applications from cooperating packages of executable software that make services available through defined interfaces.

**WSDL** – web services description language – also based on XML. Used to identify the SOAP specification to be used for the API and the formats of the SOAP messages used for input and output to the code modules; Also used to identify the particular web service accessible via a corporate intranet or across the Internet by being published to a relevant intranet or internet web server.

**UDDI** – universal description, discovery and integration – acts as an electronic directory accessible via corporate intranet or internet and allows interested parties to learn of the existence of web services.

**Baseline for software release** = Configuration management

**Reengineering** – process of updating an existing system by extracting and reusing design and program components.

**Reverse engineering** – process of taking apart an app to see how it functions; Can be done by decompiling code.

**Configuration management**: version control software and check out process. Used for software dev and for other stuff – programs, documentation, data. Change control works off of configuration mgmt.

**Logical path monitor** – reports on the sequence of steps executed by a programmer.

**Program maintenance** is facilitated by more cohesive (the performance of a single, dedicated functions by a program) and more loosely coupled (independence of the comparable units) programs.

**Structured walk through** is a management tool – it involves peer reviews to detect software errors during a program development activity.

**Benefits realization**: continuous process, business process, often includes a post implementation review PIR

**Auditor** you are not there to 'fix things' only to report on compliance

Records flow of designated transactions through logic paths within programs => **Snapshot**

**Audit Report**: should contain business objective and brief details of purpose of audit. Framework/standard used to conduct, timelines, observations, recommendations, details of residual risk; if any and conclusion of audit

Identifies specific program logic that has not been tested, and analyzes programs during execution to indicate whether program statements have been executed =>**Mapping**

**First concern** of an auditor is does the application meet business requirements; **close second** is there adequate controls in place.

**Computer Aided Software Engineering (CASE)** - Automated tools to aid in the software development process. Their use may include the application of software tools for requirements analysis, software design, code generation, testing, documentation generation. Don't guarantee that software will meet user requirements or be correct.

**Job descriptions** contain clear statements of accountability for information security, from a control perspective, job description establish responsibility and accountability

**Business Process Re-engineering**: This is the process of responding to competitive and economic pressures and customer demands to survive in a business environment; and is usually done by automating system processes so that there are fewer manual interventions and manual controls.

**Benchmarking** is a technique all about improving business process – BPR technique (PROAAI = Plan - Research – Observe – Analyze – Adopt – Improve)

**Hash totals** – verification that the total (meaningless in itself) for a predetermined numeric field (like employee number) that exists for all docs in the batch = same total calculated by system.

**Data Validation** identifies data errors, incomplete or missing data or inconsistencies among related items and edit controls are preventive controls used before data is processed. Input data should be evaluated as close to the time and point of origination as possible

**Limit check** – data should not exceed a certain predetermined limit

**Range check** – data should be within the range of predetermined values

**Reasonableness check** – input data matched to predetermined reasonable limits or occurrence rates – normally receive 20 orders, if receive 25 then that's a problem

**Table lookups** – input data compared to predetermined criteria maintained in a lookup table.☐☐

**Existence check** – data entered correctly and meet predetermined criteria – valid transaction code must be entered in the transaction code field.

**Key verification:** keying in process repeated by two different people.

**Check digit** – a numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect value submitted.

**Completeness check** – a field should always contain data and not zeros or nulls

**Logical relationship check:** if this condition is true, then one or more additional conditions or relationships may be required to be true.

**Domain integrity test** – verify that the edit and validation routines are working satisfactorily, all data items are in the correct domain.

**Redundancy check** - appends calculated bits onto the end of each segment of data to detect transmission errors) check to see if it is a redundant transmission

**Atomicity** – transaction either completed in its entirety or not at all

**Consistency** – all integrity conditions (consistent state) with each transaction – so database moves from one consistent state to another

**Isolation** – each transaction isolated from other transactions so each transaction only accesses data that are part of a consistent database state

**Snapshot** – take snapshots of data as flows through the app. Very useful as an audit trail.

**Mapping** – identifies unused code and helps identify potential exposures

**Tracing/Tagging** – shows exact picture of sequence of events – shows trail of instructions executed during application processing. Tagging involves placing a flag on selected transactions at input and using tracing to track them.

**Audit hooks** – embed hooks in app systems to function as red flags and to induce IS auditors to act before an error or irregularity gets out of hand. Useful when only select transactions need to be examined.

**CASE tools** can be broadly classed into these broader areas: Requirement Analysis Tool - Structure Analysis Tool - Software Design Tool - Code Generation Tool - Test Case Generation Tool - Document Production Tool -Reverse Engineering Tool

**SCM** is about linking the business processes between the related entities (buyer and seller). Important for just in time inventory – store does not keep inventory – stuff comes as you need it – should have multiple suppliers in case one fails or you could be in trouble.

**ITF:** involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

**SCARF/EAM** focus is on controls versus data

**Validity Check** (e.g., M = male, F = female)

**Limit Check** (e.g., hours worked do not exceed 40 hours)

**Reasonableness Check** (e.g., increase in salary is reasonable compared to base salary)

**Field Check** (e.g., numbers do not appear in fields reserved for words)

**Sequence Check** (e.g., successive input data are in some prescribed order)

**Range Check** (e.g., particular fields fall within specified ranges - pay rates for hourly employees in a firm should fall between $8 and $20)

**Relationship Check** (logically related data elements are compatible - employee rated as "hourly" gets paid at a rate within the range of $8 and $20)

**Audit Charter:** States management's responsibility, Objectives for, and delegation of authority to the, Outlines the overall authority, scope and response audit function.