GOPAS

Notes and keywords for CISM certification

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory | MVP:Enterprise Security | CEH | CHFI | CISA | CISM |
ondrej@sevecek.com | www.sevecek.com |

GOPAS: info@gopas,cz | www.gopas.cz | www.facebook.com/P.S.GOPAS

CISM exam

- 300 questions / 6 hours / 70%
- nothing around except for a pen

- 5 domains
  - Information security governance
  - Information security risk management
  - Information security program development and management
  - Information security incident management
  - Current technical controls awareness

GOPAS

Format and other notes

- [synonym/s]
- (note/s)

- Avanset VCE Player 1 month license
  - www.avanset.com
  - www.examcollection.com

- CISM Certified Information Security Manager All-in-One Exam Guide (Peter H. Gregory)
  - paperback, Kindle

GOPAS

Security

- Confidentiality
- Integrity

  vs.
- Availability

- information, operations, ...
- electronic, paper, spoken etc.

GOPAS

Owners

- risk owner
  - approves the treatment plan and accepts the residual risks
  - those who can do something about the risk
- data owners
  - data owner
    - responsibility and authority
  - data custodian
    - the IT guy
  - data steward
    - knows the business data, responsible for their quality and whether the data are fit for the purpose (the BI guys, GDPR data protection officer)
  - data architect
    - based on input from data steward produces designs
- process owner
- technical asset owner
- business asset owner
- project sponsor
  - the one who signs-off (approves) on the project and its phases

GOPAS

Recovery sites

- cold site (longest time, cheapest)
  - just a space reserved, no equipment
- warm site
  - equipment ready, just bring-in the backups
  - bare-metal restore
- hot site (shortest time, most expensive)
  - everything running in parallel at any particular time
  - regional clusters, (a)synchronous data replication, ...
- redundant site
- reciprocal arrangement/agreement
  - warm sites only

GOPAS

Testing

- Unit testing
  - individual modules of the whole solution
  - code, practices/procedures, hardware, equipment
  - who: software developer
- Integration testing [I&T]
  - group of unit-tested modules
  - who: software developer
- System testing
  - overall testing without knowledge of the internals [black-box testing]
  - who: software developer + customer
- Acceptance testing
  - top level user needs, business processes, requirements
  - who: customer

GOPAS

Security evaluation and testing

- Ethical hacker = white-hat hacker
- Black-hat hacker

- Black-box pentest
  - ethical hackers only :-)
- White-box [clear-box, glass-box] pentest
  - may find unrealistic intrusions

GOPAS

Risks

- inherent
  - the natural risks if no controls or other mitigating factors were in place
- residual
  - the risks remaining after remediation has been applied

- control risk
  - the potential of a control to fail
- audit risk
  - measure of audit/review tendency to fail to detect problems

GOPAS

Risks

- Environmental threats
  - storms, earth movement, flooding, fire, disease
- Labor
- Violence
- Malware
- Hacking attack
- Hardware failures
- Software failures
- Utilities
- Transportation
- Hazardous materials
- Criminal
- Errors

GOPAS

Risk treatment/mitigation

- treat, remediate, mitigate and minimize
  - using controls
- transfer
  - insurance
  - contract to share/assume liability [hold-harmless, save-harmless, indemnity]
- accept residuum
- terminate/avoid

- cost/benefit analysis [CBA/BCA]
  - benefit-cost ration [BCR]

GOPAS

Quantitative risk analysis

- Asset value
  - server
  - customer's buying behavior data
  - radio internet connection
- Exposure factor
  - percentage of asset value if a threat realizes
- Single loss expectancy [SLE]
- Annualized rate of occurrence [ARO]
- Annualized loss expectancy
  - SLE x ARO

- Can history be used?

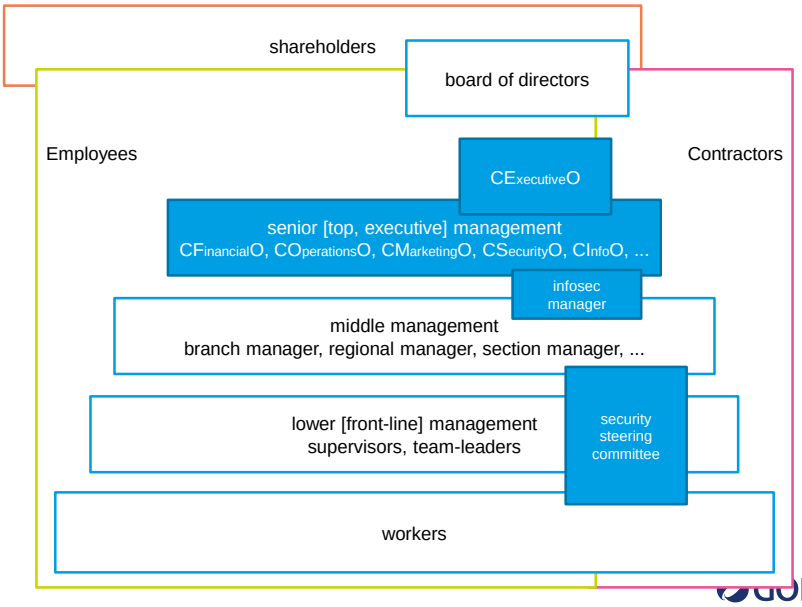
GOPAS

Roles

- stock owner [shareholder]
- stakeholder
  - anybody interested in the organization
  - employees, management, government, customers, creditors, trade unions, owners, investors, suppliers
- board of directors
  - CEO might act as inside chairman [director]
  - or the company may employ outside [independent] chairman [director]
- management
  - senior [executive, top, upper, higher] management = authorize budget spending
  - middle management = communicate strategy and direction to lower management
  - lower [front-line] management = supervisors, team-leaders
- contractor
- (security) steering committee
  - high-level stakeholders + experts + CISO
  - provides guidance to top management
- (chief) information security manager [officer]
- incident response team
  - security event => security incident
- normal user
  - person who interacts with a system, typically through an interface, to extract some functional benefit
- system user
  - normal user with some special responsibilities, such as testers
  - password policies often do not require password expiration

GOPAS

Organizational structure



GOPAS

First rule governance

- Top management full support and dedication

GOPAS

First rule of independence

- Lower level send requirements up
  - any requirements
  - access requests
- Manager decides and approves
- Infosec manager monitors and recommends
- Worker implements
- Auditor controls

GOPAS

Steering committee

GOPAS

Framework and its relations

- security strategy
  - overall direction, not always currently implemented or currently possible
- security policy
  - currently enforced
  - what should be done
  - but not how it should be done
    - roles and responsibilities
    - development practices and change management
    - operational practices (+ service desk, backups, monitoring)
    - other processes and documents (incidents, projects, vulnerability, support, data storage)
    - acceptable use
    - privacy policy
- security standard
  - technology, protocol, suppliers, methodology, configuration, architecture, ...
  - "standard document editor", "standard contractor NDA agreement", "standard firewall config blocks all with exceptions", ...
- security procedure
- security governance
  - no security without governance
  - no nothing without governance
- corporate strategy
- business strategy

GOPAS

Rule of responsibilities and authority

- Top management is responsible and has the eternal authority
  - can delegate, but must delegate explicitly
  - approve/sponsor
- Infosec manager (coordinator)
  - report
  - assess
  - recommend
  - oversee
  - justify
  - investigate
  - directly managing incident response team
- Anybody else
  - plan
  - design
  - implement
  - implement
  - monitor
  - (pen)test
  - respond to incidents and exceptions
  - behave
  - report

GOPAS

Detection or errors

- False negative/rejection [FRR, Type 1]
- False positive/acceptance [FAR, Type 2]
- Crossover [equal] error rate [CER]
  - the level to tune any security control to
- Biometrics quality in decreasing order of CER
  - iris, retina, fingerprint, hand geometry, voice pattern, keystroke pattern, signature
  - (Zephyr Chart)
- Biometrics in decreasing order of user acceptance
  - voice, keystroke, signature, hand geometry, hand print, fingerprint, iris, retina

GOPAS

Rules of incident response

- Ensure personal safety
- Report to management
- ...
- ...
- ...
- Act
- Evaluate
- Improve

GOPAS

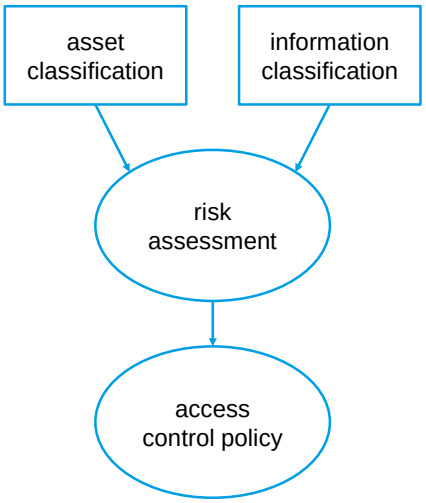
Continuity = availability

- business continuity planning
- business impact analysis
- recovery time objective [RTO]
  - time until normal operation
  - disaster tolerance
  - acceptable interruption window (until operation even if partial) <= RTO
  - lower DT = shorter AIW
- recovery point objective [RPO]

- backup strategy
  - frequency, amount, types (full, incremental, differential)
- disaster recovery strategy

GOPAS

Classifications



GOPAS

Planning

- SWOT analysis [strengths, weaknesses, opportunities, threats]
- balanced scorecard [BSC]
  - report (using SWOT) used by management => strategy
  - vision statement + strategic objectives + monitoring measures
- standard IT balanced scorecard
  - business contribution as seen from non-IT executives position
  - end-user satisfaction with systems and support
  - operational excellence - number of support cases, unscheduled downtime, problems reported
  - innovation and training
- digital dashboard = business dashboard = enterprise dashboard = executive dashboard
- management cockpit
- desk exercise

GOPAS

Review

- key performance indicator [KPI]
- key recovery indicator

GOPAS

SDLC [Software development life cycle]

1. Initiation
   - market conditions, costs, regulation, change in risks, customer requirements
2. Feasibility study
3. Requirements definition
4. Design and specification
5. Development
6. Testing
7. Implementation
8. Post-implementation

GOPAS

Rule of essential and cheapest solution

- Employee awareness training

GOPAS

Other terms

- Business record
  - legally required documents
  - employment contracts, accounting source documents, minutes, internal memoranda, other legal documents
- Business case
  - reasoning for initiating a project or a task
- TCO [total cost of ownership]
- Baseline comparison
  - comparison (cost, measurement, etc.) with other companies or industries or with historical experience
- Opportunity cost
  - = the cost :-)
- Retrofitting
  - adding something where it was not before

GOPAS

Access Control

- Discretionary Access Control [DAC]
  - per-object permissions applied to individual/groups of subjects
  - access based on identity
- Mandatory Access Control [MAC]
  - security levels applied to subjects and rules that define the leveled access to objects, or just a single level for each object
  - access based on level
- Role-based Access Control [RBAC]
  - "groups" used by both DAC or MAC
  - static separation of duties
    - subject cannot be member of two conflicting roles/groups (admin/auditor, invoicing/payments, ...)
  - dynamic separation of duties
    - subject can be member of two conflicting roles, but must not do the conflicting operations (cannot audit own administrative configurations, cannot issue payments for invoices he approves)
- Dual control
  - two operators are needed to do the task
- Two-men control
  - two operators each verify and approve the other one's tasks

GOPAS

Sample questions

Notes and keywords for CISM certification

GOPAS

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- A. Historical cost of the asset
- B. Acceptable level of potential business impacts
- C. Cost versus benefit of additional mitigating controls
- D. Annualized loss expectancy (ALE)

GOPAS

For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

- A. Biometrics
- B. Symmetric encryption keys
- C. Secure Sockets Layer (SSL)-based authentication
- D. Two-factor authentication

GOPAS

Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

- A. are compatible with the provider's own classification.
- B. are communicated to the provider.
- C. exceed those of the outsourcer.
- D. are stated in the contract.

GOPAS

Risk acceptance is a component of which of the following?

- A. Assessment
- B. Mitigation
- C. Evaluation
- D. Monitoring

GOPAS

The MOST important function of a risk management program is to:

- A. quantify overall risk.
- B. minimize residual risk.
- C. eliminate inherent risk.
- D. maximize the sum of all annualized loss expectancies (ALEs).

GOPAS

Which of the following are seldom changed in response to technological changes?

- A. Standards
- B. Procedures
- C. Policies
- D. Guidelines

GOPAS

Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

- A. The program's governance oversight mechanisms
- B. Information security periodicals and manuals
- C. The program's security architecture and design
- D. Training and certification of the information security team

GOPAS

Which of the following is the BEST justification to convince management to invest in an information security program?

- A. Cost reduction
- B. Compliance with company policies
- C. Protection of business assets
- D. Increased business value

GOPAS

Which of the following is the MOST important factor when designing information security architecture?

- A. Technical platform interfaces
- B. Scalability of the network
- C. Development methodologies
- D. Stakeholder requirements

GOPAS

In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

- A. develop an operational plan for achieving compliance with the legislation.
- B. identify systems and processes that contain privacy components.
- C. restrict the collection of personal information until compliant.
- D. identify privacy legislation in other countries that may contain similar requirements.

GOPAS

An extranet server should be placed:

- A. outside the firewall.
- B. on the firewall server.
- C. on a screened subnet.
- D. on the external router.

GOPAS

Which of the following has the highest priority when defining an emergency response plan?

- A. Critical data
- B. Critical infrastructure
- C. Safety of personnel
- D. Vital records

GOPAS

Retention of business records should PRIMARILY be based on:

- A. business strategy and direction.
- B. regulatory and legal requirements.
- C. storage capacity and longevity.
- D. business ease and value analysis.

GOPAS

In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

- A. volume of sensitive data.
- B. recovery point objective (RPO).
- C. recovery time objective (RTO).
- D. interruption window.

GOPAS

Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

- A. The number of false positives increases
- B. The number of false negatives increases
- C. Active probing is missed
- D. Attack profiles are ignored

GOPAS

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

- A. Ethics
- B. Proportionality
- C. Integration
- D. Accountability

GOPAS

Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

- A. removed into the custody of law enforcement investigators.
- B. kept in the tape library pending further analysis.
- C. sealed in a signed envelope and locked in a safe under dual control.
- D. handed over to authorized independent investigators.

GOPAS

There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

- A. Black box pen test
- B. Security audit
- C. Source code review
- D. Vulnerability scan

GOPAS

In business-critical applications, user access should be approved by the:

- A. information security manager.
- B. data owner.
- C. data custodian.
- D. business management.

GOPAS

Which of the following would be the BEST metric for the IT risk management process?

- A. Number of risk management action plans
- B. Percentage of critical assets with budgeted remedial
- C. Percentage of unresolved risk exposures
- D. Number of security incidents identified

GOPAS

An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

- A. perform a comprehensive assessment of the organization's exposure to the hacker's techniques.
- B. initiate awareness training to counter social engineering.
- C. immediately advise senior management of the elevated risk.
- D. increase monitoring activities to provide early detection of intrusion.

GOPAS

When a significant security breach occurs, what should be reported FIRST to senior management?

- A. A summary of the security logs that illustrates the sequence of events
- B. An explanation of the incident and corrective action taken
- C. An analysis of the impact of similar attacks at other organizations
- D. A business case for implementing stronger logical access controls

GOPAS

Which of the following should be included in an annual information security budget that is submitted for management approval?

- A. A cost-benefit analysis of budgeted resources
- B. All of the resources that are recommended by the business
- C. Total cost of ownership (TCO)
- D. Baseline comparisons

GOPAS

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- A. Prevent the system from being accessed remotely
- B. Create a strong random password
- C. Ask for a vendor patch
- D. Track usage of the account by audit trails

GOPAS

Priority should be given to which of the following to ensure effective implementation of information security governance?

- A. Consultation
- B. Negotiation
- C. Facilitation
- D. Planning

GOPAS

Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

- A. Baseline security standards
- B. System access violation logs
- C. Role-based access controls
- D. Exit routines

GOPAS

Senior management commitment and support for information security can BEST be enhanced through:

- A. a formal security policy sponsored by the chief executive officer (CEO).
- B. regular security awareness training for employees.
- C. periodic review of alignment with business management goals.
- D. senior management signoff on the information security strategy.

GOPAS

What is the BEST defense against a Structured Query Language (SQL) injection attack?

- A. Regularly updated signature files
- B. A properly configured firewall
- C. An intrusion detection system
- D. Strict controls on input fields

GOPAS

Isolation and containment measures for a compromised computer have been taken and information security management is now investigating. What is the MOST appropriate next step?

- A. Run a forensics tool on the machine to gather evidence
- B. Reboot the machine to break remote connections
- C. Make a copy of the whole system's memory
- D. Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/ IDP) ports

GOPAS

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

- A. revise the information security program.
- B. evaluate a balanced business scorecard.
- C. conduct regular user awareness sessions.
- D. perform penetration tests.

GOPAS

Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

- A. The information security department has difficulty filling vacancies.
- B. The chief information officer (CIO) approves security policy changes.
- C. The information security oversight committee only meets quarterly.
- D. The data center manager has final signoff on all security projects.

GOPAS

Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

- A. Programming
- B. Specification
- C. User testing
- D. Feasibility

GOPAS

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

- A. Symmetric cryptography
- B. Public key infrastructure (PKI)
- C. Message hashing
- D. Message authentication code

GOPAS

Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

- A. Obtain the support of the board of directors.
- B. Improve the content of the information security awareness program.
- C. Improve the employees' knowledge of security policies.
- D. Implement logical access controls to the information systems.

GOPAS

A digital signature using a public key infrastructure (PKI) will:

- A. not ensure the integrity of a message.
- B. rely on the extent to which the certificate authority (CA) is trusted.
- C. require two parties to the message exchange.
- D. provide a high level of confidentiality.

GOPAS

What is the MOST appropriate change management procedure for the handling of emergency program changes?

- A. Formal documentation does not need to be completed before the change
- B. Business management approval must be obtained prior to the change
- C. Documentation is completed with approval soon after the change
- D. All changes must follow the same process

GOPAS

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- A. ensure the provider is made liable for losses.
- B. recommend not renewing the contract upon expiration.
- C. recommend the immediate termination of the contract.
- D. determine the current level of security.

GOPAS

The cost of implementing a security control should not exceed the:

- A. annualized loss expectancy.
- B. cost of an incident.
- C. asset value.
- D. implementation opportunity costs.

GOPAS

The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

- A. uses multiple redirects for completing a data commit transaction.
- B. has implemented cookies as the sole authentication mechanism.
- C. has been installed with a non-1egitimate license key.
- D. is hosted on a server along with other applications.

GOPAS

It is MOST important that information security architecture be aligned with which of the following?

- A. Industry best practices
- B. Information technology plans
- C. Information security best practices
- D. Business objectives and goals

GOPAS

Access control to a sensitive intranet application by mobile users can BEST be implemented through:

- A. data encryption.
- B. digital signatures.
- C. strong passwords.
- D. two-factor authentication.

GOPAS

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- A. a strong authentication.
- B. IP antispoofing filtering.
- C. network encryption protocol.
- D. access lists of trusted devices.

GOPAS

Which of the following is generally considered a fundamental component of an information security program?

- A. Role-based access control systems
- B. Automated access provisioning
- C. Security awareness training
- D. Intrusion prevention systems (IPSs)

GOPAS

In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

- A. Procedural design
- B. Architectural design
- C. System design specifications
- D. Software development

GOPAS

When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

- A. services delivery objective.
- B. recovery time objective (RTO).
- C. recovery window.
- D. maximum tolerable outage (MTO).

GOPAS

The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

- A. return on investment (ROD.
- B. a vulnerability assessment.
- C. annual loss expectancy (ALE).
- D. a business case.

GOPAS

Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

- A. Security policies and procedures
- B. Annual self-assessment by management
- C. Security- steering committees
- D. Security awareness campaigns

GOPAS

When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

- A. Business management
- B. Operations manager
- C. Information security manager
- D. System users

GOPAS

Which of the following would present the GREATEST risk to information security?

- A. Virus signature files updates are applied to all servers every day
- B. Security access logs are reviewed within five business days
- C. Critical patches are applied within 24 hours of their release
- D. Security incidents are investigated within five business days

GOPAS

The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

- A. the existence of messages is unknown.
- B. required key sizes are smaller.
- C. traffic cannot be sniffed.
- D. reliability of the data is higher in transit.

GOPAS

The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

- A. the existence of messages is unknown.
- B. required key sizes are smaller.
- C. traffic cannot be sniffed.
- D. reliability of the data is higher in transit.

GOPAS

The implementation of continuous monitoring controls is the BEST option where:

- A. incidents may have a high impact and frequency
- B. legislation requires strong information security controls
- C. incidents may have a high impact but low frequency
- D. Electronic commerce is a primary business driver

GOPAS

Detailed business continuity plans should be based PRIMARILY on:

- A. consideration of different alternatives.
- B. the solution that is least expensive.
- C. strategies that cover all applications.
- D. strategies validated by senior management.

GOPAS

Which of the following would help to change an organization's security culture?

- A. Develop procedures to enforce the information security policy
- B. Obtain strong management support
- C. Implement strict technical security controls
- D. Periodically audit compliance with the information security policy

GOPAS

What is the MOS T cost-effective means of improving security awareness of staff personnel?

- A. Employee monetary incentives
- B. User education and training
- C. A zero-tolerance security policy
- D. Reporting of security infractions

GOPAS

The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

- A. enable independent and objective review of the root cause of the incidents.
- B. obtain support for enhancing the expertise of the third-party teams.
- C. identify lessons learned for further improving the information security management process.
- D. obtain better buy-in for the information security program.

GOPAS

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

- A. end users.
- B. legal counsel.
- C. operational units.
- D. audit management.

GOPAS

An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

- A. Key performance indicators (KPIs)
- B. Business impact analysis (BIA)
- C. Gap analysis
- D. Technical vulnerability assessment

GOPAS

Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

- A. Number of attacks detected
- B. Number of successful attacks
- C. Ratio of false positives to false negatives
- D. Ratio of successful to unsuccessful attacks

GOPAS

What is the MOST important element to include when developing user security awareness material?

- A. Information regarding social engineering
- B. Detailed security policies
- C. Senior management endorsement
- D. Easy-to-read and compelling information

GOPAS

Information security managers should use risk assessment techniques to:

- A. justify selection of risk mitigation strategies.
- B. maximize the return on investment (ROD.
- C. provide documentation for auditors and regulators.
- D. quantify risks that would otherwise be subjective.

GOPAS

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

- A. Access control policy
- B. Data classification policy
- C. Encryption standards
- D. Acceptable use policy

GOPAS

Which of the following roles would represent a conflict of interest for an information security manager?

- A. Evaluation of third parties requesting connectivity
- B. Assessment of the adequacy of disaster recovery plans
- C. Final approval of information security policies
- D. Monitoring adherence to physical security controls

GOPAS

From an information security manager perspective, what is the immediate benefit of clearly- defined roles and responsibilities?

- A. Enhanced policy compliance
- B. Improved procedure flows
- C. Segregation of duties
- D. Better accountability

GOPAS

Which of the following is a key area of the ISO 27001 framework?

- A. Operational risk assessment
- B. Financial crime metrics
- C. Capacity management
- D. Business continuity management

GOPAS

Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does il always introduce?

- A. Remote buffer overflow
- B. Cross site scripting
- C. Clear text authentication
- D. Man-in-the-middle attack

GOPAS

Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

- A. Tuning
- B. Patching
- C. Encryption
- D. Packet filtering

GOPAS

An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

- A. corporate data privacy policy.
- B. data privacy policy where data are collected.
- C. data privacy policy of the headquarters' country.
- D. data privacy directive applicable globally.

GOPAS

A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

- A. Risk assessment results
- B. Severity criteria
- C. Emergency call tree directory
- D. Table of critical backup files

GOPAS

The PRIMARY objective of a risk management program is to:

- A. minimize inherent risk.
- B. eliminate business risk.
- C. implement effective controls.
- D. minimize residual risk.

GOPAS

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- A. Business impact analyses
- B. Security gap analyses
- C. System performance metrics
- D. Incident response processes

GOPAS

What is the MOST cost-effective method of identifying new vendor vulnerabilities?

- A. External vulnerability reporting sources
- B. Periodic vulnerability assessments performed by consultants
- C. Intrusion prevention software
- D. honey pots located in the DMZ

GOPAS

Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

- A. Manager
- B. Custodian
- C. User
- D. Owner

GOPAS

Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

- A. Implement countermeasures.
- B. Eliminate the risk.
- C. Transfer the risk.
- D. Accept the risk.

GOPAS