

# Exam Questions CISM

Certified Information Security Manager

<https://www.2passeasy.com/dumps/CISM/>



#### NEW QUESTION 1

Which of the following is responsible for legal and regulatory liability?

- A. Chief security officer (CSO)
- B. Chief legal counsel (CLC)
- C. Board and senior management
- D. Information security steering group

**Answer: C**

#### Explanation:

The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

#### NEW QUESTION 2

When an organization is implementing an information security governance program, its board of directors should be responsible for:

- A. drafting information security policie
- B. reviewing training and awareness program
- C. setting the strategic direction of the progra
- D. auditing for complianc

**Answer: C**

#### Explanation:

A board of directors should establish the strategic direction of the program to ensure that it is in sync with the company's vision and business goals. The board must incorporate the governance program into the overall corporate business strategy. Drafting information security policies is best fulfilled by someone such as a security manager with the expertise to bring balance, scope and focus to the policies. Reviewing training and awareness programs may best be handled by security management and training staff to ensure that the training is on point and follows best practices. Auditing for compliance is best left to the internal and external auditors to provide an objective review of the program and how it meets regulatory and statutory compliance.

#### NEW QUESTION 3

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

**Answer: D**

#### Explanation:

Without well-defined roles and responsibilities, there cannot be accountability. Choice A is incorrect because policy compliance requires adequately defined accountability first and therefore is a byproduct. Choice B is incorrect because people can be assigned to execute procedures that are not well designed. Choice C is incorrect because segregation of duties is not automatic, and roles may still include conflicting duties.

#### NEW QUESTION 4

When a security standard conflicts with a business objective, the situation should be resolved by:

- A. changing the security standar
- B. changing the business objectiv
- C. performing a risk analysi
- D. authorizing a risk acceptanc

**Answer: C**

#### Explanation:

Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. It is highly improbable that a business objective could be changed to accommodate a security standard, while risk acceptance\* is a process that derives from the risk analysis.

#### NEW QUESTION 5

Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

- A. Continuous analysis, monitoring and feedback
- B. Continuous monitoring of the return on security investment (ROSD)
- C. Continuous risk reduction
- D. Key risk indicator (KRD) setup to security management processes

**Answer: A**

#### Explanation:

To improve the governance framework and achieve a higher level of maturity, an organization needs to conduct continuous analysis, monitoring and feedback compared to the current state of maturity. Return on security investment (ROSI) may show the performance result of the security-related activities; however, the result is interpreted in terms of money and extends to multiple facets of security initiatives. Thus, it may not be an adequate option. Continuous risk reduction would demonstrate the effectiveness of the security governance framework, but does not indicate a higher level of maturity. Key risk indicator (KRI) setup is a tool to be used in internal control assessment. KRI setup presents a threshold to alert management when controls are being compromised in business processes. This is a control tool rather than a maturity model support tool.

#### NEW QUESTION 6

Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

- A. The security officer
- B. Senior management
- C. The end user
- D. The custodian

**Answer:** B

#### Explanation:

Routine administration of all aspects of security is delegated, but top management must retain overall responsibility. The security officer supports and implements information security for senior management. The end user does not perform categorization. The custodian supports and implements information security measures as directed.

#### NEW QUESTION 7

The MOST complete business case for security solutions is one that.

- A. includes appropriate justification
- B. explains the current risk profile
- C. details regulatory requirement
- D. identifies incidents and losses

**Answer:** A

#### Explanation:

Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

#### NEW QUESTION 8

Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

- A. organizational risk
- B. organization-wide metric
- C. security need
- D. the responsibilities of organizational unit

**Answer:** A

#### Explanation:

Information security exists to help the organization meet its objectives. The information security manager should identify information security needs based on organizational needs. Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior management after the overall organizational risk is identified.

#### NEW QUESTION 9

Which of the following is a benefit of information security governance?

- A. Reduction of the potential for civil or legal liability
- B. Questioning trust in vendor relationships
- C. Increasing the risk of decisions based on incomplete management information
- D. Direct involvement of senior management in developing control processes

**Answer:** A

#### Explanation:

Information security governance decreases the risk of civil or legal liability. The remaining answers are incorrect. Option D appears to be correct, but senior management would provide oversight and approval as opposed to direct involvement in developing control processes.

#### NEW QUESTION 10

What will have the HIGHEST impact on standard information security governance models?

- A. Number of employees
- B. Distance between physical locations
- C. Complexity of organizational structure
- D. Organizational budget

**Answer:** C

**Explanation:**

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance. Organizational budget is not a major impact once good governance models are in place, hence governance will help in effective management of the organization's budget.

#### NEW QUESTION 10

Senior management commitment and support for information security can BEST be obtained through presentations that:

- A. use illustrative examples of successful attack
- B. explain the technical risks to the organization
- C. evaluate the organization against best security practice
- D. tie security risks to key business objective

**Answer:** D

**Explanation:**

Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they are presented in terms of key business objectives.

#### NEW QUESTION 11

How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

- A. Give organization standards preference over local regulations
- B. Follow local regulations only
- C. Make the organization aware of those standards where local regulations causes conflicts
- D. Negotiate a local version of the organization standards

**Answer:** D

**Explanation:**

Adherence to local regulations must always be the priority. Not following local regulations can prove detrimental to the group organization. Following local regulations only is incorrect since there needs to be some recognition of organization requirements. Making an organization aware of standards is a sensible step, but is not a total solution. Negotiating a local version of the organization standards is the most effective compromise in this situation.

#### NEW QUESTION 13

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- A. establishing a periodic risk assessment
- B. promoting regulatory requirement
- C. developing a business case
- D. developing effective metric

**Answer:** C

**Explanation:**

Business case development, including a cost-benefit analysis, will be most persuasive to management. A risk assessment may be included in the business case, but by itself will not be as effective in gaining management support. Informing management of regulatory requirements may help gain support for initiatives, but given that more than half of all organizations are not in compliance with regulations, it is unlikely to be sufficient in many cases. Good metrics which provide assurance that initiatives are meeting organizational goals will also be useful, but are insufficient in gaining management support.

#### NEW QUESTION 18

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

- A. Examples of genuine incidents at similar organizations
- B. Statement of generally accepted best practices
- C. Associating realistic threats to corporate objectives
- D. Analysis of current technological exposures

**Answer:** C

**Explanation:**

Linking realistic threats to key business objectives will direct executive attention to them. All other options are supportive but not of as great a value as choice C when trying to obtain the funds for a new program.

#### NEW QUESTION 19

Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

- A. baselin
- B. strateg
- C. procedur
- D. polic

**Answer:** D

#### Explanation:

A policy is a high-level statement of an organization's beliefs, goals, roles and objectives. Baselines assume a minimum security level throughout an organization. The information security strategy aligns the information security program with business objectives rather than making control statements. A procedure is a step-by-step process of how policy and standards will be implemented.

#### NEW QUESTION 22

Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

- A. Update platform-level security settings
- B. Conduct disaster recovery test exercises
- C. Approve access to critical financial systems
- D. Develop an information security strategy paper

**Answer:** D

#### Explanation:

Developing a strategy paper on information security would be the most appropriate. Approving access would be the job of the data owner. Updating platform-level security and conducting recovery test exercises would be less essential since these are administrative tasks.

#### NEW QUESTION 25

Which of the following is MOST important in developing a security strategy?

- A. Creating a positive business security environment
- B. Understanding key business objectives
- C. Having a reporting line to senior management
- D. Allocating sufficient resources to information security

**Answer:** B

#### Explanation:

Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

#### NEW QUESTION 28

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

**Answer:** D

#### Explanation:

Investing in an information security program should increase business value and confidence. Cost reduction by itself is rarely the motivator for implementing an information security program. Compliance is secondary to business value. Increasing business value may include protection of business assets.

#### NEW QUESTION 32

Which of the following should be the FIRST step in developing an information security plan?

- A. Perform a technical vulnerabilities assessment
- B. Analyze the current business strategy
- C. Perform a business impact analysis
- D. Assess the current levels of security awareness

**Answer:** B

#### Explanation:

Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.



#### NEW QUESTION 34

Logging is an example of which type of defense against systems compromise?

- A. Containment
- B. Detection
- C. Reaction
- D. Recovery

**Answer: B**

#### Explanation:

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

#### NEW QUESTION 36

Which of the following situations would MOST inhibit the effective implementation of security governance:

- A. The complexity of technology
- B. Budgetary constraints
- C. Conflicting business priorities
- D. High-level sponsorship

**Answer: D**

#### Explanation:

The need for senior management involvement and support is a key success factor for the implementation of appropriate security governance. Complexity of technology, budgetary constraints and conflicting business priorities are realities that should be factored into the governance model of the organization, and should not be regarded as inhibitors.

#### NEW QUESTION 39

Which of the following requirements would have the lowest level of priority in information security?

- A. Technical
- B. Regulatory
- C. Privacy
- D. Business

**Answer: A**

#### Explanation:

Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

#### NEW QUESTION 41

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 employee
- C. periodic review of alignment with business management goal
- D. senior management signoff on the information security strateg

**Answer: C**

#### Explanation:

Ensuring that security activities continue to be aligned and support business goals is critical to obtaining their support. Although having the chief executive officer (CEO) signoff on the security policy and senior management signoff on the security strategy makes for good visibility and demonstrates good tone at the top, it is a one-time discrete event that may be quickly forgotten by senior management. Security awareness training for employees will not have as much effect on senior management commitment.

#### NEW QUESTION 43

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

- A. return on investment (RO
- B. a vulnerability assessmen
- C. annual loss expectancy (ALE).
- D. a business cas

**Answer: D**

#### Explanation:

A business case shows both direct and indirect benefits, along with the investment required and the expected returns, thus making it useful to present to senior

management. Return on investment (ROD) would only provide the costs needed to preclude specific risks, and would not provide other indirect benefits such as process improvement and learning. A vulnerability assessment is more technical in nature and would only identify and assess the vulnerabilities. This would also not provide insights on indirect benefits. Annual loss expectancy (ALE) would not weigh the advantages of implementing single sign-on (SSO) in comparison to the cost of implementation.

#### NEW QUESTION 45

Acceptable risk is achieved when:

- A. residual risk is minimize
- B. transferred risk is minimize
- C. control risk is minimize
- D. inherent risk is minimize

**Answer:** A

#### Explanation:

Residual risk is the risk that remains after putting into place an effective risk management program; therefore, acceptable risk is achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party and may not necessarily be equal to the minimal form of residual risk. Control risk is the risk that controls may not prevent/detect an incident with a measure of control effectiveness. Inherent risk cannot be minimized.

#### NEW QUESTION 47

After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

- A. Senior management
- B. Business manager
- C. IT audit manager
- D. Information security officer (ISO)

**Answer:** B

#### Explanation:

The business manager will be in the best position, based on the risk assessment and mitigation proposals, to decide which controls should/could be implemented, in line with the business strategy and with budget. Senior management will have to ensure that the business manager has a clear understanding of the risk assessed but in no case will be in a position to decide on specific controls. The IT audit manager will take part in the process to identify threats and vulnerabilities, and to make recommendations for mitigations. The information security officer (ISO) could make some decisions regarding implementation of controls. However, the business manager will have a broader business view and full control over the budget and, therefore, will be in a better position to make strategic decisions.

#### NEW QUESTION 51

To determine the selection of controls required to meet business objectives, an information security manager should:

- A. prioritize the use of role-based access control
- B. focus on key control
- C. restrict controls to only critical application
- D. focus on automated control

**Answer:** B

#### Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

#### NEW QUESTION 55

One way to determine control effectiveness is by determining:

- A. whether it is preventive, detective or compensator
- B. the capability of providing notification of failure
- C. the test results of intended objective
- D. the evaluation and analysis of reliability

**Answer:** C

#### Explanation:

Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

#### NEW QUESTION 59

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- A. Recover)' time objective (RTO)
- B. Maximum tolerable outage (MTO)
- C. Recovery point objectives (RPOs)
- D. Services delivery objectives (SDOs)

**Answer:** A

**Explanation:**

Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

#### NEW QUESTION 63

All risk management activities are PRIMARILY designed to reduce impacts to:

- A. a level defined by the security manage
- B. an acceptable level based on organizational risk toleranc
- C. a minimum level consistent with regulatory requirement
- D. the minimum level possibl

**Answer:** B

**Explanation:**

The aim of risk management is to reduce impacts to an acceptable level. "Acceptable" or "reasonable" are relative terms that can vary based on environment and circumstances. A minimum level that is consistent with regulatory requirements may not be consistent with business objectives, and regulators typically do not assign risk levels. The minimum level possible may not be aligned with business requirements.

#### NEW QUESTION 68

The BEST strategy for risk management is to:

- A. achieve a balance between risk and organizational goal
- B. reduce risk to an acceptable leve
- C. ensure that policy development properly considers organizational risk
- D. ensure that all unmitigated risks are accepted by managemen

**Answer:** B

**Explanation:**

The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to l>e considered a strategy.

#### NEW QUESTION 70

Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

- A. Disclosure of personal information
- B. Sufficient coverage of the insurance policy for accidental losses
- C. Intrinsic value of the data stored on the equipment
- D. Replacement cost of the equipment

**Answer:** C

**Explanation:**

When mobile equipment is lost or stolen, the information contained on the equipment matters most in determining the impact of the loss. The more sensitive the information, the greater the liability. If staff carries mobile equipment for business purposes, an organization must develop a clear policy as to what information should be kept on the equipment and for what purpose. Personal information is not defined in the question as the data that were lost. Insurance may be a relatively smaller issue as compared with information theft or opportunity loss, although insurance is also an important factor for a successful business. Cost of equipment would be a less important issue as compared with other choices.

#### NEW QUESTION 71

An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

- A. threa
- B. los
- C. vulnerabilit
- D. probabilit

**Answer:** C

**Explanation:**

Implementing more restrictive preventive controls mitigates vulnerabilities but not the threats. Losses and probability of occurrence may not be primarily or directly affected.

#### NEW QUESTION 76



A risk management program would be expected to:

- A. remove all inherent risk
- B. maintain residual risk at an acceptable level
- C. implement preventive controls for every threat
- D. reduce control risk to zero

**Answer: B**

**Explanation:**

The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

#### NEW QUESTION 78

When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

- A. the information security steering committee
- B. customers who may be impacted
- C. data owners who may be impacted
- D. regulatory agencies overseeing privacy

**Answer: C**

**Explanation:**

The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

#### NEW QUESTION 82

A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

- A. Understand the business requirements of the developer portal
- B. Perform a vulnerability assessment of the developer portal
- C. Install an intrusion detection system (IDS)
- D. Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

**Answer: A**

**Explanation:**

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

#### NEW QUESTION 84

Which of the following is the PRIMARY reason for implementing a risk management program?

- A. Allows the organization to eliminate risk
- B. Is a necessary part of management's due diligence
- C. Satisfies audit and regulatory requirements
- D. Assists in incrementing the return on investment (ROI)

**Answer: B**

**Explanation:**

The key reason for performing risk management is that it is part of management's due diligence. The elimination of all risk is not possible. Satisfying audit and regulatory requirements is of secondary importance. A risk management program may or may not increase the return on investment (ROI).

#### NEW QUESTION 86

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 technique
- 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

**Answer: C**

**Explanation:**

Information about possible significant new risks from credible sources should be provided to management along with advice on steps that need to be taken to counter the threat. The security manager should assess the risk, but senior management should be immediately advised. It may be prudent to initiate an

awareness campaign subsequent to sounding the alarm if awareness training is not current. Monitoring activities should also be increased.

#### NEW QUESTION 90

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

**Answer: C**

#### Explanation:

Gap analysis would help identify the actual gaps between the desired state and the current implementation of information security management. BIA is primarily used for business continuity planning. Technical vulnerability assessment is used for detailed assessment of technical controls, which would come later in the process and would not provide complete information in order to identify gaps.

#### NEW QUESTION 92

The recovery time objective (RTO) is reached at which of the following milestones?

- A. Disaster declaration
- B. Recovery of the backups
- C. Restoration of the system
- D. Return to business as usual processing

**Answer: C**

#### Explanation:

The recovery time objective (RTO) is based on the amount of time required to restore a system; disaster declaration occurs at the beginning of this period. Recovery of the backups occurs shortly after the beginning of this period. Return to business as usual processing occurs significantly later than the RTO. RTO is an "objective," and full restoration may or may not coincide with the RTO. RTO can be the minimum acceptable operational level, far short of normal operations.

#### NEW QUESTION 93

The MOST important reason for conducting periodic risk assessments is because:

- A. risk assessments are not always precis
- B. security risks are subject to frequent chang
- C. reviewers can optimize and reduce the cost of control
- D. it demonstrates to senior management that the security function can add valu

**Answer: B**

#### Explanation:

Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

#### NEW QUESTION 96

After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

- A. transferre
- B. treate
- C. accepte
- D. terminate

**Answer: C**

#### Explanation:

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.

#### NEW QUESTION 100

It is important to classify and determine relative sensitivity of assets to ensure that:

- A. cost of protection is in proportion to sensitivit
- B. highly sensitive assets are protecte
- C. cost of controls is minimize
- D. countermeasures are proportional to ris

**Answer: D**

**Explanation:**

Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

**NEW QUESTION 104**

A risk analysis should:

- A. include a benchmark of similar companies in its scop
- B. assume an equal degree of protection for all asset
- C. address the potential size and likelihood of los
- D. give more weight to the likelihood v
- E. the size of the los

**Answer: C**

**Explanation:**

A risk analysis should take into account the potential size and likelihood of a loss. It could include comparisons with a group of companies of similar size. It should not assume an equal degree of protection for all assets since assets may have different risk factors. The likelihood of the loss should not receive greater emphasis than the size of the loss; a risk analysis should always address both equally.

**NEW QUESTION 108**

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 countermeasure
- B. Eliminate the ris
- C. Transfer the ris
- D. Accept the ris

**Answer: C**

**Explanation:**

Risks are typically transferred to insurance companies when the probability of an incident is low but the impact is high. Examples include: hurricanes, tornados and earthquakes. Implementing countermeasures may not be the most cost-effective approach to security management. Eliminating the risk may not be possible. Accepting the risk would leave the organization vulnerable to a catastrophic disaster which may cripple or ruin the organization. It would be more cost effective to pay recurring insurance costs than to be affected by a disaster from which the organization cannot financially recover.

**NEW QUESTION 113**

The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

- A. sales departmen
- B. database administrato
- C. chief information officer (CIO).
- D. head of the sales departmen

**Answer: D**

**Explanation:**

The owner of the information asset should be the person with the decision-making power in the department deriving the most benefit from the asset. In this case, it would be the head of the sales department. The organizational unit cannot be the owner of the asset because that removes personal responsibility. The database administrator is a custodian. The chief information officer (CIO) would not be an owner of this database because the CTO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

**NEW QUESTION 118**

Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

- A. User assessments of changes
- B. Comparison of the program results with industry standards
- C. Assignment of risk within the organization
- D. Participation by all members of the organization

**Answer: D**

**Explanation:**

Effective risk management requires participation, support and acceptance by all applicable members of the organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

**NEW QUESTION 120**

Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

- A. conduct a risk assessment and allow or disallow based on the outcom
- B. recommend a risk assessment and implementation only if the residual risks are accepte
- C. recommend against implementation because it violates the company's policie
- D. recommend revision of current polic

**Answer:** B

**Explanation:**

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

#### NEW QUESTION 121

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

**Answer:** B

**Explanation:**

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

#### NEW QUESTION 124

A risk assessment should be conducted:

- A. once a year for each business process and subproces
- B. every three to six months for critical business processe
- C. by external parties to maintain objectivit
- D. annually or whenever there is a significant chang

**Answer:** D

**Explanation:**

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

#### NEW QUESTION 126

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- A. Risk analysis process
- B. Business impact analysis (BIA)
- C. Risk management balanced scorecard
- D. Risk-based audit program

**Answer:** B

**Explanation:**

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

#### NEW QUESTION 128

Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

- A. Annual loss expectancy (ALE) of incidents
- B. Frequency of incidents
- C. Total cost of ownership (TCO)
- D. Approved budget for the project

**Answer:** C

**Explanation:**

The total cost of ownership (TCO) would be the most relevant piece of information in that it would establish a cost baseline and it must be considered for the full life cycle of the control. Annual loss expectancy (ALE) and the frequency of incidents could help measure the benefit, but would have more of an indirect relationship

as not all incidents may be mitigated by implementing a two-factor authentication system. The approved budget for the project may have no bearing on what the project may actually cost.

#### NEW QUESTION 130

Which of the following is MOST essential for a risk management program to be effective?

- A. Flexible security budget
- B. Sound risk baseline
- C. New risks detection
- D. Accurate risk reporting

**Answer: C**

#### Explanation:

All of these procedures are essential for implementing risk management. However, without identifying new risks, other procedures will only be useful for a limited period.

#### NEW QUESTION 133

When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

- A. Estimated productivity losses
- B. Possible scenarios with threats and impacts
- C. Value of information assets
- D. Vulnerability assessment

**Answer: B**

#### Explanation:

Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

#### NEW QUESTION 134

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

**Answer: D**

#### Explanation:

Risk should be addressed as early as possible in the development cycle. The feasibility study should include risk assessment so that the cost of controls can be estimated before the project proceeds. 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. Assessment would not be relevant in choice A or C.

#### NEW QUESTION 135

When residual risk is minimized:

- A. acceptable risk is probable
- B. transferred risk is acceptable
- C. control risk is reduced
- D. risk is transferable

**Answer: A**

#### Explanation:

Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

#### NEW QUESTION 137

Quantitative risk analysis is MOST appropriate when assessment data:

- A. include customer perception
- B. contain percentage estimate
- C. do not contain specific detail
- D. contain subjective information

**Answer: B**

#### Explanation:



Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

#### NEW QUESTION 139

A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

- A. Risk analysis results
- B. Audit report findings
- C. Penetration test results
- D. Amount of IT budget available

**Answer:** A

#### Explanation:

Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

#### NEW QUESTION 142

Which of the following is the MOST appropriate use of gap analysis?

- A. Evaluating a business impact analysis (BIA)
- B. Developing a balanced business scorecard
- C. Demonstrating the relationship between controls
- D. Measuring current state v
- E. desired future state

**Answer:** D

#### Explanation:

A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a business impact analysis (BIA), developing a balanced business scorecard or demonstrating the relationship between variables.

#### NEW QUESTION 143

The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

- A. Mitigating controls
- B. Visibility of impact
- C. Likelihood of occurrence
- D. Incident frequency

**Answer:** B

#### Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

#### NEW QUESTION 144

The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

- A. provide in-depth defenses
- B. separate test and production
- C. permit traffic load balancing
- D. prevent a denial-of-service attack

**Answer:** C

#### Explanation:

Having two entry points, each guarded by a separate firewall, is desirable to permit traffic load balancing. As they both connect to the Internet and to the same demilitarized zone (DMZ), such an arrangement is not practical for separating test from production or preventing a denial-of-service attack.

#### NEW QUESTION 146

Which of the following is the BEST metric for evaluating the effectiveness of security awareness training? The number of:

- A. password reset
- B. reported incident
- C. incidents resolved
- D. access rule violation

**Answer:** B

**Explanation:**

Reported incidents will provide an indicator of the awareness level of staff. An increase in reported incidents could indicate that the staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. The number of incidents resolved may not correlate to staff awareness.

**NEW QUESTION 148**

Which of the following is the MOST important risk associated with middleware in a client-server environment?

- A. Server patching may be prevented
- B. System backups may be incomplete
- C. System integrity may be affected
- D. End-user sessions may be hijacked

**Answer: C**

**Explanation:**

The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely to occur.

**NEW QUESTION 150**

Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

- A. Patch management
- B. Change management
- C. Security metrics
- D. Version control

**Answer: B**

**Explanation:**

Change management controls the process of introducing changes to systems. Failure to have good change management may introduce new weaknesses into otherwise secure systems. Patch management corrects discovered weaknesses by applying a correction to the original program code. Security metrics provide a means for measuring effectiveness. Version control is a subset of change management.

**NEW QUESTION 152**

An information security program should be sponsored by:

- A. infrastructure managemen
- B. the corporate audit departmen
- C. key business process owner
- D. information security managemen

**Answer: C**

**Explanation:**

The information security program should ideally be sponsored by business managers, as represented by key business process owners. Infrastructure management is not sufficiently independent and lacks the necessary knowledge regarding specific business requirements. A corporate audit department is not in as good a position to fully understand how an information security program needs to meet the needs of the business. Audit independence and objectivity will be lost, impeding traditional audit functions. Information security implements and executes the program. Although it should promote it at all levels, it cannot sponsor the effort due to insufficient operational knowledge and lack of proper authority.

**NEW QUESTION 157**

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

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

**Answer: B**

**Explanation:**

The certificate authority (CA) is a trusted third party that attests to the identity of the signatory, and reliance will be a function of the level of trust afforded the CA. A digital signature would provide a level of assurance of message integrity, but it is a three-party exchange, including the CA. Digital signatures do not require encryption of the message in order to preserve confidentiality.

**NEW QUESTION 162**

The MAIN advantage of implementing automated password synchronization is that it:

- A. reduces overall administrative workloa
- B. increases security between multi-tier system

- C. allows passwords to be changed less frequently
- D. reduces the need for two-factor authentication

**Answer:** A

**Explanation:**

Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multi-tier systems, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

#### NEW QUESTION 167

Which of the following is the MOST important reason why information security objectives should be defined?

- A. Tool for measuring effectiveness
- B. General understanding of goals
- C. Consistency with applicable standards
- D. Management sign-off and support initiatives

**Answer:** A

**Explanation:**

The creation of objectives can be used in part as a source of measurement of the effectiveness of information security management, which feeds into the overall governance. General understanding of goals and consistency with applicable standards are useful, but are not the primary reasons for having clearly defined objectives. Gaining management understanding is important, but by itself will not provide the structure for governance.

#### NEW QUESTION 170

Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

- A. Patch management
- B. Change management
- C. Security baselines
- D. Virus detection

**Answer:** B

**Explanation:**

Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses. Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

#### NEW QUESTION 173

The effectiveness of virus detection software is MOST dependent on which of the following?

- A. Packet filtering
- B. Intrusion detection
- C. Software upgrades
- D. Definition tables

**Answer:** D

**Explanation:**

The effectiveness of virus detection software depends on virus signatures which are stored in virus definition tables. Software upgrades are related to the periodic updating of the program code, which would not be as critical. Intrusion detection and packet filtering do not focus on virus detection.

#### NEW QUESTION 176

The BEST metric for evaluating the effectiveness of a firewall is the:

- A. number of attacks blocked
- B. number of packets dropped
- C. average throughput rate
- D. number of firewall rules

**Answer:** A

**Explanation:**

The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not effective measurements.

#### NEW QUESTION 179

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

**Answer:** D

**Explanation:**

Structured Query Language (SQL) injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent of fooling the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written; software is available to test for such weaknesses. All other choices would fail to prevent such an attack.

#### NEW QUESTION 180

Which of the following is MOST effective in preventing security weaknesses in operating systems?

- A. Patch management
- B. Change management
- C. Security baselines
- D. Configuration management

**Answer:** A

**Explanation:**

Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

#### NEW QUESTION 185

The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

- A. helps ensure that communications are secure
- B. increases security between multi-tier system
- C. allows passwords to be changed less frequently
- D. eliminates the need for secondary authentication

**Answer:** A

**Explanation:**

Virtual Private Network (VPN) tunneling for remote users provides an encrypted link that helps ensure secure communications. It does not affect password change frequency, nor does it eliminate the need for secondary authentication or affect security within the internal network.

#### NEW QUESTION 187

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

**Answer:** D

**Explanation:**

Operational risk assessment, financial crime metrics and capacity management can complement the information security framework, but only business continuity management is a key component.

#### NEW QUESTION 190

The MOST important reason that statistical anomaly-based intrusion detection systems (stat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

- A. create more overhead than signature-based IDS
- B. cause false positives from minor changes to system variable
- C. generate false alarms from varying user or system action
- D. cannot detect new types of attack

**Answer:** C

**Explanation:**

A statistical anomaly-based intrusion detection system (stat IDS) collects data from normal traffic and establishes a baseline. It then periodically samples the network activity based on statistical methods and compares samples to the baseline. When the activity is outside the baseline parameter (clipping level), the IDS notifies the administrator. The baseline variables can include a host's memory or central processing unit (CPU) usage, network packet types and packet quantities. If actions of the users or the systems on the network vary widely with periods of low activity and periods of frantic packet exchange, a stat IDS may not be suitable, as the dramatic swing from one level to another almost certainly will generate false alarms. This weakness will have the largest impact on the operation of the IT

systems. Due to the nature of stat IDS operations (i.e., they must constantly attempt to match patterns of activity to the baseline parameters), a stat IDS requires much more overhead and processing than signature-based versions. Due to the nature of a stat IDS—based on statistics and comparing data with baseline parameters—this type of IDS may not detect minor changes to system variables and may generate many false positives. Choice D is incorrect; since the stat IDS can monitor multiple system variables, it can detect new types of variables by tracing for abnormal activity of any kind.

#### NEW QUESTION 192

In an organization, information systems security is the responsibility of:

- A. all personne
- B. information systems personne
- C. information systems security personne
- D. functional personne

**Answer:** A

#### Explanation:

All personnel of the organization have the responsibility of ensuring information systems security-this can include indirect personnel such as physical security personnel. Information systems security cannot be the responsibility of information systems personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of information systems security personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of functional personnel alone since they cannot ensure security.

#### NEW QUESTION 197

It is important to develop an information security baseline because it helps to define:

- A. critical information resources needing protectio
- B. a security policy for the entire organizatio
- C. the minimum acceptable security to be implemente
- D. required physical and logical access control

**Answer:** C

#### Explanation:

Developing an information security baseline helps to define the minimum acceptable security that will be implemented to protect the information resources in accordance with the respective criticality levels. Before determining the security baseline, an information security manager must establish the security policy, identify criticality levels of organization's information resources and assess the risk environment in which those resources operate.

#### NEW QUESTION 199

Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

- A. Certificate-based authentication of web client
- B. Certificate-based authentication of web server
- C. Data confidentiality between client and web server
- D. Multiple encryption algorithms

**Answer:** A

#### Explanation:

Web browsers have the capability of authenticating through client-based certificates; nevertheless, it is not commonly used. When using https, servers always authenticate with a certificate and, once the connection is established, confidentiality will be maintained between client and server. By default, web browsers and servers support multiple encryption algorithms and negotiate the best option upon connection.

#### NEW QUESTION 204

Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

- A. Periodic focus group meetings
- B. Periodic compliance reviews
- C. Computer-based certification training (CBT)
- D. Employee's signed acknowledgement

**Answer:** C

#### Explanation:

Using computer-based training (CBT) presentations with end-of-section reviews provides feedback on how well users understand what has been presented. Periodic compliance reviews are a good tool to identify problem areas but do not ensure that procedures are known or understood. Eocus groups may or may not provide meaningful detail. Although a signed employee acknowledgement is good, it does not indicate whether the material has been read and/or understood.

#### NEW QUESTION 205

The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

- A. contribute cost-effective expertise not available internall
- B. be made responsible for meeting the security program requirement
- C. replace the dependence on internal resource
- D. deliver more effectively on account of their knowledg



**Answer:** A

**Explanation:**

Choice A represents the primary driver for the information security manager to make use of external resources. The information security manager will continue to be responsible for meeting the security program requirements despite using the services of external resources. The external resources should never completely replace the role of internal resources from a strategic perspective. The external resources cannot have a better knowledge of the business of the information security manager's organization than do the internal resources.

#### NEW QUESTION 209

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

**Answer:** B

**Explanation:**

Public key infrastructure (PKI) combines public key encryption with a trusted third party to publish and revoke digital certificates that contain the public key of the sender. Senders can digitally sign a message with their private key and attach their digital certificate (provided by the trusted third party). These characteristics allow senders to provide authentication, integrity validation and nonrepudiation. Symmetric cryptography provides confidentiality. Mashing can provide integrity and confidentiality. Message authentication codes provide integrity.

#### NEW QUESTION 211

An intranet server should generally be placed on the:

- A. internal network
- B. firewall serve
- C. external route
- D. primary domain controlle

**Answer:** A

**Explanation:**

An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary- domain controllers do not normally share the physical device as the intranet server.

#### NEW QUESTION 213

Good information security standards should:

- A. define precise and unambiguous allowable limit
- B. describe the process for communicating violation
- C. address high-level objectives of the organizatio
- D. be updated frequently as new software is release

**Answer:** A

**Explanation:**

A security standard should clearly state what is allowable; it should not change frequently. The process for communicating violations would be addressed by a security procedure, not a standard. High-level objectives of an organization would normally be addressed in a security policy.

#### NEW QUESTION 216

What is the BEST way to ensure that contract programmers comply with organizational security policies?

- A. Explicitly refer to contractors in the security standards
- B. Have the contractors acknowledge in writing the security policies
- C. Create penalties for noncompliance in the contracting agreement
- D. Perform periodic security reviews of the contractors

**Answer:** D

**Explanation:**

Periodic reviews are the most effective way of obtaining compliance. None of the other options detects the failure of contract programmers to comply.

#### NEW QUESTION 221

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

- A. Mantrap
- B. Biometric lock
- C. Closed-circuit television (CCTV)

D. Security guard

**Answer:** B

**Explanation:**

A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

#### NEW QUESTION 223

Which would be the BEST recommendation to protect against phishing attacks?

- A. Install an antispam system
- B. Publish security guidance for customers
- C. Provide security awareness to the organization's staff
- D. Install an application-level firewall

**Answer:** B

**Explanation:**

Customers of the organization are the target of phishing attacks. Installing security software or training the organization's staff will be useless. The effort should be put on the customer side.

#### NEW QUESTION 227

Which of the following events generally has the highest information security impact?

- A. Opening a new office
- B. Merging with another organization
- C. Relocating the data center
- D. Rewiring the network

**Answer:** B

**Explanation:**

Merging with or acquiring another organization causes a major impact on an information security management function because new vulnerabilities and risks are inherited. Opening a new office, moving the data center to a new site, or rewiring a network may have information security risks, but generally comply with corporate security policy and are easier to secure.

#### NEW QUESTION 229

Which of the following is the MOST effective, positive method to promote security awareness?

- A. Competitions and rewards for compliance
- B. Lock-out after three incorrect password attempts
- C. Strict enforcement of password formats
- D. Disciplinary action for noncompliance

**Answer:** A

**Explanation:**

Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

#### NEW QUESTION 233

Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

- A. mandatory access control
- B. discretionary access control
- C. lattice-based access control
- D. role-based access control

**Answer:** D

**Explanation:**

Role-based access controls will grant temporary employee access based on the job function to be performed. This provides a better means of ensuring that the access is not more or less than what is required. Discretionary, mandatory and lattice-based access controls are all security models, but they do not address the issue of temporary employees as well as role-based access controls.

#### NEW QUESTION 236

The return on investment of information security can BEST be evaluated through which of the following?

- A. Support of business objectives
- B. Security metrics
- C. Security deliverables

D. Process improvement models

**Answer:** A

**Explanation:**

One way to determine the return on security investment is to illustrate how information security supports the achievement of business objectives. Security metrics measure improvement and effectiveness within the security practice but do not tie to business objectives. Similarly, listing deliverables and creating process improvement models does not necessarily tie into business objectives.

#### NEW QUESTION 241

Which item would be the BEST to include in the information security awareness training program for new general staff employees?

- A. Review of various security models
- B. Discussion of how to construct strong passwords
- C. Review of roles that have privileged access
- D. Discussion of vulnerability assessment results

**Answer:** B

**Explanation:**

All new employees will need to understand techniques for the construction of strong passwords. The other choices would not be applicable to general staff employees.

#### NEW QUESTION 246

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

- A. Batch patches into frequent server updates
- B. Initially load the patches on a test machine
- C. Set up servers to automatically download patches
- D. Automatically push all patches to the servers

**Answer:** B

**Explanation:**

Some patches can conflict with application code. For this reason, it is very important to first test all patches in a test environment to ensure that there are no conflicts with existing application systems. For this reason, choices C and D are incorrect as they advocate automatic updating. As for frequent server updates, this is an incomplete (vague) answer from the choices given.

#### NEW QUESTION 248

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

- A. end user
- B. legal counsel
- C. operational unit
- D. audit management

**Answer:** C

**Explanation:**

Procedures at the operational level must be developed by or with the involvement of operational units that will use them. This will ensure that they are functional and accurate. End users and legal counsel are normally not involved in procedure development. Audit management generally oversees information security operations but does not get involved at the procedural level.

#### NEW QUESTION 249

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

- A. set their accounts to expire in six months or less
- B. avoid granting system administration role
- C. ensure they successfully pass background check
- D. ensure their access is approved by the data owner

**Answer:** B

**Explanation:**

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. Setting expiration dates, requiring background checks and having the data owner assign access are all positive elements, but these will not prevent contract personnel from obtaining access to sensitive information.

#### NEW QUESTION 251

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

- A. Periodic review of network configuration

- B. Review intrusion detection system (IDS) logs for evidence of attacks
- C. Periodically perform penetration tests
- D. Daily review of server logs for evidence of hacker activity

**Answer:** C

**Explanation:**

Due to the complexity of firewall rules and router tables, plus the sheer size of intrusion detection systems (IDSs) and server logs, a physical review will be insufficient. The best approach for confirming the adequacy of these configuration settings is to periodically perform attack and penetration tests.

#### NEW QUESTION 255

Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

- A. User ad hoc reporting is not logged
- B. Network traffic is through a single switch
- C. Operating system (OS) security patches have not been applied
- D. Database security defaults to ERP settings

**Answer:** C

**Explanation:**

The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security- weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

#### NEW QUESTION 256

Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

- A. Passwords stored in encrypted form
- B. User awareness
- C. Strong passwords that are changed periodically
- D. Implementation of lock-out policies

**Answer:** D

**Explanation:**

Implementation of account lock-out policies significantly inhibits brute-force attacks. In cases where this is not possible, strong passwords that are changed periodically would be an appropriate choice. Passwords stored in encrypted form will not defeat an online brute-force attack if the password itself is easily guessed. User awareness would help but is not the best approach of the options given.

#### NEW QUESTION 259

The PRIMARY focus of the change control process is to ensure that changes are:

- A. authorize
- B. applie
- C. documente
- D. teste

**Answer:** A

**Explanation:**

All steps in the change control process must be signed off on to ensure proper authorization. It is important that changes are applied, documented and tested; however, they are not the primary focus.

#### NEW QUESTION 263

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

**Answer:** C

**Explanation:**

Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self- assessment exercises are all good but do not exemplify the taking of ownership by management.

#### NEW QUESTION 268

In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

- A. Applying patches

- B. Changing access rules
- C. Upgrading hardware
- D. Backing up files

**Answer:** B

**Explanation:**

Security software will generally have a well-controlled process for applying patches, backing up files and upgrading hardware. The greatest risk occurs when access rules are changed since they are susceptible to being opened up too much, which can result in the creation of a security exposure.

#### NEW QUESTION 271

The BEST way to ensure that an external service provider complies with organizational security policies is to:

- A. Explicitly include the service provider in the security policie
- B. Receive acknowledgment in writing stating the provider has read all policie
- C. Cross-reference to policies in the service level agreement
- D. Perform periodic reviews of the service provide

**Answer:** D

**Explanation:**

Periodic reviews will be the most effective way of obtaining compliance from the external service provider. References in policies and service level agreements and requesting written acknowledgement will not be as effective since they will not trigger the detection of noncompliance.

#### NEW QUESTION 272

Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

- A. Utilize an intrusion detection syste
- B. Establish minimum security baseline
- C. Implement vendor recommended setting
- D. Perform periodic penetration testin

**Answer:** D

**Explanation:**

Penetration testing is the best way to assure that perimeter security is adequate. An intrusion detection system (IDS) may detect an attempted attack, hut it will not confirm whether the perimeter is secured. Minimum security baselines and applying vendor recommended settings are beneficial, but they will not provide the level of assurance that is provided by penetration testing.

#### NEW QUESTION 277

Managing the life cycle of a digital certificate is a role of a(n):

- A. system administrato
- B. security administrato
- C. system developpe
- D. independent trusted sourc

**Answer:** D

**Explanation:**

Digital certificates must be managed by an independent trusted source in order to maintain trust in their authenticity. The other options are not necessarily entrusted with this capability.

#### NEW QUESTION 282

Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

- A. A problem management process
- B. Background screening
- C. A change control process
- D. Business impact analysis (BIA)

**Answer:** C

**Explanation:**

A change control process is the methodology that ensures that anything that could be impacted by a development change will be reevaluated. Problem management is the general process intended to manage all problems, not those specifically related to security. Background screening is the process to evaluate employee references when they are hired. BIA is the methodology used to evaluate risks in the business continuity process.

#### NEW QUESTION 284

Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

- A. Attempt to reset several passwords to weaker values



- B. Install code to capture passwords for periodic audit
- C. Sample a subset of users and request their passwords for review
- D. Review general security settings on each platform

**Answer:** D

**Explanation:**

Reviewing general security settings on each platform will be the most efficient method for determining password strength while not compromising the integrity of the passwords. Attempting to reset several passwords to weaker values may not highlight certain weaknesses. Installing code to capture passwords for periodic audit, and sampling a subset of users and requesting their passwords for review, would compromise the integrity of the passwords.

#### NEW QUESTION 289

Which of the following represents a PRIMARY area of interest when conducting a penetration test?

- A. Data mining
- B. Network mapping
- C. Intrusion Detection System (IDS)
- D. Customer data

**Answer:** B

**Explanation:**

Network mapping is the process of determining the topology of the network one wishes to penetrate. This is one of the first steps toward determining points of attack in a network. Data mining is associated with ad hoc reporting and, together with customer data, they are potential targets after the network is penetrated. The intrusion detection mechanism in place is not an area of focus because one of the objectives is to determine how effectively it protects the network or how easy it is to circumvent.

#### NEW QUESTION 294

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

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

**Answer:** C

**Explanation:**

One of the main problems with using SNMP v1 and v2 is the clear text "community string" that it uses to authenticate. It is easy to sniff and reuse. Most times, the SNMP community string is shared throughout the organization's servers and routers, making this authentication problem a serious threat to security. There have been some isolated cases of remote buffer overflows against SNMP daemons, but generally that is not a problem. Cross site scripting is a web application vulnerability that is not related to SNMP. A man-in-the-middle attack against a user datagram protocol (UDP) makes no sense since there is no active session; every request has the community string and is answered independently.

#### NEW QUESTION 296

How would an organization know if its new information security program is accomplishing its goals?

- A. Key metrics indicate a reduction in incident impact
- B. Senior management has approved the program and is supportive of it
- C. Employees are receptive to changes that were implemented
- D. There is an immediate reduction in reported incident

**Answer:** A

**Explanation:**

Option A is correct since an effective security program will show a trend in impact reduction. Options B and C may well derive from a performing program, but are not as significant as option A. Option D may indicate that it is not successful.

#### NEW QUESTION 299

Data owners are normally responsible for which of the following?

- A. Applying emergency changes to application data
- B. Administering security over database records
- C. Migrating application code changes to production
- D. Determining the level of application security required

**Answer:** D

**Explanation:**

Data owners approve access to data and determine the degree of protection that should be applied (data classification). Administering database security, making emergency changes to data and migrating code to production are infrastructure tasks performed by custodians of the data.

#### NEW QUESTION 303

Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have his, her password reset?

- A. Performing reviews of password resets
- B. Conducting security awareness programs
- C. Increasing the frequency of password changes
- D. Implementing automatic password syntax checking

**Answer: B**

#### Explanation:

Social engineering can be mitigated best through periodic security awareness training for staff members who may be the target of such an attempt. Changing the frequency of password changes, strengthening passwords and checking the number of password resets may be desirable, but they will not be as effective in reducing the likelihood of a social engineering attack.

#### NEW QUESTION 307

The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

- A. Data owner
- B. Data custodian
- C. Systems programmer
- D. Security administrator

**Answer: C**

#### Explanation:

A systems programmer should not have privileges to modify the access control list (ACL) because this would give the programmer unlimited control over the system. The data owner would request and approve updates to the ACL, but it is not a violation of the separation of duties principle if the data owner has update rights to the ACL. The data custodian and the security administrator could carry out the updates on the ACL since it is part of their duties as delegated to them by the data owner.

#### NEW QUESTION 310

A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

- A. Enable access through a separate device that requires adequate authentication
- B. Implement manual procedures that require password change after each use
- C. Request the vendor to add multiple user IDs
- D. Analyze the logs to detect unauthorized access

**Answer: A**

#### Explanation:

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual.

Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but, because it is detective, it would not be the most effective in this instance.

#### NEW QUESTION 311

The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

- A. perform penetration testin
- B. establish security baseline
- C. implement vendor default setting
- D. link policies to an independent standar

**Answer: B**

#### Explanation:

Security baselines will provide the best assurance that each platform meets minimum criteria. Penetration testing will not be as effective and can only be performed periodically. Vendor default settings will not necessarily meet the criteria set by the security policies, while linking policies to an independent standard will not provide assurance that the platforms meet these levels of security.

#### NEW QUESTION 315

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

**Answer: C**

**Explanation:**

Source code review is the best way to find and remove an application backdoor. Application backdoors can be almost impossible to identify' using a black box pen test or a security audit. A vulnerability scan will only find "known" vulnerability patterns and will therefore not find a programmer's application backdoor.

**NEW QUESTION 316**

Which of the following should be in place before a black box penetration test begins?

- A. IT management approval
- B. Proper communication and awareness training
- C. A clearly stated definition of scope
- D. An incident response plan

**Answer: C**

**Explanation:**

Having a clearly stated definition of scope is most important to ensure a proper understanding of risk as well as success criteria, IT management approval may not be required based on senior management decisions. Communication, awareness and an incident response plan are not a necessary requirement. In fact, a penetration test could help promote the creation and execution of the incident response plan.

**NEW QUESTION 318**

Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

- A. Conduct awareness sessions on intellectual property policy
- B. Require all employees to sign a nondisclosure agreement
- C. Promptly remove all access when an employee leaves the organization
- D. Restrict access to a need-to-know basis

**Answer: D**

**Explanation:**

Security awareness regarding intellectual property policy will not prevent violations of this policy. Requiring all employees to sign a nondisclosure agreement and promptly removing all access when an employee leaves the organization are good controls, but not as effective as restricting access to a need-to-know basis.

**NEW QUESTION 320**

The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

- A. simulate an attack and review IDS performance
- B. use a honeypot to check for unusual activity
- C. audit the configuration of the IDS
- D. benchmark the IDS against a peer site

**Answer: A**

**Explanation:**

Simulating an attack on the network demonstrates whether the intrusion detection system (IDS) is properly tuned. Reviewing the configuration may or may not reveal weaknesses since an anomaly-based system uses trends to identify potential attacks. A honeypot is not a good first step since it would need to have already been penetrated. Benchmarking against a peer site would generally not be practical or useful.

**NEW QUESTION 322**

An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

- A. Design a training program for the staff involved to heighten information security awareness
- B. Set role-based access permissions on the shared folder
- C. The end user develops a PC macro program to compare sender and recipient file contents
- D. Shared folder operators sign an agreement to pledge not to commit fraudulent activities

**Answer: B**

**Explanation:**

Ideally, requesting that the IT department develop an automated integrity check would be desirable, but given the temporary nature of the problem, the risk can be mitigated by setting stringent access permissions on the shared folder. Operations staff should only have write access and disbursement staff should only have read access, and everyone else, including the administrator, should be disallowed. An information security awareness program and/or signing an agreement to not engage in fraudulent activities may help deter attempts made by employees; however, as long as employees see a chance of personal gain when internal control is loose, they may embark on unlawful activities such as alteration of payment files. A PC macro would be an inexpensive automated solution to develop with control reports. However, sound independence or segregation of duties cannot be expected in the reconciliation process since it is run by an end-user group. Therefore, this option may not provide sufficient proof.

**NEW QUESTION 325**

A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

- A. User
- B. Network
- C. Operations
- D. Database

**Answer:** A

**Explanation:**

As owners of the system, user management signoff is the most important. If a system does not meet the needs of the business, then it has not met its primary objective. The needs of network, operations and database management are secondary to the needs of the business.

#### NEW QUESTION 327

The PRIMARY objective of security awareness is to:

- A. ensure that security policies are understood
- B. influence employee behavior
- C. ensure legal and regulatory compliance
- D. notify of actions for noncompliance

**Answer:** B

**Explanation:**

It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, or meeting legal and regulatory requirements is important but secondary.

#### NEW QUESTION 332

An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

- A. A due diligence security review of the business partner's security controls
- B. Ensuring that the business partner has an effective business continuity program
- C. Ensuring that the third party is contractually obligated to all relevant security requirements
- D. Talking to other clients of the business partner to check references for performance

**Answer:** C

**Explanation:**

The key requirement is that the information security manager ensures that the third party is contractually bound to follow the appropriate security requirements for the process being outsourced. This protects both organizations. All other steps are contributory to the contractual agreement, but are not key.

#### NEW QUESTION 334

Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

- A. System analyst
- B. Quality control manager
- C. Process owner
- D. Information security manager

**Answer:** C

**Explanation:**

Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

#### NEW QUESTION 335

What is the PRIMARY objective of a post-event review in incident response?

- A. Adjust budget provisioning
- B. Preserve forensic data
- C. Improve the response process
- D. Ensure the incident is fully documented

**Answer:** C

**Explanation:**

The primary objective is to find any weakness in the current process and improve it. The other choices are all secondary.

#### NEW QUESTION 337

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 dat
- B. recovery point objective (RPO).
- C. recovery' time objective (RTO).
- D. interruption windo

**Answer:** B

**Explanation:**

The recovery point objective (RPO) defines the maximum loss of data (in terms of time) acceptable by the business (i.e., age of data to be restored). It will directly determine the basic elements of the backup strategy frequency of the backups and what kind of backup is the most appropriate (disk-to-disk, on tape, mirroring). The volume of data will be used to determine the capacity of the backup solution. The recovery time objective (RTO)—the time between disaster and return to normal operation—will not have any impact on the backup strategy. The availability to restore backups in a time frame consistent with the interruption window will have to be checked and will influence the strategy (e.g., full backup vs. incremental), but this will not be the primary factor.

#### NEW QUESTION 341

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/ I'DP) ports

**Answer:** C

**Explanation:**

When investigating a security breach, it is important to preserve all traces of evidence left by the invader. For this reason, it is imperative to preserve the memory' contents of the machine in order to analyze them later. The correct answer is choice C because a copy of the whole system's memory is obtained for future analysis by running the appropriate tools. This is also important from a legal perspective since an attorney may suggest that the system was changed during the conduct of the investigation. Running a computer forensics tool in the compromised machine will cause the creation of at least one process that may overwrite evidence. Rebooting the machine will delete the contents of the memory, erasing potential evidence. Collecting information about current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports is correct, but doing so by using tools may also erase memory contents.

#### NEW QUESTION 346

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

- A. obtaining evidence as soon as possibl
- B. preserving the integrity of the evidenc
- C. disconnecting all IT equipment involve
- D. reconstructing the sequence of event

**Answer:** B

**Explanation:**

The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are pan of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

#### NEW QUESTION 347

A desktop computer that was involved in a computer security incident should be secured as evidence by:

- A. disconnecting the computer from all power source
- B. disabling all local user accounts except for one administrato
- C. encrypting local files and uploading exact copies to a secure serve
- D. copying all files using the operating system (OS) to write-once medi

**Answer:** A

**Explanation:**

To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing it remotely changes the operating system (OS) and temporary files on the computer and invalidates it as admissible evidence.

#### NEW QUESTION 350

The FIRST priority when responding to a major security incident is:

- A. documentatio
- B. monitorin
- C. restoratio
- D. containmen

**Answer:** D

**Explanation:**



The first priority in responding to a security incident is to contain it to limit the impact. Documentation, monitoring and restoration are all important, but they should follow containment.

#### NEW QUESTION 352

Which of the following should be determined FIRST when establishing a business continuity program?

- A. Cost to rebuild information processing facilities
- B. Incremental daily cost of the unavailability of systems
- C. Location and cost of offsite recovery facilities
- D. Composition and mission of individual recovery teams

**Answer: B**

#### Explanation:

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

#### NEW QUESTION 356

Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

- A. Incident response metrics
- B. Periodic auditing of the incident response process
- C. Action recording and review
- D. Post incident review

**Answer: D**

#### Explanation:

Post event reviews are designed to identify gaps and shortcomings in the actual incident response process so that these gaps may be improved over time. The other choices will not provide the same level of feedback in improving the process.

#### NEW QUESTION 361

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

- A. rebuild the server from the last verified backu
- B. place the web server in quarantin
- C. shut down the server in an organized manne
- D. rebuild the server with original media and relevant patche

**Answer: D**

#### Explanation:

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

#### NEW QUESTION 364

A post-incident review should be conducted by an incident management team to determine:

- A. relevant electronic evidenc
- B. lessons learne
- C. hacker's identit
- D. areas affecte

**Answer: B**

#### Explanation:

Post-incident reviews are beneficial in determining ways to improve the response process through lessons learned from the attack. Evaluating the relevance of evidence, who launched the attack or what areas were affected are not the primary purposes for such a meeting because these should have been already established during the response to the incident.

#### NEW QUESTION 369

Which of the following is MOST important in determining whether a disaster recovery test is successful?

- A. Only business data files from offsite storage are used
- B. IT staff fully recovers the processing infrastructure
- C. Critical business processes are duplicated
- D. All systems are restored within recovery time objectives (RTOs)

**Answer:**

C

**Explanation:**

To ensure that a disaster recovery test is successful, it is most important to determine whether all critical business functions were successfully recovered and duplicated. Although ensuring that only materials taken from offsite storage are used in the test is important, this is not as critical in determining a test's success. While full recovery of the processing infrastructure is a key recovery milestone, it does not ensure the success of a test. Achieving the RTOs is another important milestone, but does not necessarily prove that the critical business functions can be conducted, due to interdependencies with other applications and key elements such as data, staff, manual processes, materials and accessories, etc.

**NEW QUESTION 372**

Of the following, which is the MOST important aspect of forensic investigations?

- A. The independence of the investigator
- B. Timely intervention
- C. Identifying the perpetrator
- D. Chain of custody

**Answer: D**

**Explanation:**

Establishing the chain of custody is one of the most important steps in conducting forensic investigations since it preserves the evidence in a manner that is admissible in court. The independence of the investigator may be important, but is not the most important aspect. Timely intervention is important for containing incidents, but not as important for forensic investigation. Identifying the perpetrator is important, but maintaining the chain of custody is more important in order to have the perpetrator convicted in court.

**NEW QUESTION 374**

An intrusion detection system (IDS) should:

- A. run continuously
- B. ignore anomalies
- C. require a stable, rarely changed environment
- D. be located on the network

**Answer: A**

**Explanation:**

If an intrusion detection system (IDS) does not run continuously the business remains vulnerable. An IDS should detect, not ignore anomalies. An IDS should be flexible enough to cope with a changing environment. Both host and network based IDS are recommended for adequate detection.

**NEW QUESTION 379**

The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

- A. regulatory' requirement
- B. business requirement
- C. financial valu
- D. IT resource availabilit

**Answer: B**

**Explanation:**

The criticality to business should always drive the decision. Regulatory requirements could be more flexible than business needs. The financial value of an asset could not correspond to its business value. While a consideration, IT resource availability is not a primary factor.

**NEW QUESTION 383**

Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

- A. Setting up a backup site
- B. Maintaining redundant systems
- C. Aligning with recovery time objectives (RTOs)
- D. Data backup frequency

**Answer: C**

**Explanation:**

BCP.'DRP should align with business RTOs. The RTO represents the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RTO must be taken into consideration when prioritizing systems for recovery efforts to ensure that those systems that the business requires first are the ones that are recovered first.

**NEW QUESTION 387**

Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

- A. determining the extent of property damag

- B. preserving environmental condition
- C. ensuring orderly plan activatio
- D. reducing the extent of operational damag

**Answer:** D

**Explanation:**

During an incident, emergency actions should minimize or eliminate casualties and damage to the business operation, thus reducing business interruptions. Determining the extent of property damage is not the consideration; emergency actions should minimize, not determine, the extent of the damage. Protecting/preserving environmental conditions may not be relevant. Ensuring orderly plan activation is important but not as critical as reducing damage to the operation.

#### NEW QUESTION 390

An incident response policy must contain:

- A. updated call tree
- B. escalation criteri
- C. press release template
- D. critical backup files inventor

**Answer:** B

**Explanation:**

Escalation criteria, indicating the circumstances under which specific actions are to be undertaken, should be contained within an incident response policy. Telephone trees, press release templates and lists of critical backup files are too detailed to be included in a policy document.

#### NEW QUESTION 392

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

**Answer:** B

**Explanation:**

Quickly ranking the severity criteria of an incident is a key element of incident response. The other choices refer to documents that would not likely be included in a computer incident response team (CIRT) manual.

#### NEW QUESTION 397

Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

- A. A hot site facility will be shared in multiple disaster declarations
- B. All equipment is provided "at time of disaster, not on floor"
- C. The facility is subject to a "first-come, first-served" policy
- D. Equipment may be substituted with equivalent model

**Answer:** B

**Explanation:**

Equipment provided "at time of disaster (ATOD), not on floor" means that the equipment is not available but will be acquired by the commercial hot site provider ON a best effort basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations, and that priority may be established on a first-come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

#### NEW QUESTION 402

Detailed business continuity plans should be based PRIMARILY on:

- A. consideration of different alternative
- B. the solution that is least expensiv
- C. strategies that cover all application
- D. strategies validated by senior managemen

**Answer:** D

**Explanation:**

A recovery strategy identifies the best way to recover a system in ease of disaster and provides guidance based on detailed recovery procedures that can be developed. Different strategies should be developed and all alternatives presented to senior management. Senior management should select the most appropriate strategy from the alternatives provided. The selected strategy should be used for further development of the detailed business continuity plan. The selection of strategy depends on criticality of the business process and applications supporting the processes. It need not necessarily cover all applications. All recovery strategies have associated costs, which include costs of preparing for disruptions and putting them to use in the event of a disruption. The latter can be insured against, but not the former. The best recovery option need not be the least expensive.

#### NEW QUESTION 404

When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

- A. Reboot the router connecting the DMZ to the firewall
- B. Power down all servers located on the DMZ segment
- C. Monitor the probe and isolate the affected segment
- D. Enable server trace logging on the affected segment

**Answer:** C

#### Explanation:

In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the demilitarized zone (DMZ) servers and enabling server trace routing are not warranted.

#### NEW QUESTION 409

The business continuity policy should contain which of the following?

- A. Emergency call trees
- B. Recovery criteria
- C. Business impact assessment (BIA)
- D. Critical backups inventory

**Answer:** B

#### Explanation:

Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

#### NEW QUESTION 412

The BEST approach in managing a security incident involving a successful penetration should be to:

- A. allow business processes to continue during the response
- B. allow the security team to assess the attack profile
- C. permit the incident to continue to trace the source
- D. examine the incident response process for deficiencies

**Answer:** A

#### Explanation:

Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted. Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable but it, too, is subordinate to allowing business processes to continue.

#### NEW QUESTION 414

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISM Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISM Product From:

<https://www.2passeasy.com/dumps/CISM/>

## Money Back Guarantee

### CISM Practice Exam Features:

- \* CISM Questions and Answers Updated Frequently
- \* CISM Practice Questions Verified by Expert Senior Certified Staff
- \* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year