

Exam Questions CISM

Certified Information Security Manager

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



NEW QUESTION 1

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- A. Regular password audits
- B. Single sign-on system
- C. Security awareness program
- D. Penalties for noncompliance

Answer: C

Explanation:

To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

NEW QUESTION 2

Which of the following would BEST ensure the success of information security governance within an organization?

- A. Steering committees approve security projects
- B. Security policy training provided to all managers
- C. Security training available to all employees on the intranet
- D. Steering committees enforce compliance with laws and regulations

Answer: A

Explanation:

The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. Compliance with laws and regulations is part of the responsibility of the steering committee but it is not a full answer. Awareness training is important at all levels in any medium, and also an indicator of good governance. However, it must be guided and approved as a security project by the steering committee.

NEW QUESTION 3

Successful implementation of information security governance will FIRST require:

- A. security awareness trainin
- B. updated security policie
- C. a computer incident management tea
- D. a security architectur

Answer: B

Explanation:

Updated security policies are required to align management objectives with security procedures; management objectives translate into policy, policy translates into procedures. Security procedures will necessitate specialized teams such as the computer incident response and management group as well as specialized tools such as the security mechanisms that comprise the security architecture. Security awareness will promote the policies, procedures and appropriate use of the security mechanisms.

NEW QUESTION 4

The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

- A. the plan aligns with the organization's business pla
- B. departmental budgets are allocated appropriately to pay for the pla
- C. regulatory oversight requirements are me
- D. the impact of the plan on the business units is reduce

Answer: A

Explanation:

The steering committee controls the execution of the information security strategy according to the needs of the organization and decides on the project prioritization and the execution plan. The steering committee does not allocate department budgets for business units. While ensuring that regulatory oversight requirements are met could be a consideration, it is not the main reason for the review. Reducing the impact on the business units is a secondary concern but not the main reason for the review.

NEW QUESTION 5

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

- A. organizational ris
- 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 6

Which of the following is the MOST important prerequisite for establishing information security management within an organization?

- A. Senior management commitment
- B. Information security framework
- C. Information security organizational structure
- D. Information security policy

Answer: A

Explanation:

Senior management commitment is necessary in order for each of the other elements to succeed. Without senior management commitment, the other elements will likely be ignored within the organization.

NEW QUESTION 7

The PRIMARY goal in developing an information security strategy is to:

- A. establish security metrics and performance monitorin
- B. educate business process owners regarding their dutie
- C. ensure that legal and regulatory requirements are met
- D. support the business objectives of the organizatio

Answer: D

Explanation:

The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

NEW QUESTION 8

Effective IT governance is BEST ensured by:

- A. utilizing a bottom-up approac
- B. management by the IT departmen
- C. referring the matter to the organization's legal departmen
- D. utilizing a top-down approac

Answer: D

Explanation:

Effective IT governance needs to be a top-down initiative, with the board and executive management setting clear policies, goals and objectives and providing for ongoing monitoring of the same. Focus on the regulatory issues and management priorities may not be reflected effectively by a bottom-up approach. IT governance affects the entire organization and is not a matter concerning only the management of IT. The legal department is part of the overall governance process, but cannot take full responsibility.

NEW QUESTION 9

At what stage of the applications development process should the security department initially become involved?

- A. When requested
- B. At testing
- C. At programming
- D. At detail requirements

Answer: D

Explanation:

Information security has to be integrated into the requirements of the application's design. It should also be part of the information security governance of the organization. The application owner may not make a timely request for security involvement. It is too late during systems testing, since the requirements have already been agreed upon. Code reviews are part of the final quality assurance process.

NEW QUESTION 10

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 10

When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

- A. Create separate policies to address each regulation
- B. Develop policies that meet all mandated requirements
- C. Incorporate policy statements provided by regulators
- D. Develop a compliance risk assessment

Answer: B

Explanation:

It will be much more efficient to craft all relevant requirements into policies than to create separate versions. Using statements provided by regulators will not capture all of the requirements mandated by different regulators. A compliance risk assessment is an important tool to verify that procedures ensure compliance once the policies have been established.

NEW QUESTION 11

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 15

A good privacy statement should include:

- A. notification of liability on accuracy of informatio
- B. notification that information will be encrypte
- C. what the company will do with information it collect
- D. a description of the information classification proces

Answer: C

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. Choice A is incorrect because that information should be located in the web site's disclaimer. Choice B is incorrect because, although encryption may be applied, this is not generally disclosed. Choice D is incorrect because information classification would be contained in a separate policy.

NEW QUESTION 16

Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

- A. Chief security officer (CSO)
- B. Chief operating officer (COO)
- C. Chief privacy officer (CPO)
- D. Chief legal counsel (CLC)

Answer: B

Explanation:

The chief operating officer (COO) is most knowledgeable of business operations and objectives. The chief privacy officer (CPO) and the chief legal counsel (CLC) may not have the knowledge of the day- to-day business operations to ensure proper guidance, although they have the same influence within the organization as the COO. Although the chief security officer (CSO) is knowledgeable of what is needed, the sponsor for this task should be someone with far-reaching influence across the organization.

NEW QUESTION 21

What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

- A. Functional requirements are not adequately considere

- B. User training programs may be inadequate
- C. Budgets allocated to business units are not appropriate
- D. Information security plans are not aligned with business requirements

Answer: D

Explanation:

The steering committee controls the execution of the information security strategy, according to the needs of the organization, and decides on the project prioritization and the execution plan. User management is an important group that should be represented to ensure that the information security plans are aligned with the business needs. Functional requirements and user training programs are considered to be part of the projects but are not the main risks. The steering committee does not approve budgets for business units.

NEW QUESTION 22

When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- A. information security metric
- B. knowledge required to analyze each issue
- C. linkage to business area objective
- D. baseline against which metrics are evaluated

Answer: C

Explanation:

The link to business objectives is the most important element that would be considered by management. Information security metrics should be put in the context of impact to management objectives. Although important, the security knowledge required would not be the first element to be considered. Baseline against the information security metrics will be considered later in the process.

NEW QUESTION 24

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 28

Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

- A. assessing the frequency of incident
- B. quantifying the cost of control failure
- C. calculating return on investment (ROI) projection
- D. comparing spending against similar organizations

Answer: C

Explanation:

Calculating the return on investment (ROI) will most closely align security with the impact on the bottom line. Frequency and cost of incidents are factors that go into determining the impact on the business but, by themselves, are insufficient. Comparing spending against similar organizations can be problematic since similar organizations may have different business goals and appetites for risk.

NEW QUESTION 31

Information security should be:

- A. focused on eliminating all risk
- B. a balance between technical and business requirements
- C. driven by regulatory requirements
- D. defined by the board of directors

Answer: B

Explanation:

Information security should ensure that business objectives are met given available technical capabilities, resource constraints and compliance requirements. It is not practical or feasible to eliminate all risks. Regulatory requirements must be considered, but are inputs to the business considerations. The board of directors does not define information security, but provides direction in support of the business goals and objectives.

NEW QUESTION 35

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- A. it implies compliance risk
- B. short-term impact cannot be determine
- C. it violates industry security practice
- D. changes in the roles matrix cannot be detecte

Answer: A

Explanation:

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

NEW QUESTION 38

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

When developing an information security program, what is the MOST useful source of information for determining available resources?

- A. Proficiency test
- B. Job descriptions
- C. Organization chart
- D. Skills inventory

Answer: D

Explanation:

A skills inventory would help identify- the available resources, any gaps and the training requirements for developing resources. Proficiency testing is useful but only with regard to specific technical skills. Job descriptions would not be as useful since they may be out of date or not sufficiently detailed. An organization chart would not provide the details necessary to determine the resources required for this activity.

NEW QUESTION 45

The MOST useful way to describe the objectives in the information security strategy is through:

- A. attributes and characteristics of the 'desired state.'
- B. overall control objectives of the security progra
- C. mapping the IT systems to key business processe
- D. calculation of annual loss expectation

Answer: A

Explanation:

Security strategy will typically cover a wide variety of issues, processes, technologies and outcomes that can best be described by a set of characteristics and attributes that are desired. Control objectives are developed after strategy and policy development. Mapping IT systems to key business processes does not address strategy issues. Calculation of annual loss expectations would not describe the objectives in the information security strategy.

NEW QUESTION 46

Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- A. Include security responsibilities in the job description
- B. Require the administrator to obtain security certification
- C. Train the system administrator on penetration testing and vulnerability assessment
- D. Train the system administrator on risk assessment

Answer: A

Explanation:

The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the

organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

NEW QUESTION 51

Which of the following should be determined while defining risk management strategies?

- A. Risk assessment criteria
- B. Organizational objectives and risk appetite
- C. IT architecture complexity
- D. Enterprise disaster recovery plans

Answer: B

Explanation:

While defining risk management strategies, one needs to analyze the organization's objectives and risk appetite and define a risk management framework based on this analysis. Some organizations may accept known risks, while others may invest in and apply mitigation controls to reduce risks. Risk assessment criteria would become part of this framework, but only after proper analysis. IT architecture complexity and enterprise disaster recovery plans are more directly related to assessing risks than defining strategies.

NEW QUESTION 56

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

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

Answer: D

Explanation:

A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good, qualified information security professionals.

NEW QUESTION 57

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

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

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 59

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

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

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 (ROI) 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 61

Information security projects should be prioritized on the basis of:

- A. time required for implementation
- B. impact on the organization
- C. total cost for implementation

D. mix of resources require

Answer: B
Explanation:

Explanation:

Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

NEW QUESTION 66

An information security manager must understand the relationship between information security and business operations in order to:

- A. support organizational objective
- B. determine likely areas of noncompliance
- C. assess the possible impacts of compromise
- D. understand the threats to the business

Answer: A

Explanation:

Security exists to provide a level of predictability for operations, support for the activities of the organization and to ensure preservation of the organization. Business operations must be the driver for security activities in order to set meaningful objectives, determine and manage the risks to those activities, and provide a basis to measure the effectiveness of and provide guidance to the security program. Regulatory compliance may or may not be an organizational requirement. If compliance is a requirement, some level of compliance must be supported but compliance is only one aspect. It is necessary to understand the business goals in order to assess potential impacts and evaluate threats. These are some of the ways in which security supports organizational objectives, but they are not the only ways.

NEW QUESTION 71

In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

- A. prepare a security budget
- B. conduct a risk assessment
- C. develop an information security policy
- D. obtain benchmarking information

Answer: B

Explanation:

Risk assessment, evaluation and impact analysis will be the starting point for driving management's attention to information security. All other choices will follow the risk assessment.

NEW QUESTION 75

Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

- A. map the major threats to business objectives
- B. review available sources of risk information
- C. identify the value of the critical assets
- D. determine the financial impact if threats materialize

Answer: A

Explanation:

Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

NEW QUESTION 78

An organization has to comply with recently published industry regulatory requirements—compliance that potentially has high implementation costs. What should the information security manager do FIRST?

- A. Implement a security committee
- B. Perform a gap analysis
- C. Implement compensating controls
- D. Demand immediate compliance

Answer: B

Explanation:

Since they are regulatory requirements, a gap analysis would be the first step to determine the level of compliance already in place. Implementing a security committee or compensating controls would not be the first step. Demanding immediate compliance would not assess the situation.

NEW QUESTION 80

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 82

The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

- A. hourly billing rate charged by the carrier
- B. value of the data transmitted over the network
- C. aggregate compensation of all affected business users
- D. financial losses incurred by affected business unit

Answer: D

Explanation:

The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

NEW QUESTION 86

Previously accepted risk should be:

- A. re-assessed periodically since the risk can be escalated to an unacceptable level due to revised conditions
- B. accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptable
- C. avoided next time since risk avoidance provides the best protection to the company
- D. removed from the risk log once it is accepted

Answer: A

Explanation:

Acceptance of risk should be regularly reviewed to ensure that the rationale for the initial risk acceptance is still valid within the current business context. The rationale for initial risk acceptance may no longer be valid due to change(s) and, hence, risk cannot be accepted permanently. Risk is an inherent part of business and it is impractical and costly to eliminate all risk. Even risks that have been accepted should be monitored for changing conditions that could alter the original decision.

NEW QUESTION 89

Phishing is BEST mitigated by which of the following?

- A. Security monitoring software
- B. Encryption
- C. Two-factor authentication
- D. User awareness

Answer: D

Explanation:

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.

NEW QUESTION 91

Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

- A. Defining job roles
- B. Performing a risk assessment
- C. Identifying data owners
- D. Establishing data retention policies

Answer: C

Explanation:

Identifying the data owners is the first step, and is essential to implementing data classification. Defining job roles is not relevant. Performing a risk assessment is important, but will require the participation of data owners (who must first be identified). Establishing data retention policies may occur after data have been classified.

NEW QUESTION 94

A successful risk management program should lead to:

- A. optimization of risk reduction efforts against cost
- B. containment of losses to an annual budgeted amount
- C. identification and removal of all man-made threat
- D. elimination or transference of all organizational risk

Answer: A

Explanation:

Successful risk management should lead to a breakeven point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, while losses cannot be budgeted in advance with absolute certainty.

NEW QUESTION 97

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 102

Which of the following would be the MOST relevant factor when defining the information classification policy?

- A. Quantity of information
- B. Available IT infrastructure
- C. Benchmarking
- D. Requirements of data owners

Answer: D

Explanation:

When defining the information classification policy, the requirements of the data owners need to be identified. The quantity of information, availability of IT infrastructure and benchmarking may be part of the scheme after the fact and would be less relevant.

NEW QUESTION 104

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

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

Answer: D

Explanation:

Although the information owner may be in a management position and is also considered a user, the information owner role has the responsibility for determining information classification levels. Management is responsible for higher-level issues such as providing and approving budget, supporting activities, etc. The information custodian is responsible for day-to-day security tasks such as protecting information, backing up information, etc. Users are the lowest level. They use the data, but do not classify the data. The owner classifies the data.

NEW QUESTION 108

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

- A. Platform security
- B. Entitlement changes
- C. Intrusion detection
- D. Antivirus controls

Answer: B

Explanation:

Data owners are responsible for assigning user entitlements and approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

NEW QUESTION 110

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- A. Control risk
- B. Inherent risk
- C. Risk exposure
- D. Residual risk

Answer: D

Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

NEW QUESTION 115

Which of the following are the essential ingredients of a business impact analysis (BIA)?

- A. Downtime tolerance, resources and criticality
- B. Cost of business outages in a year as a factor of the security budget
- C. Business continuity testing methodology being deployed
- D. Structure of the crisis management team

Answer: A

Explanation:

The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function. Options B, C and D are all associated with business continuity planning, but are not related to the BIA.

NEW QUESTION 118

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

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

Answer: D

Explanation:

It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

NEW QUESTION 123

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 department
- B. database administrator
- C. chief information officer (CIO).
- D. head of the sales department

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 CIO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

NEW QUESTION 128

Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

- A. Performing a business impact analysis (BIA)
- B. Considering personal information devices as part of the security policy
- C. Initiating IT security training and familiarization
- D. Basing the information security infrastructure on risk assessment

Answer: D

Explanation:

The information security infrastructure should be based on risk. While considering personal information devices as part of the security policy may be a consideration, it is not the most important requirement. A BIA is typically carried out to prioritize business processes as part of a business continuity plan. Initiating IT security training may not be important for the purpose of the information security infrastructure.

NEW QUESTION 133

When implementing security controls, an information security manager must PRIMARILY focus on:

- A. minimizing operational impact
- B. eliminating all vulnerabilities
- C. usage by similar organization
- D. certification from a third part

Answer: A

Explanation:

Security controls must be compatible with business needs. It is not feasible to eliminate all vulnerabilities. Usage by similar organizations does not guarantee that controls are adequate. Certification by a third party is important, but not a primary concern.

NEW QUESTION 138

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 142

An information security organization should PRIMARILY:

- A. support the business objectives of the company by providing security-related support service
- B. be responsible for setting up and documenting the information security responsibilities of the information security team member
- C. ensure that the information security policies of the company are in line with global best practices and standard
- D. ensure that the information security expectations are conveyed to employee

Answer: A

Explanation:

The information security organization is responsible for options B and D within an organization, but they are not its primary mission. Reviewing and adopting appropriate standards (option C) is a requirement. The primary objective of an information security organization is to ensure that security supports the overall business objectives of the company.

NEW QUESTION 146

What is the BEST technique to determine which security controls to implement with a limited budget?

- A. Risk analysis
- B. Annualized loss expectancy (ALE) calculations
- C. Cost-benefit analysis
- D. Impact analysis

Answer: C

Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

NEW QUESTION 148

Information security managers should use risk assessment techniques to:

- A. justify selection of risk mitigation strategie
- B. maximize the return on investment (RO
- C. provide documentation for auditors and regulator

D. quantify risks that would otherwise be subjectiv

Answer: A

Explanation:

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

NEW QUESTION 150

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 151

Which of the following would BEST address the risk of data leakage?

- A. File backup procedures
- B. Database integrity checks
- C. Acceptable use policies
- D. Incident response procedures

Answer: C

Explanation:

Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

NEW QUESTION 156

Identification and prioritization of business risk enables project managers to:

- A. establish implementation milestone
- B. reduce the overall amount of slack tim
- C. address areas with most significanc
- D. accelerate completion of critical path

Answer: C

Explanation:

Identification and prioritization of risk allows project managers to focus more attention on areas of greater importance and impact. It will not reduce the overall amount of slack time, facilitate establishing implementation milestones or allow a critical path to be completed any sooner.

NEW QUESTION 157

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 160

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

- A. password reset
- B. reported incident
- C. incidents resolve
- 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 162

A test plan to validate the security controls of a new system should be developed during which phase of the project?

- A. Testing
- B. Initiation
- C. Design
- D. Development

Answer: C

Explanation:

In the design phase, security checkpoints are defined and a test plan is developed. The testing phase is too late since the system has already been developed and is in production testing. In the initiation phase, the basic security objective of the project is acknowledged. Development is the coding phase and is too late to consider test plans.

NEW QUESTION 164

Who can BEST approve plans to implement an information security governance framework?

- A. Internal auditor
- B. Information security management
- C. Steering committee
- D. Infrastructure management

Answer: C

Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

NEW QUESTION 168

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- A. Security in storage and transmission of sensitive data
- B. Provider's level of compliance with industry standards
- C. Security technologies in place at the facility
- D. Results of the latest independent security review

Answer: A

Explanation:

How the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

NEW QUESTION 172

The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

- A. service level monitorin
- B. penetration testin
- C. periodically auditin
- D. security awareness trainin

Answer: C

Explanation:

Regular audit exercise can spot any gap in the information security compliance. Service level monitoring can only pinpoint operational issues in the organization's operational environment. Penetration testing can identify security vulnerability but cannot ensure information compliance Training can increase users' awareness on the information security policy, but is not more effective than auditing.

NEW QUESTION 174

At what stage of the applications development process would encryption key management initially be addressed?

- A. Requirements development
- B. Deployment
- C. Systems testing
- D. Code reviews

Answer: A

Explanation:

Encryption key management has to be integrated into the requirements of the application's design. During systems testing and deployment would be too late since the requirements have already been agreed upon. Code reviews are part of the final quality assurance (QA) process and would also be too late in the process.

NEW QUESTION 175

Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

- A. Ease of installation
- B. Product documentation
- C. Available support
- D. System overhead

Answer: D

Explanation:

Monitoring products can impose a significant impact ON system overhead for servers and networks. Product documentation, telephone support and ease of installation, while all important, would be secondary.

NEW QUESTION 179

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- A. Stress testing
- B. Patch management
- C. Change management
- D. Security baselines

Answer: C

Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

NEW QUESTION 183

Which of the following devices should be placed within a demilitarized zone (DMZ)?

- A. Network switch
- B. Web server
- C. Database server
- D. File/print server

Answer: B

Explanation:

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

NEW QUESTION 187

Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

- A. Gantt chart
- B. Waterfall chart
- C. Critical path
- D. Rapid Application Development (RAD)

Answer: C

Explanation:

The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

NEW QUESTION 188

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission

outside the organization's network?

- A. Configuration of firewalls
- B. Strength of encryption algorithms
- C. Authentication within application
- D. Safeguards over keys

Answer: D

Explanation:

If keys are in the wrong hands, documents will be able to be read regardless of where they are on the network. Choice A is incorrect because firewalls can be perfectly configured, but if the keys make it to the other side, they will not prevent the document from being decrypted. Choice B is incorrect because even easy encryption algorithms require adequate resources to break, whereas encryption keys can be easily used. Choice C is incorrect because the application "front door" controls may be bypassed by accessing data directly.

NEW QUESTION 193

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- A. invite an external consultant to create the security strateg
- B. allocate budget based on best practice
- C. benchmark similar organization
- D. define high-level business security requirement

Answer: D

Explanation:

All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

NEW QUESTION 195

An e-commerce order fulfillment web server should generally be placed on which of the following?

- A. Internal network
- B. Demilitarized zone (DMZ)
- C. Database server
- D. Domain controller

Answer: B

Explanation:

An e-commerce order fulfillment web server should be placed within a DMZ to protect it and the internal network from external attack. Placing it on the internal network would expose the internal network to potential attack from the Internet. Since a database server should reside on the internal network, the same exposure would exist. Domain controllers would not normally share the same physical device as a web server.

NEW QUESTION 197

When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

- A. calculating the residual ris
- B. enforcing the security standar
- C. redesigning the system chang
- D. implementing mitigating control

Answer: A

Explanation:

Decisions regarding security should always weigh the potential loss from a risk against the existing controls. Each situation is unique; therefore, it is not advisable to always decide in favor of enforcing a standard. Redesigning the proposed change might not always be the best option because it might not meet the business needs. Implementing additional controls might be an option, but this would be done after the residual risk is known.

NEW QUESTION 199

Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

- A. Encrypting first by receiver's private key and second by sender's public key
- B. Encrypting first by sender's private key and second by receiver's public key
- C. Encrypting first by sender's private key and second decrypting by sender's public key
- D. Encrypting first by sender's public key and second by receiver's private key

Answer: B

Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the

receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and, second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

NEW QUESTION 202

An extranet server should be placed:

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

Answer: C

Explanation:

An extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

NEW QUESTION 203

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

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

Answer: D

Explanation:

Planning is the key to effective implementation of information security governance. Consultation, negotiation and facilitation come after planning.

NEW QUESTION 208

The MOST important success factor to design an effective IT security awareness program is to:

- A. customize the content to the target audience
- B. ensure senior management is represented
- C. ensure that all the staff is trained
- D. avoid technical content but give concrete examples

Answer: A

Explanation:

Awareness training can only be effective if it is customized to the expectations and needs of attendees. Needs will be quite different depending on the target audience and will vary between business managers, end users and IT staff; program content and the level of detail communicated will therefore be different. Other criteria are also important; however, the customization of content is the most important factor.

NEW QUESTION 211

What is an appropriate frequency for updating operating system (OS) patches on production servers?

- A. During scheduled rollouts of new applications
- B. According to a fixed security patch management schedule
- C. Concurrently with quarterly hardware maintenance
- D. Whenever important security patches are released

Answer: D

Explanation:

Patches should be applied whenever important security updates are released. They should not be delayed to coincide with other scheduled rollouts or maintenance. Due to the possibility of creating a system outage, they should not be deployed during critical periods of application activity such as month-end or quarter-end closing.

NEW QUESTION 215

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

- A. critical information resources needing protection
- B. a security policy for the entire organization
- C. the minimum acceptable security to be implemented
- 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 217

The information classification scheme should:

- A. consider possible impact of a security breach
- B. classify personal information in electronic form
- C. be performed by the information security manager
- D. classify systems according to the data processes

Answer: A

Explanation:

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Systems are not classified per se, but the data they process and store should definitely be classified.

NEW QUESTION 221

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. Focus 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 223

Security awareness training is MOST likely to lead to which of the following?

- A. Decrease in intrusion incidents
- B. Increase in reported incidents
- C. Decrease in security policy changes
- D. Increase in access rule violations

Answer: B

Explanation:

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

NEW QUESTION 225

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. Hashing can provide integrity and confidentiality. Message authentication codes provide integrity.

NEW QUESTION 226

Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

- A. Never use open source tools
- B. Focus only on production servers

- C. Follow a linear process for attacks
- D. Do not interrupt production processes

Answer: D

Explanation:

The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments since, if compromised, the test environment could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than a linear process.

NEW QUESTION 230

Which of the following is the BEST indicator that an effective security control is built into an organization?

- A. The monthly service level statistics indicate a minimal impact from security issue
- B. The cost of implementing a security control is less than the value of the asset
- C. The percentage of systems that is compliant with security standard
- D. The audit reports do not reflect any significant findings on security

Answer: A

Explanation:

The best indicator of effective security control is the evidence of little disruption to business operations. Choices B, C and D can support this evidence, but are supplemental to choice A.

NEW QUESTION 232

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 234

A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

- A. System monitoring for traffic on network ports
- B. Security code reviews for the entire application
- C. Reverse engineering the application binaries
- D. Running the application from a high-privileged account on a test system

Answer: B

Explanation:

Security code reviews for the entire application is the best measure and will involve reviewing the entire source code to detect all instances of back doors. System monitoring for traffic on network ports would not be able to detect all instances of back doors and is time consuming and would take a lot of effort. Reverse engineering the application binaries may not provide any definite clues. Back doors will not surface by running the application on high-privileged accounts since back doors are usually hidden accounts in the applications.

NEW QUESTION 235

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 240

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 245

To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

- A. create a separate account for the programmer as a power user
- B. log all of the programmers' activity for review by supervisor
- C. have the programmer sign a letter accepting full responsibility
- D. perform regular audits of the application

Answer: B

Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers' actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

NEW QUESTION 250

Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

- A. Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans
- B. Periodic audits of the disaster recovery/business continuity plans
- C. Comprehensive walk-through testing
- D. Inclusion as a required step in the system life cycle process

Answer: D

Explanation:

Information security should be an integral component of the development cycle; thus, it should be included at the process level. Choices A, B and C are good mechanisms to ensure compliance, but would not be nearly as timely in ensuring that the plans are always up-to-date. Choice D is a preventive control, while choices A, B and C are detective controls.

NEW QUESTION 251

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 roles
- C. ensure they successfully pass background checks
- 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 252

The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

- A. identifying vulnerabilities in the system
- B. sustaining the organization's security posture
- C. the existing systems that will be affected
- D. complying with segregation of duties

Answer: B

Explanation:

It is important to maintain the organization's security posture at all times. The focus should not be confined to the new system being developed or acquired, or to the existing systems in use. Segregation of duties is only part of a solution to improving the security of the systems, not the primary reason to involve security in

the systems development life cycle (SDLC).

NEW QUESTION 255

What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

- A. Mandatory
- B. Discretionary
- C. Walled garden
- D. Role-based

Answer: A

Explanation:

Mandatory access controls restrict access to files based on the security classification of the file. This prevents users from sharing files with unauthorized users. Role-based access controls grant access according to the role assigned to a user; they do not prohibit file sharing. Discretionary and lattice-based access controls are not as effective as mandatory access controls in preventing file sharing. A walled garden is an environment that controls a user's access to web content and services. In effect, the walled garden directs the user's navigation within particular areas, and does not necessarily prevent sharing of other material.

NEW QUESTION 257

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

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

Answer: C

Explanation:

The system design specifications phase is when security specifications are identified. The procedural design converts structural components into a procedural description of the software. The architectural design is the phase that identifies the overall system design, but not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.

NEW QUESTION 259

Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

- A. Provide security awareness training to the third-party provider's employees
- B. Conduct regular security reviews of the third-party provider
- C. Include security requirements in the service contract
- D. Request that the third-party provider comply with the organization's information security policy

Answer: B

Explanation:

Regular security audits and reviews of the practices of the provider to prevent potential information security damage will help verify the security of outsourced services. Depending on the type of services outsourced, security awareness may not be necessary. Security requirements should be included in the contract, but what is most important is verifying that the requirements are met by the provider. It is not necessary to require the provider to fully comply with the policy if only some of the policy is related and applicable.

NEW QUESTION 264

Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

- A. Security audit reports
- B. Balanced scorecard
- C. Capability maturity model (CMM)
- D. Systems and business security architecture

Answer: C

Explanation:

The capability maturity model (CMM) grades each defined area of security processes on a scale of 0 to 5 based on their maturity, and is commonly used by entities to measure their existing state and then determine the desired one. Security audit reports offer a limited view of the current state of security. Balanced scorecard is a document that enables management to measure the implementation of their strategy and assists in its translation into action. Systems and business security architecture explain the security architecture of an entity in terms of business strategy, objectives, relationships, risks, constraints and enablers, and provides a business-driven and business-focused view of security architecture.

NEW QUESTION 267

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

- A. authorize
- B. applied
- C. documented
- D. tested

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 269

Which of the following is the MOST likely outcome of a well-designed information security awareness course?

- A. Increased reporting of security incidents to the incident response function
- B. Decreased reporting of security incidents to the incident response function
- C. Decrease in the number of password resets
- D. Increase in the number of identified system vulnerabilities

Answer: A

Explanation:

A well-organized information security awareness course informs all employees of existing security policies, the importance of following safe practices for data security and the need to report any possible security incidents to the appropriate individuals in the organization. The other choices would not be the likely outcomes.

NEW QUESTION 271

What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

- A. Perform periodic penetration testing
- B. Establish minimum security baselines
- C. Implement vendor default settings
- D. Install a honeypot on the network

Answer: D

Explanation:

Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed sporadically. Vendor default settings are not effective.

NEW QUESTION 276

In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

- A. testing time window prior to deployment
- B. technical skills of the team responsible
- C. certification of validity for deployment
- D. automated deployment to all the servers

Answer: A

Explanation:

Having the patch tested prior to implementation on critical systems is an absolute prerequisite where availability is a primary concern because deploying patches that could cause a system to fail could be worse than the vulnerability corrected by the patch. It makes no sense to deploy patches on every system. Vulnerable systems should be the only candidate for patching. Patching skills are not required since patches are more often applied via automated tools.

NEW QUESTION 277

Which of the following measures is the MOST effective deterrent against disgruntled staff abusing their privileges?

- A. Layered defense strategy
- B. System audit log monitoring
- C. Signed acceptable use policy
- D. High-availability systems

Answer: C

Explanation:

A layered defense strategy would only prevent those activities that are outside of the user's privileges. A signed acceptable use policy is often an effective deterrent against malicious activities because of the potential for termination of employment and/or legal actions being taken against the individual. System audit log monitoring is after the fact and may not be effective. High-availability systems have high costs and are not always feasible for all devices and components or systems.

NEW QUESTION 278

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 system
- 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 280

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

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

Answer: B

Explanation:

XSRF exploits inadequate authentication mechanisms in web applications that rely only on elements such as cookies when performing a transaction. XSRF is related to an authentication mechanism, not to redirection. Option C is related to intellectual property rights, not to XSRF vulnerability. Merely hosting multiple applications on the same server is not the root cause of this vulnerability.

NEW QUESTION 285

Successful social engineering attacks can BEST be prevented through:

- A. preemployment screenin
- B. close monitoring of users' access pattern
- C. periodic awareness trainin
- D. efficient termination procedure

Answer: C

Explanation:

Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

NEW QUESTION 288

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

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

Answer: C

Explanation:

Even in the case of an emergency change, all change management procedure steps should be completed as in the case of normal changes. The difference lies in the timing of certain events. With an emergency change, it is permissible to obtain certain approvals and other documentation on "the morning after" once the emergency has been satisfactorily resolved. Obtaining business approval prior to the change is ideal but not always possible.

NEW QUESTION 293

Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

- A. Adequate security policies and procedures
- B. Periodic compliance reviews
- C. Security steering committees
- D. Security awareness campaigns

Answer: D

Explanation:

Security awareness campaigns will be more effective at changing an organizational culture than the creation of steering committees and security policies and procedures. Compliance reviews are helpful; however, awareness by all staff is more effective because compliance reviews are focused on certain areas groups and do not necessarily educate.

NEW QUESTION 295

What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

- A. Provide detailed instructions on how to carry out different types of tasks
- B. Ensure consistency of activities to provide a more stable environment
- C. Ensure compliance to security standards and regulatory requirements
- D. Ensure reusability to meet compliance to quality requirements

Answer: B

Explanation:

Developing procedures and guidelines to ensure that business processes address information security risk is critical to the management of an information security program. Developing procedures and guidelines establishes a baseline for security program performance and consistency of security activities.

NEW QUESTION 299

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 incidents

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 302

Of the following, retention of business records should be PRIMARILY based on:

- A. periodic vulnerability assessments
- B. regulatory and legal requirements
- C. device storage capacity and longevity
- D. past litigation

Answer: B

Explanation:

Retention of business records is a business requirement that must consider regulatory and legal requirements based on geographic location and industry. Options A and C are important elements for making the decision, but the primary driver is the legal and regulatory requirements that need to be followed by all companies. Record retention may take into consideration past litigation, but it should not be the primary decision factor.

NEW QUESTION 305

A security awareness program should:

- A. present top management's perspective
- B. address details on specific exploits
- C. address specific groups and roles
- D. promote security department procedures

Answer: C

Explanation:

Different groups of employees have different levels of technical understanding and need awareness training that is customized to their needs; it should not be presented from a specific perspective. Specific details on technical exploits should be avoided since this may provide individuals with knowledge they might misuse or it may confuse the audience. This is also not the best forum in which to present security department procedures.

NEW QUESTION 306

Which of the following are the MOST important individuals to include as members of an information security steering committee?

- A. Direct reports to the chief information officer
- B. IT management and key business process owners
- C. Cross-section of end users and IT professionals
- D. Internal audit and corporate legal departments

Answer: B

Explanation:

Security steering committees provide a forum for management to express its opinion and take some ownership in the decision making process. It is imperative that business process owners be included in this process. None of the other choices includes input by business process owners.

NEW QUESTION 309

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 313

Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

- A. The right to conduct independent security reviews
- B. A legally binding data protection agreement
- C. Encryption between the organization and the provider
- D. A joint risk assessment of the system

Answer: A

Explanation:

A key requirement of an outsource contract involving critical business systems is the establishment of the organization's right to conduct independent security reviews of the provider's security controls. A legally binding data protection agreement is also critical, but secondary to choice A, which permits examination of the actual security controls prevailing over the system and, as such, is the more effective risk management tool. Network encryption of the link between the organization and the provider may well be a requirement, but is not as critical since it would also be included in choice A. A joint risk assessment of the system in conjunction with the outsource provider may be a compromise solution, should the right to conduct independent security reviews of the controls related to the system prove contractually difficult.

NEW QUESTION 317

In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

- A. ensure access to individual functions can be granted to individual users only
- B. implement role-based access control in the application
- C. enforce manual procedures ensuring separation of conflicting duties
- D. create service accounts that can only be used by authorized team members

Answer: B

Explanation:

Role-based access control is the best way to implement appropriate segregation of duties. Roles will have to be defined once and then the user could be changed from one role to another without redefining the content of the role each time. Access to individual functions will not ensure appropriate segregation of duties. Giving a user access to all functions and implementing, in parallel, a manual procedure ensuring segregation of duties is not an effective method, and would be difficult to enforce and monitor. Creating service accounts that can be used by authorized team members would not provide any help unless their roles are properly segregated.

NEW QUESTION 320

A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

- A. an effective control over connectivity and continuity
- B. a service level agreement (SLA) including code escrow
- C. a business impact analysis (BIA)
- D. a third-party certification

Answer: A

Explanation:

The principal risk focus is the connection procedures to maintain continuity- in case of any contingency. Although an information security manager may be interested in the service level agreement (SLA), code escrow is not a concern. A business impact analysis (BIA) refers to contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

NEW QUESTION 323

An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

- A. Request that the third-party provider perform background checks on their employees
- B. Perform an internal risk assessment to determine needed controls
- C. Audit the third-party provider to evaluate their security controls
- D. Perform a security assessment to detect security vulnerabilities

Answer: B

Explanation:

An internal risk assessment should be performed to identify the risk and determine needed controls. A background check should be a standard requirement for the service provider. Audit objectives should be determined from the risk assessment results. Security assessment does not cover the operational risks.

NEW QUESTION 325

The BEST time to perform a penetration test is after:

- A. an attempted penetration has occurred
- B. an audit has reported weaknesses in security control
- C. various infrastructure changes are made
- D. a high turnover in systems staff

Answer: C

Explanation:

Changes in the systems infrastructure are most likely to inadvertently introduce new exposures. Conducting a test after an attempted penetration is not as productive since an organization should not wait until it is attacked to test its defenses. Any exposure identified by an audit should be corrected before it would be appropriate to test. A turnover in administrative staff does not warrant a penetration test, although it may warrant a review of password change practices and configuration management.

NEW QUESTION 327

When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

- A. Business continuity plan
- B. Disaster recovery plan
- C. Incident response plan
- D. Vulnerability management plan

Answer: C

Explanation:

An incident response plan documents the step-by-step process to follow, as well as the related roles and responsibilities pertaining to all parties involved in responding to an information security breach. A business continuity plan or disaster recovery plan would be triggered during the execution of the incident response plan in the case of a breach impacting the business continuity. A vulnerability management plan is a procedure to address technical vulnerabilities and mitigate the risk through configuration changes (patch management).

NEW QUESTION 329

When creating a forensic image of a hard drive, which of the following should be the FIRST step?

- A. Identify a recognized forensics software tool to create the image
- B. Establish a chain of custody log
- C. Connect the hard drive to a write blocker
- D. Generate a cryptographic hash of the hard drive content

Answer: B

Explanation:

The first step in any investigation requiring the creation of a forensic image should always be to maintain the chain of custody. Identifying a recognized forensics software tool to create the image is one of the important steps, but it should come after several of the other options. Connecting the hard drive to a write blocker is an important step, but it must be done after the chain of custody has been established. Generating a cryptographic hash of the hard drive contents is another important step, but one that comes after several of the other options.

NEW QUESTION 333

An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

- A. Unsure that critical data on the server are backed up
- B. Shut down the compromised server
- C. Initiate the incident response process
- D. Shut down the network

Answer: C

Explanation:

The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

NEW QUESTION 335

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 339

Which of the following application systems should have the shortest recovery time objective (RTO)?

- A. Contractor payroll
- B. Change management
- C. E-commerce web site
- D. Fixed asset system

Answer: C

Explanation:

In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours, if not minutes. Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

NEW QUESTION 341

When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

- A. Business continuity coordinator
- B. Information security manager
- C. Business process owners
- D. Industry averages benchmarks

Answer: C

Explanation:

Business process owners are in the best position to understand the true impact on the business that a system outage would create. The business continuity coordinator, industry averages and even information security will not be able to provide that level of detailed knowledge.

NEW QUESTION 346

What is the BEST method for mitigating against network denial of service (DoS) attacks?

- A. Ensure all servers are up-to-date on OS patches
- B. Employ packet filtering to drop suspect packets
- C. Implement network address translation to make internal addresses nonroutable
- D. Implement load balancing for Internet facing devices

Answer: B

Explanation:

Packet filtering techniques are the only ones which reduce network congestion caused by a network denial of service (DoS) attack. Patching servers, in general, will not affect network traffic. Implementing network address translation and load balancing would not be as effective in mitigating most network DoS attacks.

NEW QUESTION 350

Which of the following actions should be taken when an online trading company discovers a network attack in progress?

- A. Shut off all network access points
- B. Dump all event logs to removable media
- C. Isolate the affected network segment
- D. Enable trace logging on all event

Answer: C

Explanation:

Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

NEW QUESTION 352

An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

- A. Inform senior management
- B. Determine the extent of the compromise

- C. Report the incident to the authorities
- D. Communicate with the affected customer

Answer: B

Explanation:

Before reporting to senior management, affected customers or the authorities, the extent of the exposure needs to be assessed.

NEW QUESTION 355

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

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 359

Detailed business continuity plans should be based PRIMARILY on:

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

Answer: D

Explanation:

A recovery strategy identifies the best way to recover a system in case 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 the 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 361

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 366

The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

- A. weaknesses in network security
- B. patterns of suspicious access
- C. how an attack was launched on the network
- D. potential attacks on the internal network

Answer: D

Explanation:

The most important function of an intrusion detection system (IDS) is to identify potential attacks on the network. Identifying how the attack was launched is secondary. It is not designed specifically to identify weaknesses in network security or to identify patterns of suspicious logon attempts.

NEW QUESTION 369

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

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

Answer: C

Explanation:

The length of the recovery window is defined by business management and determines the acceptable time frame between a disaster and the restoration of critical services/applications. The technical implementation of the disaster recovery (DR) site will be based on this constraint, especially the choice between a hot, warm or cold site. The service delivery objective is supported during the alternate process mode until the normal situation is restored, which is directly related to business needs. The recovery time objective (RTO) is commonly agreed to be the time frame between a disaster and the return to normal operations. It is then longer than the interruption window and is very difficult to estimate in advance. The time frame between the reduced operation mode at the end of the interruption window and the return to normal operations depends on the magnitude of the disaster. Technical disaster recovery solutions alone will not be used for returning to normal operations. Maximum tolerable outage (MTO) is the maximum time acceptable by a company operating in reduced mode before experiencing losses. Theoretically, recovery time objectives (RTOs) equal the interruption window plus the maximum tolerable outage. This will not be the primary factor for the choice of the technical disaster recovery solution.

NEW QUESTION 373

.....

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