Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
When personal information is transmitted across networks, there MUST be adequate controls over:

A. change managemen
B. privacy protectio
C. consent to data transfe
D. encryption device

Answer: B

Explanation:

Privacy protection is necessary to ensure that the receiving party has the appropriate level of protection of personal data. Change management primarily protects only the information, not the privacy of the individuals. Consent is one of the protections that is frequently, but not always, required. Encryption is a method of achieving the actual control, but controls over the devices may not ensure adequate privacy protection and. therefore, is a partial answer.

NEW QUESTION 2
Which of the following is responsible for legal and regulatory liability?

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

Answer: C

Explanation:

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

NEW QUESTION 3
When an organization is implementing an information security governance program, its board of directors should be responsible for:

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

Answer: C

Explanation:

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

NEW QUESTION 4
Which of the following is MOST likely to be discretionary?

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

Answer: C

Explanation:

Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control; as such, they are discretionary.

NEW QUESTION 5
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 6
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

A. escalate issues to an external third party for resolutio
B. ensure that senior management provides authority for security to address the issue
C. insist that managers or units not in agreement with the security solution accept the ris
D. refer the issues to senior management along with any security recommendation

Answer: D

Explanation:

Senior management is in the best position to arbitrate since they will look at the overall needs of the business in reaching a decision. The authority may be delegated to others by senior management after their review of the issues and security recommendations. Units should not be asked to accept the risk without first receiving input from senior management.

NEW QUESTION 7
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 8
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 9
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

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

Answer: B

Explanation:

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules (types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

NEW QUESTION 10
A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BES T approach of the information security manager?

A. Acceptance of the business manager's decision on the risk to the corporation
B. Acceptance of the information security manager's decision on the risk to the corporation
C. Review of the assessment with executive management for final input
D. A new risk assessment and BIA are needed to resolve the disagreement

Answer: C

Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

NEW QUESTION 10
The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

A. generally accepted industry best practice
B. business requirement
C. legislative and regulatory requirement
D. storage availabilit

Answer: B

Explanation:

The primary concern will be to comply with legislation and regulation but only if this is a genuine business requirement. Best practices may be a useful guide but not a primary concern. Legislative and regulatory requirements are only relevant if compliance is a business need. Storage is irrelevant since whatever is needed must be provided

NEW QUESTION 14
The MOST basic requirement for an information security governance program is to:

A. be aligned with the corporate business strateg
B. be based on a sound risk management approac
C. provide adequate regulatory complianc
D. provide best practices for security- initiative

Answer: A

Explanation:

To receive senior management support, an information security program should be aligned with the corporate business strategy. Risk management is a requirement of an information security program which should take into consideration the business strategy. Security governance is much broader than just regulatory compliance. Best practice is an operational concern and does not have a direct impact on a governance program.

NEW QUESTION 19
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

A. Laws and regulations of the country of origin may not be enforceable in the foreign countr
B. A security breach notification might get delayed due to the time differenc
C. Additional network intrusion detection sensors should be installed, resulting in an additional cos
D. The company could lose physical control over the server and be unable to monitor the physical security posture of the server

Answer: A

Explanation:

A company is held to the local laws and regulations of the country in which the company resides, even if the company decides to place servers with a vendor that hosts the servers in a foreign country. A potential violation of local laws applicable to the company might not be recognized or rectified (i.e., prosecuted) due to the lack of knowledge of the local laws that are applicable and the inability to enforce the laws. Option B is not a problem. Time difference does not play a role in a 24/7 environment. Pagers, cellular phones, telephones, etc. are usually available to communicate notifications. Option C is a manageable problem that requires additional funding, but can be addressed. Option D is a problem that can be addressed. Most hosting providers have standardized the level of physical security that is in place. Regular physical audits or a SAS 70 report can address such concerns.

NEW QUESTION 23
While implementing information security governance an organization should FIRST:

A. adopt security standard
B. determine security baseline
C. define the security strateg
D. establish security policie

Answer: C

Explanation:

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

suitable security-standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

NEW QUESTION 25
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

A. performance measuremen
B. integratio
C. alignmen
D. value deliver

Answer: C

Explanation:

Strategic alignment of security with business objectives is a key indicator of performance measurement. In guiding a security program, a meaningful performance measurement will also rely on an understanding of business objectives, which will be an outcome of alignment. Business linkages do not by themselves indicate integration or value delivery. While alignment is an important precondition, it is not as important an indicator.

NEW QUESTION 28
Which of the following is MOST important in developing a security strategy?

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

Answer: B

Explanation:

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

NEW QUESTION 32
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

A. Compliance with international security standard
B. Use of a two-factor authentication syste
C. Existence of an alternate hot site in case of business disruptio
D. Compliance with the organization's information security requirement

Answer: D

Explanation:

Prom a security standpoint, compliance with the organization's information security requirements is one of the most important topics that should be included in the contract with third-party service provider. The scope of implemented controls in any ISO 27001-compliant organization depends on the security requirements established by each organization. Requiring compliance only with this security standard does not guarantee that a service provider complies with the organization's security requirements. The requirement to use a specific kind of control methodology is not usually stated in the contract with third-party service providers.

NEW QUESTION 36
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

A. a statement regarding what the company will do with the information it collect
B. a disclaimer regarding the accuracy of information on its web sit
C. technical information regarding how information is protecte
D. a statement regarding where the information is being hoste

Answer: A

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. A disclaimer is not necessary since it does not refer to data privacy. Technical details regarding how information is protected are not mandatory to publish on the web site and in fact would not be desirable. It is not mandatory to say where information is being hosted.

NEW QUESTION 40
Which of the following should be the FIRST step in developing an information security plan?

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

Answer: B

Explanation:

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

NEW QUESTION 41
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 issu
C. linkage to business area objective
D. baseline against which metrics are evaluate

Answer: C

Explanation:

The link to business objectives is the most important clement 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. Baselining against the information security metrics will be considered later in the process.

NEW QUESTION 46
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 48
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

A. corporate data privacy polic
B. data privacy policy where data are collecte
C. data privacy policy of the headquarters' countr
D. data privacy directive applicable globall

Answer: B

Explanation:

As a subsidiary, the local entity will have to comply with the local law for data collected in the country. Senior management will be accountable for this legal compliance. The policy, being internal, cannot supersede the local law. Additionally, with local regulations differing from the country in which the organization is headquartered, it is improbable that a group wide policy will address all the local legal requirements. In case of data collected locally (and potentially transferred to a country with a different data privacy regulation), the local law applies, not the law applicable to the head office. The data privacy laws are country-specific.

NEW QUESTION 51
Which of the following situations would MOST inhibit the effective implementation of security governance:

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

Answer: D

Explanation:

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

NEW QUESTION 55
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 59
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 61
The MOST important component of a privacy policy is:

A. notification
B. warrantie
C. liabilitie
D. geographic coverag

Answer: A

Explanation:

Privacy policies must contain notifications and opt-out provisions: they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

NEW QUESTION 66
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 71
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 73
Who in an organization has the responsibility for classifying information?

A. Data custodian
B. Database administrator
C. Information security officer
D. Data owner

Answer: D

Explanation:

The data owner has full responsibility over data. The data custodian is responsible for securing the information. The database administrator carries out the technical administration. The information security officer oversees the overall classification management of the information.

NEW QUESTION 78
Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

A. More uniformity in quality of service
B. Better adherence to policies
C. Better alignment to business unit needs
D. More savings in total operating costs

Answer: C

Explanation:

Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

NEW QUESTION 82
When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

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

Answer: C

Explanation:

The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

NEW QUESTION 84
The cost of implementing a security control should not exceed the:

A. annualized loss expectanc
B. cost of an inciden
C. asset valu
D. implementation opportunity cost

Answer: C

Explanation:

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses drat are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

NEW QUESTION 86
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 budge
B. conduct a risk assessmen
C. develop an information security polic
D. obtain benchmarking informatio

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 90
An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

A. ensure that security processes are consistent across the organizatio
B. enforce baseline security levels across the organizatio
C. ensure that security processes are fully documente
D. implement monitoring of key performance indicators for security processe

Answer: A

Explanation:

The organization first needs to move from ad hoc to repeatable processes. The organization then needs to document the processes and implement process monitoring and measurement. Baselining security levels will not necessarily assist in process improvement since baselining focuses primarily on control improvement. The organization needs to standardize processes both before documentation, and before monitoring and measurement.

NEW QUESTION 91
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdiction
B. establish baseline standards for all locations and add supplemental standards as require
C. bring all locations into conformity with a generally accepted set of industry best practice
D. establish a baseline standard incorporating those requirements that all jurisdictions have in commo

Answer: B

Explanation:

It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach—forcing all locations to be in compliance with the regulations places an undue burden on those locations.

NEW QUESTION 95
After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

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

Answer: B

Explanation:

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

NEW QUESTION 98
To determine the selection of controls required to meet business objectives, an information
security manager should:

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

Answer: B

Explanation:

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

NEW QUESTION 101
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 committe
B. Perform a gap analysi
C. Implement compensating control
D. Demand immediate complianc

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 105
All risk management activities are PRIMARILY designed to reduce impacts to:

A. a level defined by the security manage

B. an acceptable level based on organizational risk toleranc
C. a minimum level consistent with regulatory requirement
D. the minimum level possibl

Answer: B

Explanation:

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

NEW QUESTION 109
The value of information assets is BEST determined by:

A. individual business manager
B. business systems analyst
C. information security managemen
D. industry averages benchmarkin

Answer: A

Explanation:

Individual business managers are in the best position to determine the value of information assets since they are most knowledgeable of the assets' impact on the business. Business systems developers and information security managers are not as knowledgeable regarding the impact on the business. Peer companies' industry averages do not necessarily provide detailed enough information nor are they as relevant to the unique aspects of the business.

NEW QUESTION 113
The MOST effective use of a risk register is to:

A. identify risks and assign roles and responsibilities for mitigatio
B. identify threats and probabilitie
C. facilitate a thorough review of all IT-related risks on a periodic basi
D. record the annualized financial amount of expected losses due to risk

Answer: C

Explanation:

A risk register is more than a simple list—it should lie used as a tool to ensure comprehensive documentation, periodic review and formal update of all risk elements in the enterprise's IT and related organization. Identifying risks and assigning roles and responsibilities for mitigation are elements of the register. Identifying threats and probabilities are two elements that are defined in the risk matrix, as differentiated from the broader scope of content in, and purpose for, the risk register. While the annualized loss expectancy (ALE) should be included in the register, this quantification is only a single element in the overall risk analysis program.

NEW QUESTION 116
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 121
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

A. a lack of proper input validation control
B. weak authentication controls in the web application laye
C. flawed cryptographic secure sockets layer (SSL) implementations and short key length
D. implicit web application trust relationship

Answer: A

Explanation:

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web

application trust relationships do not relate directly to the attack.

NEW QUESTION 124
Previously accepted risk should be:

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

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 129
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 131
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

A. Feasibility
B. Design
C. Development
D. Testing

Answer: A

Explanation:

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

NEW QUESTION 134
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 136
Which program element should be implemented FIRST in asset classification and control?

A. Risk assessment
B. Classification
C. Valuation
D. Risk mitigation

Answer: C

Explanation:

Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

NEW QUESTION 139
Which of (lie 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 144
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 147
The recovery point objective (RPO) requires which of the following?

A. Disaster declaration
B. Before-image restoration
C. System restoration
D. After-image processing

Answer: B

Explanation:

The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

NEW QUESTION 149
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 152
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precis
B. security risks are subject to frequent chang
C. reviewers can optimize and reduce the cost of control

D. it demonstrates to senior management that the security function can add valu

Answer: B

Explanation:

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

NEW QUESTION 156
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

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

Answer: B

Explanation:

A security gap analysis is a process which measures all security controls in place against typically good business practice, and identifies related weaknesses. A business impact analysis is less suited to identify security deficiencies. System performance metrics may indicate security weaknesses, but that is not their primary purpose. Incident response processes exist for cases where security weaknesses are exploited.

NEW QUESTION 160
To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

A. Conducting a qualitative and quantitative risk analysi
B. Assigning value to the asset
C. Weighing the cost of implementing the plan v
D. financial los
E. Conducting a business impact analysis (BIA).

Answer: D

Explanation:

BIA is an essential component of an organization's business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. It is the first crucial step in business continuity planning. Qualitative and quantitative risk analysis will have been completed to define the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. Assigning value to assets is part of the BIA process. Weighing the cost of implementing the plan vs. financial loss is another part of the BIA.

NEW QUESTION 164
A risk analysis should:

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

Answer: C

Explanation:

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

NEW QUESTION 167
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

A. Countermeasure cost-benefit analysis
B. Penetration testing
C. Frequent risk assessment programs
D. Annual loss expectancy (ALE) calculation

Answer: A

Explanation:

In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control. Frequent risk assessment programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will

contribute to the value of the risk but. alone, will not justify a control.

NEW QUESTION 171
An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

A. mitigate the impact by purchasing insuranc
B. implement a circuit-level firewall to protect the networ
C. increase the resiliency of security measures in plac
D. implement a real-time intrusion detection syste

Answer: A

Explanation:

Since residual risk will always be too high, the only practical solution is to mitigate the financial impact by purchasing insurance.

NEW QUESTION 176
Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

A. Implement countermeasure
B. Eliminate the ris
C. Transfer the ris
D. Accept the ris

Answer: C

Explanation:

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

NEW QUESTION 177
Which of the following attacks is BEST mitigated by utilizing strong passwords?

A. Man-in-the-middle attack
B. Brute force attack
C. Remote buffer overflow
D. Root kit

Answer: B

Explanation:

A brute force attack is normally successful against weak passwords, whereas strong passwords would not prevent any of the other attacks. Man-in-the-middle attacks intercept network traffic, which could contain passwords, but is not naturally password-protected. Remote buffer overflows rarely require a password to exploit a remote host. Root kits hook into the operating system's kernel and, therefore, operate underneath any authentication mechanism.

NEW QUESTION 180
The valuation of IT assets should be performed by:

A. an IT security manage
B. an independent security consultan
C. the chief financial officer (CFO).
D. the information owne

Answer: D

Explanation:

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

NEW QUESTION 185
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

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

Answer:

C

Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

NEW QUESTION 190
A security risk assessment exercise should be repeated at regular intervals because:

A. business threats are constantly changin
B. omissions in earlier assessments can be addresse
C. repetitive assessments allow various methodologie
D. they help raise awareness on security in the busines

Answer: A

Explanation:

As business objectives and methods change, the nature and relevance of threats change as well. Choice B does not, by itself, justify regular reassessment. Choice C is not necessarily true in all cases. Choice D is incorrect because there are better ways of raising security awareness than by performing a risk assessment.

NEW QUESTION 194
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

A. External auditors
B. A peer group within a similar business
C. Process owners
D. A specialized management consultant

Answer: C

Explanation:

Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties do not have that level of detailed knowledge on the inner workings of the business. Management consultants are expected to have the necessary skills in risk analysis techniques but are still less effective than a group with intimate knowledge of the business.

NEW QUESTION 196
When implementing security controls, an information security manager must PRIMARILY focus on:

A. minimizing operational impact
B. eliminating all vulnerabilitie
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 199
Who is responsible for ensuring that information is classified?

A. Senior management
B. Security manager
C. Data owner
D. Custodian

Answer: C

Explanation:

The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

NEW QUESTION 204
The PRIMARY benefit of performing an information asset classification is to:

A. link security requirements to business objective
B. identify controls commensurate to ris
C. define access right
D. establish ownershi

Answer: B

Explanation:

All choices are benefits of information classification. However, identifying controls that are proportional to the risk in all cases is the primary benefit of the process.

NEW QUESTION 206
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 it's 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 208
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 211
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 215
Which of the following will BEST prevent external security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Securing and analyzing system access logs

Answer: B

Explanation:

Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

NEW QUESTION 219
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

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

Answer: B

Explanation:

Identifying the relevant systems and processes is the best first step. Developing an operational plan for achieving compliance with the legislation is incorrect because it is not the first step. Restricting the collection of personal information comes later. Identifying privacy legislation in other countries would not add much value.

NEW QUESTION 221
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

A. Theft of purchased software
B. Power outage lasting 24 hours
C. Permanent decline in customer confidence
D. Temporary loss of e-mail due to a virus attack

Answer: C

Explanation:

A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

NEW QUESTION 225
An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

A. eliminating the ris
B. transferring the ris
C. mitigating the ris
D. accepting the ris

Answer: C

Explanation:

Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

NEW QUESTION 226
The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

A. determining the scope for inclusion in an information security progra
B. defining the level of access control
C. justifying costs for information resource
D. determining the overall budget of an information security progra

Answer: B

Explanation:

The assigned class of sensitivity and criticality of the information resource determines the level of access controls to be put in place. The assignment of sensitivity and criticality takes place with the information assets that have already been included in the information security program and has only an indirect bearing on the costs to be incurred. The assignment of sensitivity and criticality contributes to, but does not decide, the overall budget of the information security program.

NEW QUESTION 229
Which of the following is the MOST important risk associated with middleware in a client-server environment?

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

Answer: C

Explanation:

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

NEW QUESTION 231
The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

A. Secure Sockets Layer (SSL).
B. Secure Shell (SSH).
C. IP Security (IPSec).

D. Secure/Multipurpose Internet Mail Extensions (S/MIME).

Answer: A

Explanation:

Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet. In typical use, all data transmitted between the customer and the business are, therefore, encrypted by the business's web server and remain confidential. SSH File Transfer Protocol (SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with the SSH-2 protocol to provide secure file transfer. IP Security (IPSec) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPSec operation: transport mode and tunnel mode. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of e-mail encapsulated in MIME; it is not a web transaction protocol.

NEW QUESTION 235
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart
C. Gap analysis
D. Balanced scorecard

Answer: D

Explanation:

The balanced scorecard is most effective for evaluating the degree to which information security objectives are being met. A SWOT analysis addresses strengths, weaknesses, opportunities and threats. Although useful, a SWOT analysis is not as effective a tool.
Similarly, a gap analysis, while useful for identifying the difference between the current state and the desired future state, is not the most appropriate tool. A waterfall chart is used to understand the flow of one process into another.

NEW QUESTION 240
Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

A. Use security tokens for authentication
B. Connect through an IPSec VPN
C. Use https with a server-side certificate
D. Enforce static media access control (MAC) addresses

Answer: B

Explanation:

IPSec effectively prevents man-in-the-middle (MitM) attacks by including source and destination IPs within the encrypted portion of the packet. The protocol is resilient to MitM attacks. Using token-based authentication does not prevent a MitM attack; however, it may help eliminate reusability of stolen cleartext credentials. An https session can be intercepted through Domain Name Server (DNS) or Address Resolution Protocol (ARP) poisoning. ARP poisoning—a specific kind of MitM attack—may be prevented by setting static media access control (MAC) addresses. Nevertheless, DNS and NetBIOS resolution can still be attacked to deviate traffic.

NEW QUESTION 245
Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

A. Biometric authentication
B. Embedded steganographic
C. Two-factor authentication
D. Embedded digital signature

Answer: D

Explanation:

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

NEW QUESTION 246
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 251
An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage crosstraining. Which type of authorization policy would BEST address this practice?

A. Multilevel
B. Role-based
C. Discretionary
D. Attribute-based

Answer: B

Explanation:

A role-based policy will associate data access with the role performed by an individual, thus restricting access to data required to perform the individual's tasks. Multilevel policies are based on classifications and clearances. Discretionary policies leave access decisions up to information resource managers.

NEW QUESTION 253
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

A. an adequate budget for the security progra
B. recruitment of technical IT employee
C. periodic risk assessment
D. security awareness training for employee

Answer: D

Explanation:

An information security manager has to impress upon the human resources department the need for security awareness training for all employees. Budget considerations are more of an accounting function. The human resources department would become involved once they are convinced for the need of security awareness training. Recruiting IT-savvy staff may bring in new employees with better awareness of information security, but that is not a replacement for the training requirements of the other employees. Periodic risk assessments may or may not involve the human resources department function.

NEW QUESTION 254
The BEST metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocke
B. number of packets droppe
C. average throughput rat
D. number of firewall rule

Answer: A

Explanation:

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

NEW QUESTION 258
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

A. Authentication
B. Hardening
C. Encryption
D. Nonrepudiation

Answer: C

Explanation:

Cardholder data should be encrypted using strong encryption techniques. Hardening would be secondary in importance, while nonrepudiation would not be as relevant. Authentication of the point-of-sale (POS) terminal is a previous step to acquiring the card information.

NEW QUESTION 263
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the syste
B. implement multifactor authenticatio
C. rebuild the system from the original installation mediu
D. disconnect the mail server from the networ

Answer: C

Explanation:

Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

NEW QUESTION 264
Which of the following is the MOST effective type of access control?

A. Centralized
B. Role-based
C. Decentralized
D. Discretionary

Answer: B

Explanation:

Role-based access control allows users to be grouped into job-related categories, which significantly cases the required administrative overhead. Discretionary access control would require a greater degree of administrative overhead. Decentralized access control generally requires a greater number of staff to administer, while centralized access control is an incomplete answer.

NEW QUESTION 268
What is the MOST important reason for conducting security awareness programs throughout an organization?

A. Reducing the human risk
B. Maintaining evidence of training records to ensure compliance
C. Informing business units about the security strategy
D. Training personnel in security incident response

Answer: A

Explanation:

People are the weakest link in security implementation, and awareness would reduce this risk. Through security awareness and training programs, individual employees can be informed and sensitized on various security policies and other security topics, thus ensuring compliance from each individual. Laws and regulations also aim to reduce human risk. Informing business units about the security strategy is best done through steering committee meetings or other forums.

NEW QUESTION 271
It is important to develop an information security baseline because it helps to define:

A. critical information resources needing protectio
B. a security policy for the entire organizatio
C. the minimum acceptable security to be impleme nte
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 273
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

A. Number of controls
B. Cost of achieving control objectives
C. Effectiveness of controls
D. Test results of controls

Answer: B

Explanation:

Comparison of cost of achievement of control objectives and corresponding value of assets sought to be protected would provide a sound basis for the information security manager to measure value delivery. Number of controls has no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated. Effectiveness of controls has no correlation with the value of assets unless their costs are also evaluated. Test results of controls have no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated.

NEW QUESTION 277
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager
B. Establish predetermined automatic expiration dates
C. Require managers to e-mail security when the user leaves
D. Ensure each individual has signed a security acknowledgement

Answer: B

Explanation:

Predetermined expiration dates are the most effective means of removing systems access for temporary users. Reliance on managers to promptly send in termination notices cannot always be counted on, while requiring each individual to sign a security acknowledgement would have little effect in this case.

NEW QUESTION 281
Which of the following is MOST effective in protecting against the attack technique known as phishing?

A. Firewall blocking rules
B. Up-to-date signature files
C. Security awareness training
D. Intrusion detection monitoring

Answer: C

Explanation:

Phishing relies on social engineering techniques. Providing good security awareness training will best reduce the likelihood of such an attack being successful. Firewall rules, signature files and intrusion detection system (IDS) monitoring will be largely unsuccessful at blocking this kind of attack.

NEW QUESTION 283
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

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

Answer: A

Explanation:

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

NEW QUESTION 286
Which of the following is the BEST method to securely transfer a message?

A. Password-protected removable media
B. Facsimile transmission in a secured room
C. Using public key infrastructure (PKI) encryption
D. Steganography

Answer: C

Explanation:

Using public key infrastructure (PKI) is currently accepted as the most secure method to transmit e-mail messages. PKI assures confidentiality, integrity and nonrepudiation. The other choices are not methods that are as secure as PKI. Steganography involves hiding a message in an image.

NEW QUESTION 289
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

A. Virtual private network (VPN)
B. Firewalls and routers
C. Biometric authentication
D. Two-factor authentication

Answer: A

Explanation:

Encryption of data in a virtual private network (VPN) ensures that transmitted information is not readable, even if intercepted. Firewalls and routers protect access to data resources inside the network and do not protect traffic in the public network. Biometric and two-factor authentication, by themselves, would not prevent a message from being intercepted and read.

NEW QUESTION 294
The PRIMARY objective of an Internet usage policy is to prevent:

A. access to inappropriate site
B. downloading malicious cod
C. violation of copyright law
D. disruption of Internet acces

Answer: D

Explanation:

Unavailability of Internet access would cause a business disruption. The other three objectives are secondary.

NEW QUESTION 299
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 303
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

A. Prepare an impact assessment repor
B. Conduct a penetration tes
C. Obtain approval from senior managemen
D. Back up the firewall configuration and policy file

Answer: A

Explanation:

An impact assessment report needs to be prepared first by providing the justification for the change, analysis of the changes to be made, the impact if the change does not work as expected, priority of the change and urgency of the change request. Choices B. C and D could be important steps, but the impact assessment report should be performed before the other steps.

NEW QUESTION 304
When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

A. access control matri
B. encryption strengt
C. authentication mechanis
D. data repositor

Answer: A

Explanation:

The access control matrix is the best indicator of the level of compliance with the service level agreement (SLA) data confidentiality clauses. Encryption strength, authentication mechanism and data repository might be defined in the SLA but are not confidentiality compliance indicators.

NEW QUESTION 308
Which of the following areas is MOST susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management
C. Configuration management
D. Incident response management

Answer: C

Explanation:

Configuration management provides the greatest likelihood of security weaknesses through misconfiguration and failure to update operating system (OS) code correctly and on a timely basis.

NEW QUESTION 312
Which would be the BEST recommendation to protect against phishing attacks?

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

Answer: B

Explanation:

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

NEW QUESTION 313
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

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

Answer: A

Explanation:

While choices B, C and D will all assist the currency and coverage of the program, its governance oversight mechanisms are the best method.

NEW QUESTION 317
Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

A. define the circumstances where cryptography should be use
B. define cryp,0?raphic algorithms and key length
C. describe handling procedures of cryptographic key
D. establish the use of cryptographic solution

Answer: A

Explanation:

There should be documented standards- procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

NEW QUESTION 322
What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

A. all use weak encryptio
B. are decrypted by the firewal
C. may be quarantined by mail filter
D. may be corrupted by the receiving mail serve

Answer: C

Explanation:

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

NEW QUESTION 323
Data owners will determine what access and authorizations users will have by:

A. delegating authority to data custodia
B. cloning existing user account
C. determining hierarchical preference
D. mapping to business need

Answer: D

Explanation:

Access and authorizations should be based on business needs. Data custodians implement the decisions made by data owners. Access and authorizations are not to be assigned by cloning existing user accounts or determining hierarchical preferences. By cloning, users may obtain more access rights and privileges than is required to do their job. Hierarchical preferences may be based on individual preferences and not on business needs.

NEW QUESTION 325
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 326
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 syste
B. sustaining the organization's security postur
C. the existing systems that will be affecte
D. complying with segregation of dutie

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 329
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 330
A critical component of a continuous improvement program for information security is:

A. measuring processes and providing feedbac
B. developing a service level agreement (SLA) for securit
C. tying corporate security standards to a recognized international standar
D. ensuring regulatory complianc

Answer: A

Explanation:

If an organization is unable to take measurements that will improve the level of its safety program. then continuous improvement is not possible. Although desirable, developing a service level agreement (SLA) for security, tying corporate security standards to a recognized international standard and ensuring regulatory compliance are not critical components for a continuous improvement program.

NEW QUESTION 333
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, hut not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.

NEW QUESTION 335
Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

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

Answer: D

Explanation:

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

NEW QUESTION 340
Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Reduced number of security violation reports
B. A quantitative evaluation to ensure user comprehension
C. Increased interest in focus groups on security issues
D. Increased number of security violation reports

Answer: B

Explanation:

To truly judge the effectiveness of security awareness training, some means of measurable testing is necessary to confirm user comprehension. Focus groups may or may not provide meaningful feedback but, in and of themselves, do not provide metrics. An increase or reduction in the number of violation reports may not be indicative of a high level of security awareness.

NEW QUESTION 341
Which of the following is an inherent weakness of signature-based intrusion detection systems?

A. A higher number of false positives
B. New attack methods will be missed
C. Long duration probing will be missed
D. Attack profiles can be easily spoofed

Answer: B

Explanation:

Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

NEW QUESTION 346
Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

Answer: C

Explanation:

Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting ;in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

NEW QUESTION 348
Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

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

Answer: C

Explanation:

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

NEW QUESTION 349
What is the MOST important success factor in launching a corporate information security awareness program?

A. Adequate budgetary support
B. Centralized program management
C. Top-down approach
D. Experience of the awareness trainers

Answer: C

Explanation:

Senior management support will provide enough resources and will focus attention to the program: training should start at the top levels to gain support and sponsorship. Funding is not a primary concern. Centralized management does not provide sufficient support. Trainer experience, while important, is not the primary success factor.

NEW QUESTION 351
An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

A. Research best practices
B. Meet with stakeholders
C. Establish change control procedures
D. Identify critical systems

Answer: B

Explanation:

No new process will be successful unless it is adhered to by all stakeholders; to the extent stakeholders have input, they can be expected to follow the process. Without consensus agreement from the stakeholders, the scope of the research is too wide; input on the current environment is necessary to focus research effectively. It is premature to implement procedures without stakeholder consensus and research. Without knowing what the process will be the parameters to baseline are unknown as well.

NEW QUESTION 352
The BEST way to ensure that an external service provider complies with organizational security policies is to:

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

Answer: D

Explanation:

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

NEW QUESTION 353
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 deploymen
B. technical skills of the team responsibl
C. certification of validity for deploymen
D. automated deployment to all the server

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 355
When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/disaster recovery plans is because:

A. this is a requirement of the security polic
B. software licenses may expire in the future without warnin
C. the asset inventory must be maintaine
D. service level agreements may not otherwise be me

Answer: D

Explanation:

The key requirement is to preserve availability of business operations. Choice A is a correct compliance requirement, but is not the main objective in this case. Choices B and C are supplementary requirements for business continuity/disaster recovery planning.

NEW QUESTION 358
Which of the following measures is the MOST effective deterrent against disgruntled stall 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 360
Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

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

Answer: D

Explanation:

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

NEW QUESTION 361
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 362
As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A. considered at the discretion of the information owne
B. approved by the next higher person in the organizational structur
C. formally managed within the information security framewor
D. reviewed and approved by the security manage

Answer: C

Explanation:

A formal process for managing exceptions to information security policies and standards should be included as part of the information security framework. The other options may be contributors to the process but do not in themselves constitute a formal process.

NEW QUESTION 364
Which of the following is the MOST effective at preventing an unauthorized individual from following an authorized person through a secured entrance (tailgating or piggybacking)?

A. Card-key door locks
B. Photo identification
C. Biometric scanners
D. Awareness training

Answer: D

Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. The other choices are physical controls which by themselves would not be effective against tailgating.

NEW QUESTION 365
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

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

Answer: D

Explanation:

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

NEW QUESTION 367
Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

A. are compatible with the provider's own classificatio
B. are communicated to the provide
C. exceed those of the outsource
D. are stated in the contrac

Answer: D

Explanation:

The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A. B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

NEW QUESTION 369
When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

A. submit the issue to the steering committe
B. conduct an impact analysis to quantify the risk
C. isolate the system from the rest of the networ
D. request a risk acceptance from senior managemen

Answer: B

Explanation:

An impact analysis is warranted to determine whether a risk acceptance should be granted and to demonstrate to the department the danger of deviating from the established policy. Isolating the system would not support the needs of the business. Any waiver should be granted only after performing an impact analysis.

NEW QUESTION 371
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 i
C. Employees are receptive to changes that were implemente
D. There is an immediate reduction in reported incident

Answer: A

Explanation:

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

NEW QUESTION 375
What is the MOST cost-effective method of identifying new vendor vulnerabilities?

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

Answer: A

Explanation:

External vulnerability sources are going to be the most cost-effective method of identifying these vulnerabilities. The cost involved in choices B and C would be much higher, especially if performed at regular intervals. Honeypots would not identify all vendor vulnerabilities. In addition, honeypots located in the DMZ can create a security risk if the production network is not well protected from traffic from compromised honey pots.

NEW QUESTION 377
The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

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

Answer: C

Explanation:

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

NEW QUESTION 378
Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

A. To mitigate technical risks
B. To have an independent certification of network security
C. To receive an independent view of security exposures
D. To identify a complete list of vulnerabilities

Answer: C

Explanation:

Even though the organization may have the capability to perform penetration testing with internal resources, third-party penetration testing should be performed to gain an independent view of the security exposure. Mitigating technical risks is not a direct result of a penetration test. A penetration test would not provide certification of network security nor provide a complete list of vulnerabilities.

NEW QUESTION 381
Which of the following will BEST protect against malicious activity by a former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

Answer: D

Explanation:

When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important, but are not as effective in preventing this type of situation.

NEW QUESTION 382
Which of the following is the BEST indicator that security awareness training has been effective?

A. Employees sign to acknowledge the security policy
B. More incidents are being reported
C. A majority of employees have completed training
D. No incidents have been reported in three months

Answer: B

Explanation:

More incidents being reported could be an indicator that the staff is paying more attention to security. Employee signatures and training completion may or may not have anything to do with awareness levels. The number of individuals trained may not indicate they are more aware. No recent security incidents does not reflect awareness levels, but may prompt further research to confirm.

NEW QUESTION 387
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 388
Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

A. Card key door locks
B. Photo identification
C. Awareness training
D. Biometric scanners

Answer: C

Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. Choices A, B and D are physical controls that, by themselves, would not be effective against tailgating.

NEW QUESTION 392
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 395
The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performanc
B. use a honeypot to check for unusual activit
C. audit the configuration of the ID
D. benchmark the IDS against a peer sit

Answer: A

Explanation:

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

NEW QUESTION 397
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audit
B. Perform periodic penetration testin
C. Define and monitor security metric
D. Survey business units for feedbac

Answer: C

Explanation:

Defining and monitoring security metrics is a good approach to analyze the performance of the security management process since it determines the baseline and evaluates the performance against the baseline to identify an opportunity for improvement. This is a systematic and structured approach to process improvement. Audits will identify deficiencies in established controls; however, they are not effective in evaluating the overall performance for improvement. Penetration testing will only uncover technical vulnerabilities, and cannot provide a holistic picture of information security management, feedback is subjective and not necessarily reflective of true performance.

NEW QUESTION 400
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 continuit

B. a service level agreement (SLA) including code escro
C. a business impact analysis (BIA).
D. a third-party certificatio

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 402
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

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

Answer: B

Explanation:

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

NEW QUESTION 407
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

A. Review the procedures for granting access
B. Establish procedures for granting emergency access
C. Meet with data owners to understand business needs
D. Redefine and implement proper access rights

Answer: C

Explanation:

An information security manager must understand the business needs that motivated the change prior to taking any unilateral action. Following this, all other choices could be correct depending on the priorities set by the business unit.

NEW QUESTION 412
A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

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

Answer: A

Explanation:

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

NEW QUESTION 416
Which of the following would present the GREATEST risk to information security?

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

Answer: D

Explanation:

Security incidents are configured to capture system events that are important from the security perspective; they include incidents also captured in the security

access logs and other monitoring tools. Although, in some instances, they could wait for a few days before they are researched, from the options given this would have the greatest risk to security. Most often, they should be analyzed as soon as possible. Virus signatures should be updated as often as they become available by the vendor, while critical patches should be installed as soon as they are reviewed and tested, which could occur in 24 hours.

NEW QUESTION 420
The PRIMARY objective of security awareness is to:

A. ensure that security policies are understoo
B. influence employee behavio
C. ensure legal and regulatory compliance
D. notify of actions for noncomplianc

Answer: B

Explanation:

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

NEW QUESTION 423
An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

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

Answer: C

Explanation:

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

NEW QUESTION 426
Isolation and containment measures lor a compromised computer have been taken and information security management is now investigating. What is the MOST appropriate next step?

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

Answer: C

Explanation:

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

NEW QUESTION 428
Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m. (23.00 hrs.)?

A. Most new viruses* signatures are identified over weekends
B. Technical personnel are not available to support the operation
C. Systems are vulnerable to new viruses during the intervening week
D. The update's success or failure is not known until Monday

Answer: C

Explanation:

Updating virus signature files on a weekly basis carries the risk that the systems will be vulnerable to viruses released during the week; far more frequent updating is essential. All
other issues are secondary to this very serious exposure.

NEW QUESTION 433
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewall
B. bastion host
C. decoy file

D. screened subnet

Answer: C

Explanation:

Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

NEW QUESTION 437
Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

A. Preparedness tests
B. Paper tests
C. Full operational tests
D. Actual service disruption

Answer: A

Explanation:

Preparedness tests would involve simulation of the entire test in phases and help the team better understand and prepare for the actual test scenario. Options B, C and D are not cost-effective ways to establish plan effectiveness. Paper tests in a walk-through do not include simulation and so there is less learning and it is difficult to obtain evidence that the team has understood the test plan. Option D is not recommended in most cases. Option C would require an approval from management is not easy or practical to test in most scenarios and may itself trigger a disaster.

NEW QUESTION 440
Which of the following has the highest priority when defining an emergency response plan?

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

Answer: C

Explanation:

The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

NEW QUESTION 441
A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GRF.ATEST weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks
B. The hot site may have to be shared with other customers
C. The time of declaration determines site access priority
D. The provider services all major companies in the area

Answer: D

Explanation:

Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. Access to a hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

NEW QUESTION 444
A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

A. Run a port scan on the system
B. Disable the logon ID
C. Investigate the system logs
D. Validate the incident

Answer: D

Explanation:

When investigating a possible incident, it should first be validated. Running a port scan on the system, disabling the logon IDs and investigating the system logs may be required based on preliminary forensic investigation, but doing so as a first step may destroy the evidence.

NEW QUESTION 449
Why is "slack space" of value to an information security manager as pan of an incident investigation?

A. Hidden data may be stored there
B. The slack space contains login information
C. Slack space is encrypted
D. It provides flexible space for the investigation

Answer: A

Explanation:

"Slack space" is the unused space between where the fdc data end and the end of the cluster the data occupy. Login information is not typically stored in the slack space. Encryption for the slack space is no different from the rest of the file system. The slack space is not a viable means of storage during an investigation.

NEW QUESTION 451
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the inciden
B. notify senior managemen
C. start containmen
D. notify law enforcemen

Answer: A

Explanation:

Asserting that the condition is a true security incident is the necessary first step in determining the correct response. The containment stage would follow. Notifying senior management and law enforcement could be part of the incident response process that takes place after confirming an incident.

NEW QUESTION 453
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 458
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 463
Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite
B. Conduct an assessment to determine system status
C. Perform an impact analysis of the outage
D. Isolate the screened subnet

Answer: B

Explanation:

An assessment should be conducted to determine whether any permanent damage occurred and the overall system status. It is not necessary at this point to rebuild any servers. An impact analysis of the outage or isolating the demilitarized zone (DMZ) or screen subnet will not provide any immediate benefit.

NEW QUESTION 467
Which of the following is MOST closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy

C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

Answer: D

Explanation:

Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

NEW QUESTION 471
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The CISM Practice Test Here