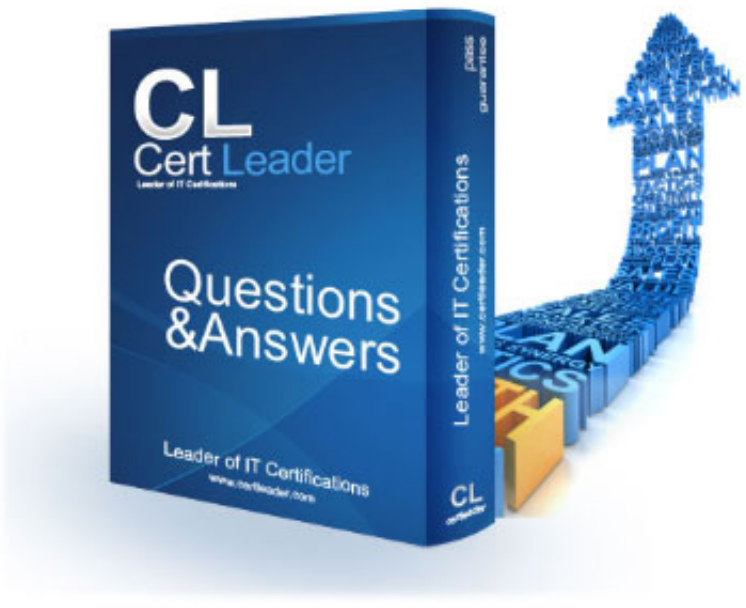
CISM Dumps

Certified Information Security Manager

https://www.certleader.com/CISM-dumps.html



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

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

Answer: C

Explanation:

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

NEW QUESTION 3
Which of the following would be MOST effective in successfully implementing restrictive password policies?

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

Answer: C

Explanation:

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

NEW QUESTION 4
The FIRST step in establishing a security governance program is to:

A. conduct a risk assessmen
B. conduct a workshop for all end user
C. prepare a security budge
D. obtain high-level sponsorshi

Answer: D

Explanation:

The establishment of a security governance program is possible only with the support and sponsorship of top management since security governance projects are enterprise wide and integrated into business processes. Conducting a risk assessment, conducting a workshop for all end users and preparing a security budget all follow once high-level sponsorship is obtained.

NEW QUESTION 5
Which of the following is MOST important to understand when developing a meaningful information security strategy?

A. Regulatory environment
B. International security standards
C. Organizational risks
D. Organizational goals

Answer: D

Explanation:

Alignment of security with business objectives requires an understanding of what an organization is trying to accomplish. The other choices are all elements that must be considered, but their importance is secondary and will vary depending on organizational goals.

NEW QUESTION 6
An outcome of effective security governance is:

A. business dependency assessment
B. strategic alignmen
C. risk assessmen
D. plannin

Answer: B

Explanation:

Business dependency assessment is a process of determining the dependency of a business on certain information resources. It is not an outcome or a product of effective security management. Strategic alignment is an outcome of effective security governance. Where there is good governance, there is likely to be strategic alignment. Risk assessment is not an outcome of effective security governance; it is a process. Planning comes at the beginning of effective security governance, and is not an outcome but a process.

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
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the
Information security program?

A. Representation by regional business leaders
B. Composition of the board
C. Cultures of the different countries
D. IT security skills

Answer: C

Explanation:

Culture has a significant impact on how information security will be implemented. Representation by regional business leaders may not have a major influence unless it concerns cultural issues. Composition of the board may not have a significant impact compared to cultural issues. IT security skills are not as key or high impact in designing a multinational information security program as would be cultural issues.

NEW QUESTION 9
Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

A. Obtain the support of the board of director
B. Improve the content of the information security awareness progra
C. Improve the employees' knowledge of security policie
D. Implement logical access controls to the information system

Answer: A

Explanation:

It is extremely difficult to implement an information security program without the aid and support of the board of directors. If they do not understand the importance of security to the achievement of the business objectives, other measures will not be sufficient. Options B and (' are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

NEW QUESTION 10
Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

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

Answer: B

Explanation:

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

NEW QUESTION 10
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)
D. Return on security investment report

Answer: B

Explanation:

Performing a risk assessment will allow the information security manager to prioritize the remedial measures and provide a means to convey a sense of urgency to management. Metrics reports are normally contained within the methodology of the risk assessment to give it credibility and provide an ongoing tool. The business impact analysis (BIA) covers continuity risks only. Return on security investment cannot be determined until a plan is developed based on the BIA.

NEW QUESTION 11
Information security governance is PRIMARILY driven by:

A. technology constraint
B. regulatory requirement
C. litigation potentia
D. business strateg

Answer: D

Explanation:

Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily in line with the business strategy.

NEW QUESTION 14
The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

A. head of internal audi
B. chief operations officer (COO).
C. chief technology officer (CTO).
D. legal counse

Answer: B

Explanation:

The chief information security officer (CISO) should ideally report to as high a level within the organization as possible. Among the choices given, the chief operations officer (COO) would have not only the appropriate level but also the knowledge of day-to-day operations. The head of internal audit and legal counsel would make good secondary choices, although they would not be as knowledgeable of the operations. Reporting to the chief technology officer (CTO) could become problematic as the CTO's goals for the infrastructure might, at times, run counter to the goals of information security.

NEW QUESTION 16
Who should be responsible for enforcing access rights to application data?

A. Data owners
B. Business process owners
C. The security steering committee
D. Security administrators

Answer: D

Explanation:

As custodians, security administrators are responsible for enforcing access rights to data. Data owners are responsible for approving these access rights. Business process owners are sometimes the data owners as well, and would not be responsible for enforcement. The security steering committee would not be responsible for enforcement.

NEW QUESTION 21
Information security policy enforcement is the responsibility of the:

A. security steering committe
B. chief information officer (CIO).
C. chief information security officer (CISO).
D. chief compliance officer (CCO).

Answer: C

Explanation:

Information security policy enforcement is the responsibility of the chief information security officer (CISO), first and foremost. The board of directors and executive management should ensure that a security policy is in line with corporate objectives. The chief information officer (CIO) and the chief compliance officer (CCO) are involved in the enforcement of the policy but are not directly responsible for it.

NEW QUESTION 26
Which of the following is the MOST important factor when designing information security architecture?

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

Answer: D

Explanation:

The most important factor for information security is that it advances the interests of the business, as defined by stakeholder requirements. Interoperability and scalability, as well as development methodologies, are all important but are without merit if a technologically-elegant solution is achieved that does not meet the needs of the business.

NEW QUESTION 28
The FIRST step in developing an information security management program is to:

A. identify business risks that affect the organizatio
B. clarify organizational purpose for creating the progra
C. assign responsibility for the progra
D. assess adequacy of controls to mitigate business risk

Answer: B

Explanation:

In developing an information security management program, the first step is to clarify the organization's purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

NEW QUESTION 31
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

A. Alignment with industry best practices
B. Business continuity investment
C. Business benefits
D. Regulatory compliance

Answer: D

Explanation:

Regulatory compliance can be a standalone driver for an information security governance measure. No further analysis nor justification is required since the entity has no choice in the regulatory requirements. Buy-in from business managers must be obtained by the information security manager when an information security governance measure is sought based on its alignment with industry best practices. Business continuity investment needs to be justified by business impact analysis. When an information security governance measure is sought based on qualitative business benefits, further analysis is required to determine whether the benefits outweigh the cost of the information security governance measure in question.

NEW QUESTION 36
Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awarenes
B. It is easier to manage and contro
C. It is more responsive to business unit need
D. It provides a faster turnaround for security request

Answer: B

Explanation:

It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization. Decentralization allows you to use

field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

NEW QUESTION 40
Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

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

Answer: A

Explanation:

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

NEW QUESTION 43
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 48
Which of the following is the MOST important information to include in a strategic plan for information security?

A. Information security staffing requirements
B. Current state and desired future state
C. IT capital investment requirements
D. information security mission statement

Answer: B

Explanation:

It is most important to paint a vision for the future and then draw a road map from the stalling point to the desired future state. Staffing, capital investment and the mission all stem from this foundation.

NEW QUESTION 53
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

A. Defining and ratifying the classification structure of information assets
B. Deciding the classification levels applied to the organization's information assets
C. Securing information assets in accordance with their classification
D. Checking if information assets have been classified properly

Answer: A

Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

NEW QUESTION 57
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 61
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

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

Answer: D

Explanation:

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

NEW QUESTION 66
Which of the following would BEST prepare an information security manager for regulatory reviews?

A. Assign an information security administrator as regulatory liaison
B. Perform self-assessments using regulatory guidelines and reports
C. Assess previous regulatory reports with process owners input
D. Ensure all regulatory inquiries are sanctioned by the legal department

Answer: B

Explanation:

Self-assessments provide the best feedback on readiness and permit identification of items requiring remediation. Directing regulators to a specific person or department, or assessing previous reports, is not as effective. The legal department should review all formal inquiries but this does not help prepare for a regulatory review.

NEW QUESTION 71
At what stage of the applications development process should the security department initially become involved?

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

Answer: D

Explanation:

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

NEW QUESTION 75
Acceptable levels of information security risk should be determined by:

A. legal counse
B. security managemen
C. external auditor
D. die steering committe

Answer: D

Explanation:

Senior management, represented in the steering committee, has ultimate responsibility for determining what levels of risk the organization is willing to assume. Legal counsel, the external auditors and security management are not in a position to make such a decision.

NEW QUESTION 78
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 83
Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

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

Answer: D

Explanation:

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

NEW QUESTION 86
When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

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

Answer: B

Explanation:

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

NEW QUESTION 90
Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

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

Answer: D

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

NEW QUESTION 94
A good privacy statement should include:

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

Answer: C

Explanation:

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

NEW QUESTION 96
Retention of business records should PRIMARILY be based on:

A. business strategy and directio
B. regulatory and legal requirement

C. storage capacity and longevit
D. business ease and value analysi

Answer: B

Explanation:

Retention of business records is generally driven by legal and regulatory requirements. Business strategy and direction would not normally apply nor would they override legal and regulatory requirements. Storage capacity and longevity are important but secondary issues. Business case and value analysis would be secondary to complying with legal and regulatory requirements.

NEW QUESTION 100
Which of the following are seldom changed in response to technological changes?

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

Answer: C

Explanation:

Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

NEW QUESTION 105
The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

A. storage capacity and shelf lif
B. regulatory and legal requirement
C. business strategy and directio
D. application systems and medi

Answer: D

Explanation:

Long-term retention of business records may be severely impacted by changes in application systems and media. For example, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply, nor do legal and regulatory requirements. Storage capacity and shelf life are important but secondary issues.

NEW QUESTION 106
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 108
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 112
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 115
The MOST appropriate role for senior management in supporting information security is the:

A. evaluation of vendors offering security product
B. assessment of risks to the organizatio
C. approval of policy statements and fundin
D. monitoring adherence to regulatory requirement

Answer: C

Explanation:

Since the members of senior management are ultimately responsible for information security, they are the ultimate decision makers in terms of governance and direction. They are responsible for approval of major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager; in some organizations, business management is involved in these other activities, though their primary role is direction and governance.

NEW QUESTION 118
Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

A. Key control monitoring
B. A robust security awareness program
C. A security program that enables business activities
D. An effective security architecture

Answer: C

Explanation:

A security program enabling business activities would be most helpful to achieve alignment between information security and organization objectives. All of the other choices are part of the security program and would not individually and directly help as much as the security program.

NEW QUESTION 122
Which of the following is MOST appropriate for inclusion in an information security strategy?

A. Business controls designated as key controls
B. Security processes, methods, tools and techniques
C. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
D. Budget estimates to acquire specific security tools

Answer: B

Explanation:

A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to periodic change, and are not appropriate content for a strategy document.

NEW QUESTION 124
Which of the following would be the MOST important goal of an information security governance program?

A. Review of internal control mechanisms
B. Effective involvement in business decision making
C. Total elimination of risk factors
D. Ensuring trust in data

Answer: D

Explanation:

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true. Involvement in decision making is important only to ensure business data integrity so that data can be trusted.

NEW QUESTION 126
A security manager meeting the requirements for the international flow of personal data will need to ensure:

A. a data processing agreemen
B. a data protection registratio
C. the agreement of the data subject
D. subject access procedure

Answer: C

Explanation:

Whenever personal data are transferred across national boundaries, the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

NEW QUESTION 131
Which of the following roles would represent a conflict of interest for an information security manager?

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

Answer: C

Explanation:

Since management is ultimately responsible for information security, it should approve information security policy statements; the information security manager should not have final approval. Evaluation of third parties requesting access, assessment of disaster recovery plans and monitoring of compliance with physical security controls are acceptable practices and do not present any conflicts of interest.

NEW QUESTION 136
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 139
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 142
The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

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

Answer: D

Explanation:

A business case shows both direct and indirect benefits, along with the investment required and the expected returns, thus making it useful to present to senior management. Return on investment (ROD would only provide the costs needed to preclude specific risks, and would not provide other indirect benefits such as process improvement and learning. A vulnerability assessment is more technical in nature and would only identify and assess the vulnerabilities. This would also not provide insights on indirect benefits. Annual loss expectancy (ALE) would not weigh the advantages of implementing single sign-on (SSO) in comparison to the cost of implementation.

NEW QUESTION 146
Who should drive the risk analysis for an organization?

A. Senior management
B. Security manager
C. Quality manager
D. Legal department

Answer: B

Explanation:

Although senior management should support and sponsor a risk analysis, the know-how and the management of the project will be with the security department. Quality management and the legal department will contribute to the project.

NEW QUESTION 149
The PRIMARY purpose of using risk analysis within a security program is to:

A. justify the security expenditur
B. help businesses prioritize the assets to be protecte
C. inform executive management of residual risk valu
D. assess exposures and plan remediatio

Answer: D

Explanation:

Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

NEW QUESTION 154
One way to determine control effectiveness is by determining:

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

Answer: C

Explanation:

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

NEW QUESTION 156
Which of the following would a security manager establish to determine the target for restoration of normal processing?

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

Answer: A

Explanation:

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

NEW QUESTION 157
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 159
The BEST strategy for risk management is to:

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

Answer: B

Explanation:

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

NEW QUESTION 163
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 165
Which of the following steps in conducting a risk assessment should be performed FIRST?

A. Identity business assets
B. Identify business risks
C. Assess vulnerabilities
D. Evaluate key controls

Answer: A

Explanation:

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

NEW QUESTION 170
A risk management program would be expected to:

A. remove all inherent ris
B. maintain residual risk at an acceptable leve
C. implement preventive controls for every threa
D. reduce control risk to zer

Answer: B

Explanation:

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

NEW QUESTION 172
Which of the following is the PRIMARY reason for implementing a risk management program?

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

Answer: B

Explanation:

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

NEW QUESTION 174
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 178
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

A. Business continuity coordinator
B. Chief operations officer (COO)
C. Information security manager
D. Internal audit

Answer: B

Explanation:

The recovery point objective (RPO) is the processing checkpoint to which systems are recovered. In addition to data owners, the chief operations officer (COO) is the most knowledgeable person to make this decision. It would be inappropriate for the information security manager or an internal audit to determine the RPO because they are not directly responsible for the data or the operation.

NEW QUESTION 180
The MAIN reason why asset classification is important to a successful information security program is because classification determines:

A. the priority and extent of risk mitigation effort
B. the amount of insurance needed in case of los
C. the appropriate level of protection to the asse
D. how protection levels compare to peer organization

Answer: C

Explanation:

Protection should be proportional to the value of the asset. Classification is based upon the value of the asset to the organization. The amount of insurance needed in case of loss may not be applicable in each case. Peer organizations may have different classification schemes for their assets.

NEW QUESTION 185
An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

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

Answer: C

Explanation:

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

NEW QUESTION 190
Which of the following are the essential ingredients of a business impact analysis (B1A)?

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

Answer: A

Explanation:

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

NEW QUESTION 191
The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

A. ensure the provider is made liable for losse
B. recommend not renewing the contract upon expiratio
C. recommend the immediate termination of the contrac
D. determine the current level of securit

Answer: D

Explanation:

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

NEW QUESTION 196
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 198
The criticality and sensitivity of information assets is determined on the basis of:

A. threat assessmen
B. vulnerability assessmen
C. resource dependency assessmen
D. impact assessmen

Answer: D

Explanation:

The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

NEW QUESTION 199
The PRIMARY objective of a risk management program is to:

A. minimize inherent ris
B. eliminate business ris
C. implement effective control
D. minimize residual ris

Answer: D

Explanation:

The goal of a risk management program is to ensure that residual risk remains within manageable levels. Management of risk does not always require the removal of inherent risk nor is this always possible. A possible benefit of good risk management is to reduce insurance premiums, but this is not its primary intention. Effective controls are naturally a clear objective of a risk management program, but with the choices given, choice C is an incomplete answer.

NEW QUESTION 200
A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this
decision is that:

A. there are sufficient safeguards in place to prevent this risk from happenin
B. the needed countermeasure is too complicated to deplo
C. the cost of countermeasure outweighs the value of the asset and potential los
D. The likelihood of the risk occurring is unknow

Answer: C

Explanation:

An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

NEW QUESTION 202
The purpose of a corrective control is to:

A. reduce adverse event
B. indicate compromis
C. mitigate impac
D. ensure complianc

Answer: C

Explanation:

Corrective controls serve to reduce or mitigate impacts, such as providing recovery capabilities. Preventive controls reduce adverse events, such as firewalls. Compromise can be detected by detective controls, such as intrusion detection systems (IDSs). Compliance could be ensured by preventive controls, such as access controls.

NEW QUESTION 204
A risk management approach to information protection is:

A. managing risks to an acceptable level, commensurate with goals and objective
B. accepting the security posture provided by commercial security product
C. implementing a training program to educate individuals on information protection and risk
D. managing risk tools to ensure that they assess all information protection vulnerabilitie

Answer: A

Explanation:

Risk management is identifying all risks within an organization, establishing an acceptable level of risk and effectively managing risks which may include mitigation or transfer. Accepting the security- posture provided by commercial security products is an approach that would be limited to technology components and may not address all business operations of the organization. Education is a part of the overall risk management process. Tools may be limited to technology and would not address non-technology risks.

NEW QUESTION 209
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 212
An information security organization should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 215
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 217
Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

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

Answer: D

Explanation:

Risk should be addressed as early as possible in the development cycle. The feasibility study should include risk assessment so that the cost of controls can be estimated before the project proceeds. Risk should also be considered in the specification phase where the controls are designed, but this would still be based on the assessment carried out in the feasibility study. Assessment would not be relevant in choice A or C.

NEW QUESTION 222
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 224
An information security manager uses security metrics to measure the:

A. performance of the information security progra
B. performance of the security baselin
C. effectiveness of the security risk analysi
D. effectiveness of the incident response tea

Answer: A

Explanation:

The security metrics should be designed so that there is a relationship to the performance of the overall security program in terms of effectiveness measurement. Use of security metrics occurs after the risk assessment process and does not measure it. Measurement of the incident response team performance is included in the overall program performance, so this is an incomplete answer.

NEW QUESTION 227
Which of the following is the BEST metric for evaluating the effectiveness of security awareness twining? The number of:

A. password reset

B. reported incident
C. incidents resolve
D. access rule violation

Answer: B

Explanation:

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

NEW QUESTION 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 233
Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. Daily
B. Weekly
C. Concurrently with O/S patch updates
D. During scheduled change control updates

Answer: A

Explanation:

New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.

NEW QUESTION 236
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

A. to u higher false reject rate (FRR).
B. to a lower crossover error rat
C. to a higher false acceptance rate (FAR).
D. exactly to the crossover error rat

Answer: A

Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary' to reduce sensitivity and thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts—the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

NEW QUESTION 239
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

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

Answer: A

Explanation:

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

NEW QUESTION 240
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 243
A digital signature using a public key infrastructure (PKI) will:

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

Answer: B

Explanation:

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

NEW QUESTION 246
The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

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

Answer: C

Explanation:

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

NEW QUESTION 248
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

A. Security compliant servers trend report
B. Percentage of security compliant servers
C. Number of security patches applied
D. Security patches applied trend report

Answer: A

Explanation:

The percentage of compliant servers will be a relevant indicator of the risk exposure of the infrastructure. However, the percentage is less relevant than the overall trend, which would provide a measurement of the efficiency of the IT security program. The number of patches applied would be less relevant, as this would depend on the number of vulnerabilities identified and patches provided by vendors.

NEW QUESTION 251
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

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

Answer: D

Explanation:

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

NEW QUESTION 255
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 257
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

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

Answer: C

Explanation:

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

NEW QUESTION 258
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks
B. Traffic sniffing
C. Virus infections
D. IP address spoofing

Answer: B

Explanation:

Network segmentation reduces the impact of traffic sniffing by limiting the amount of traffic that may be visible on any one network segment. Network segmentation would not mitigate the risk posed by denial of service (DoS) attacks, virus infections or IP address spoofing since each of these would be able to traverse network segments.

NEW QUESTION 261
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

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

Answer: D

Explanation:

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

NEW QUESTION 263
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

A. Strong authentication by password
B. Encrypted hard drives
C. Multifactor authentication procedures
D. Network-based data backup

Answer: B

Explanation:

Encryption of the hard disks will prevent unauthorized access to the laptop even when the laptop is lost or stolen. Strong authentication by password can be bypassed by a
determined hacker. Multifactor authentication can be bypassed by removal of the hard drive and insertion into another laptop. Network- based data backups do not prevent access but rather recovery from data loss.

NEW QUESTION 265
An e-commerce order fulfillment web server should generally be placed on which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 270
Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

Answer: A

Explanation:

Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Acquisition management controls the purchasing process.

NEW QUESTION 273
What is the BEST defense against a Structured Query Language (SQL) injection attack?

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

Answer: D

Explanation:

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

NEW QUESTION 276
The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 279
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A. Authentication
B. Encryption
C. Prohibit employees from copying data to l)SB devices
D. Limit the use of USB devices

Answer: B

Explanation:

Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

NEW QUESTION 282
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 284
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 286
Which of the following devices should be placed within a DMZ?

A. Router
B. Firewall
C. Mail relay
D. Authentication server

Answer: C

Explanation:

A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ, network segment.

NEW QUESTION 291
Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

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

Answer: C

Explanation:

The ratio of false positives to false negatives will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while, at the same time, minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

NEW QUESTION 294
Which of the following would be the BEST defense against sniffing?

A. Password protect the files
B. Implement a dynamic IP address scheme
C. Encrypt the data being transmitted
D. Set static mandatory access control (MAC) addresses

Answer: C

Explanation:

Encrypting the data will obfuscate the data so that they are not visible in plain text. Someone would have to collate the entire data stream and try decrypting it, which is not easy. Passwords can be recovered by brute-force attacks and by password crackers, so this is not the best defense against sniffing. IP addresses can always be discovered, even if dynamic IP addresses are implemented. The person sniffing traffic can initiate multiple sessions for possible IP addresses. Setting static mandatory access control (MAC) addresses can prevent address resolution protocol (ARP) poisoning, but it does not prevent sniffing.

NEW QUESTION 299
The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

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

Answer: C

Explanation:

A statistical anomaly-based intrusion detection system (stat IDS) collects data from normal traffic and establishes a baseline. It then periodically samples the network activity based on statistical methods and compares samples to the baseline. When the activity is outside the baseline parameter (clipping level), the IDS notifies the administrator. The baseline variables can include a host's memory or central processing unit (CPU) usage, network packet types and packet quantities. If actions of the users or the systems on the network vary widely with periods of low activity and periods of frantic packet exchange, a stat IDS may not be suitable, as the dramatic swing from one level to another almost certainly will generate false alarms. This weakness will have the largest impact on the operation of the IT systems. Due to the nature of stat IDS operations (i.e., they must constantly attempt to match patterns of activity to the baseline parameters), a stat IDS requires much more overhead and processing than signature-based versions. Due to the nature of a stat IDS—based on statistics and comparing data with baseline parameters—this type of IDS may not detect minor changes to system variables and may generate many false positives. Choice D is incorrect; since the stat IDS can monitor multiple system variables, it can detect new types of variables by tracing for abnormal activity of any kind.

NEW QUESTION 300
It is important to develop an information security baseline because it helps to define:

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

Answer: C

Explanation:

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

NEW QUESTION 303
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

A. Boundary router
B. Strong encryption
C. Internet-facing firewall
D. Intrusion detection system (IDS)

Answer: B

Explanation:

Strong encryption is the most effective means of protecting wireless networks. Boundary routers, intrusion detection systems (IDSs) and firewalling the Internet would not be as effective.

NEW QUESTION 308
To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A. revise the information security progra
B. evaluate a balanced business scorecar
C. conduct regular user awareness session
D. perform penetration test

Answer: B

Explanation:

The balanced business scorecard can track the effectiveness of how an organization executes it information security strategy and determine areas of improvement. Revising the information security program may be a solution, but is not the best solution to improve alignment of the information security objectives. User awareness is just one of the areas the organization must track through the balanced business scorecard. Performing penetration tests does not affect alignment with information security objectives.

NEW QUESTION 309
An intrusion detection system should be placed:

A. outside the firewal
B. on the firewall serve
C. on a screened subne
D. on the external route

Answer: C

Explanation:

An intrusion detection system (IDS) should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical dcvice.

NEW QUESTION 310
Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

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

Answer: C

Explanation:

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

NEW QUESTION 313
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 314
Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

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

Answer: B

Explanation:

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

NEW QUESTION 315
Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

A. Filter media access control (MAC) addresses
B. Use a Wi-Fi Protected Access (WPA2) protocol
C. Use a Wired Equivalent Privacy (WEP) key
D. Web-based authentication

Answer: B

Explanation:

WPA2 is currently one of the most secure authentication and encryption protocols for mainstream wireless products. MAC address filtering by itself is not a good security mechanism since allowed MAC addresses can be easily sniffed and then spoofed to get into the network. WEP is no longer a secure encryption mechanism for wireless communications. The WEP key can be easily broken within minutes using widely available software. And once the WEP key is obtained, all communications of every other wireless client are exposed. Finally, a web-based authentication mechanism can be used to prevent unauthorized user access to a network, but it will not solve the wireless network's main security issues, such as preventing network sniffing.

NEW QUESTION 316
Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

A. Intrusion detection system (IDS)
B. IP address packet filtering
C. Two-factor authentication
D. Embedded digital signature

Answer: C

Explanation:

Two-factor authentication provides an additional security mechanism over and above that provided by passwords alone. This is frequently used by mobile users needing to establish connectivity to a corporate network. IP address packet filtering would protect against spoofing an internal address but would not provide strong authentication. An intrusion detection system (IDS) can be used to detect an external attack but would not help in authenticating a user attempting to connect. Digital signatures ensure that transmitted information can be attributed to the named sender.

NEW QUESTION 318
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 319
Good information security standards should:

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

Answer: A

Explanation:

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

NEW QUESTION 321
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 323
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back

doors?

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

Answer: B

Explanation:

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

NEW QUESTION 325
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

A. the existence of messages is unknow
B. required key sizes are smalle
C. traffic cannot be sniffe
D. reliability of the data is higher in transi

Answer: A

Explanation:

The existence of messages is hidden when using steganography. This is the greatest risk.
Keys are relevant for encryption and not for steganography. Sniffing of steganographic traffic is also possible. Option D is not relevant.

NEW QUESTION 328
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop

Answer: D

Explanation:

The research and development department is usually the most sensitive area of the pharmaceutical organization, Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical: therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

NEW QUESTION 330
Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

A. the third party provides a demonstration on a test syste
B. goals and objectives are clearly define
C. the technical staff has been briefed on what to expec
D. special backups of production servers are take

Answer: B

Explanation:

The most important action is to clearly define the goals and objectives of the test. Assuming that adequate backup procedures are in place, special backups should not be necessary. Technical staff should not be briefed nor should there be a demo as this will reduce the spontaneity of the test.

NEW QUESTION 335
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 337
Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

A. polic
B. strateg
C. guideline
D. baselin

Answer: A

Explanation:

A security policy is a general statement to define management objectives with respect to security. The security strategy addresses higher level issues. Guidelines are optional actions and operational tasks. A security baseline is a set of minimum requirements that is acceptable to an organization.

NEW QUESTION 339
Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

A. Standards
B. Guidelines
C. Security metrics
D. IT governance

Answer: A

Explanation:

Standards are the bridge between high-level policy statements and the "how to" detailed formal of procedures. Security metrics and governance would not ensure correct alignment between policies and procedures. Similarly, guidelines are not linkage documents but rather provide suggested guidance on best practices.

NEW QUESTION 341
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 344
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 345
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 346
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 350
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

Answer: B

Explanation:

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

NEW QUESTION 351
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

A. Database administrator (DBA)
B. Finance department management
C. Information security manager
D. IT department management

Answer: B

Explanation:

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

NEW QUESTION 352
Which of the following documents would be the BES T reference to determine whether access control mechanisms are appropriate for a critical application?

A. User security procedures
B. Business process flow
C. IT security policy
D. Regulatory requirements

Answer: C

Explanation:

IT management should ensure that mechanisms are implemented in line with IT security policy. Procedures are determined by the policy. A user security procedure does not describe the access control mechanism in place. The business process flow is not relevant to the access control mechanism. The organization's own policy and procedures should take into account regulatory requirements.

NEW QUESTION 353
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 357
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 361
Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used
B. Provide clear directions to IT staff
C. Monitor intrusion detection system (IDS) and firewall logs closely
D. Establish clear rules of engagement

Answer: D

Explanation:

It is critical to establish a clear understanding on what is permissible during the engagement. Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used. As for monitoring the intrusion detection system (IDS) and firewall, and providing directions to IT staff, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

NEW QUESTION 362
The configuration management plan should PRIMARILY be based upon input from:

A. business process owner
B. the information security manage
C. the security steering committe
D. IT senior managemen

Answer: D

Explanation:

Although business process owners, an information security manager and the security steering committee may provide input regarding a configuration management plan, its final approval is the primary responsibility of IT senior management.

NEW QUESTION 367
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

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

Answer: B

Explanation:

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

NEW QUESTION 371
Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

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

Answer: C

Explanation:

A change control process is the methodology that ensures that anything that could be impacted by a development change will be reevaluated. Problem

management is the general process intended to manage all problems, not those specifically related to security. Background screening is the process to evaluate employee references when they are hired. BIA is the methodology used to evaluate risks in the business continuity process.

NEW QUESTION 374
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 377
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
D. Require that a change request be submitted for each download

Answer: A

Explanation:

Administrative accounts have permission to change data. This is not required for the developers to perform their tasks. Unauthorized change will damage the integrity of the data. Logging all usage of the account, suspending the account and activating only when needed, and requiring that a change request be submitted for each download will not reduce the exposure created by this excessive level of access. Restricting the account to read only access will ensure that the integrity can be maintained while permitting access.

NEW QUESTION 378
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

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

Answer: D

Explanation:

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

NEW QUESTION 379
When security policies are strictly enforced, the initial impact is that:

A. they may have to be modified more frequentl
B. they will be less subject to challeng
C. the total cost of security is increase
D. the need for compliance reviews is decrease

Answer: C

Explanation:

When security policies are strictly enforced, more resources are initially required, thereby increasing, the total cost of security. There would be less need for frequent modification. Challenges would be rare and the need for compliance reviews would not necessarily be less.

NEW QUESTION 383
Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

A. Information security officer
B. Security steering committee
C. Data owner
D. Data custodian

Answer:

B

Explanation:

Routine administration of all aspects of security is delegated, but senior management must retain overall responsibility. The information security officer supports and implements information security for senior management. The data owner is responsible for categorizing data security requirements. The data custodian supports and implements information security as directed.

NEW QUESTION 386
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 391
Data owners are normally responsible for which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 393
Nonrepudiation can BEST be assured by using:

A. delivery path tracin
B. reverse lookup translatio
C. out-of-hand channel
D. digital signature

Answer: D

Explanation:

Effective nonrepudiation requires the use of digital signatures. Reverse lookup translation involves converting Internet Protocol (IP) addresses to usernames. Delivery path tracing shows the route taken but does not confirm the identity of the sender. Out-of-band channels are useful when, for confidentiality, it is necessary to break a message into two parts that are sent by different means.

NEW QUESTION 395
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 397
A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

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

D. Analyze the logs to detect unauthorized access

Answer: A

Explanation:

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual.
Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but. because it is detective, it would not be the most effective in this instance.

NEW QUESTION 399
There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

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

Answer: C

Explanation:

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

NEW QUESTION 401
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 403
The PRIMARY reason for using metrics to evaluate information security is to:

A. identify security weaknesse
B. justify budgetary expenditure
C. enable steady improvemen
D. raise awareness on security issue

Answer: C

Explanation:

The purpose of a metric is to facilitate and track continuous improvement. It will not permit the identification of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

NEW QUESTION 404
The BEST way to ensure that information security policies are followed is to:

A. distribute printed copies to all employee
B. perform periodic reviews for complianc
C. include escalating penalties for noncomplianc
D. establish an anonymous hotline to report policy abuse

Answer: B

Explanation:

The best way to ensure that information security policies are followed is to periodically review levels of compliance. Distributing printed copies, advertising an abuse hotline or linking policies to an international standard will not motivate individuals as much as the consequences of being found in noncompliance. Escalating penalties will first require a compliance review.

NEW QUESTION 409
A security awareness program should:

A. present top management's perspectiv
B. address details on specific exploit
C. address specific groups and role
D. promote security department procedure

Answer: C

Explanation:

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

NEW QUESTION 411
Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs?

A. Penetration attempts investigated
B. Violation log reports produced
C. Violation log entries
D. Frequency of corrective actions taken

Answer: A

Explanation:
The most useful metric is one that measures the degree to which complete follow-through has taken place. The quantity of reports, entries on reports and the frequency of corrective actions are not indicative of whether or not investigative action was taken.

NEW QUESTION 416
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 417
Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

A. Signal strength
B. Number of administrators
C. Bandwidth
D. Encryption strength

Answer: B

Explanation:

The number of individuals with access to the network configuration presents a security risk. Encryption strength is an area where wireless networks tend to fall short; however, the potential to compromise the entire network is higher when an inappropriate number of people can alter the configuration. Signal strength and network bandwidth are secondary issues.

NEW QUESTION 422
The BEST time to perform a penetration test is after:

A. an attempted penetration has occurre
B. an audit has reported weaknesses in security control
C. various infrastructure changes are mad
D. a high turnover in systems staf

Answer: C

Explanation:

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

NEW QUESTION 426
An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

A. source routin
B. broadcast propagatio
C. unregistered port
D. nonstandard protocol

Answer: A

Explanation:

If the firewall allows source routing, any outsider can carry out spoofing attacks by stealing the internal (private) IP addresses of the organization. Broadcast propagation, unregistered ports and nonstandard protocols do not create a significant security exposure.

NEW QUESTION 427
Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

A. assess the problems and institute rollback procedures, if neede
B. disconnect the systems from the network until the problems are correcte
C. immediately uninstall the patches from these system
D. immediately contact the vendor regarding the problems that occurre

Answer: A

Explanation:

Assessing the problems and instituting rollback procedures as needed would be the best course of action. Choices B and C would not identify where the problem was, and may in fact make the problem worse. Choice D is part of the assessment.

NEW QUESTION 428
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 429
What is the PRIMARY objective of a post-event review in incident response?

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

Answer: C

Explanation:

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

NEW QUESTION 431
In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

A. volume of sensitive dat
B. recovery point objective (RPO).
C. recovery' time objective (RTO).
D. interruption windo

Answer: B

Explanation:

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

NEW QUESTION 436
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 437
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISM Exam with Our Prep Materials Via below:

https://www.certleader.com/CISM-dumps.html