Isaca

Exam Questions CISM

Certified Information Security Manager

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

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

Answer: B

Explanation:

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

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

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

Answer: C

Explanation:

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 4
Which of the following is MOST 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 5
From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

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

Answer: D

Explanation:

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 7
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 8
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 9
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
Which of the following MOST commonly falls within the scope of an information security governance steering committee?

A. Interviewing candidates for information security specialist positions
B. Developing content for security awareness programs
C. Prioritizing information security initiatives

D. Approving access to critical financial systems

Answer: C

Explanation:

Prioritizing information security initiatives is the only appropriate item. The interviewing of specialists should be performed by the information security manager, while the developing of program content should be performed by the information security staff. Approving access to critical financial systems is the responsibility of individual system data owners.

NEW QUESTION 10
An organization's information security strategy should be based on:

A. managing risk relative to business objective
B. managing risk to a zero level and minimizing insurance premium
C. avoiding occurrence of risks so that insurance is not require
D. transferring most risks to insurers and saving on control cost

Answer: A

Explanation:

Organizations must manage risks to a level that is acceptable for their business model, goals and objectives. A zero-level approach may be costly and not provide the effective benefit of additional revenue to the organization. Long-term maintenance of this approach may not be cost effective. Risks vary as business models, geography, and regulatory- and operational processes change. Insurance covers only a small portion of risks and requires that the organization have certain operational controls in place.

NEW QUESTION 12
A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

A. meet with stakeholders to decide how to compl
B. analyze key risks in the compliance proces
C. assess whether existing controls meet the regulatio
D. update the existing security/privacy polic

Answer: C

Explanation:

If the organization is in compliance through existing controls, the need to perform other work related to the regulation is not a priority. The other choices are appropriate and important; however, they are actions that are subsequent and will depend on whether there is an existing control gap.

NEW QUESTION 15
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
When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

A. aligned with the IT strategic pla
B. based on the current rate of technological chang
C. three-to-five years for both hardware and softwar
D. aligned with the business strateg

Answer: D

Explanation:

Any planning for information security should be properly aligned with the needs of the business. Technology should not come before the needs of the business, nor should planning be done on an artificial timetable that ignores business needs.

NEW QUESTION 21
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 24
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 25
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 29
The MOST complete business case for security solutions is one that.

A. includes appropriate justificatio
B. explains the current risk profil
C. details regulatory requirement
D. identifies incidents and losse

Answer: A

Explanation:

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

NEW QUESTION 34
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

A. Risk assessment report
B. Technical evaluation report
C. Business case
D. Budgetary requirements

Answer: C

Explanation:

The information security manager needs to prioritize the controls based on risk management and the requirements of the organization. The information security manager must look at the costs of the various controls and compare them against the benefit the organization will receive from the security solution. The information security manager needs to have knowledge of the development of business cases to illustrate the costs and benefits of the various controls. All other choices are supplemental.

NEW QUESTION 37
Which of the following would help to change an organization's security culture?

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

Answer: B

Explanation:

Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

NEW QUESTION 41
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 46
Which of the following is a benefit of information security governance?

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

Answer: A

Explanation:

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

NEW QUESTION 50
Which of the following is the MOST important information to include in an information security standard?

A. Creation date
B. Author name
C. Initial draft approval date
D. Last review date

Answer: D

Explanation:

The last review date confirms the currency of the standard, affirming that management has reviewed the standard to assure that nothing in the environment has changed that would necessitate an update to the standard. The name of the author as well as the creation and draft dates are not that important.

NEW QUESTION 55
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 57
Security technologies should be selected PRIMARILY on the basis of their:

A. ability to mitigate business risk
B. evaluations in trade publication
C. use of new and emerging technologie
D. benefits in comparison to their cost

Answer: A

Explanation:

The most fundamental evaluation criterion for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

NEW QUESTION 59
Which of the following is the MOST important element of an information security strategy?

A. Defined objectives
B. Time frames for delivery
C. Adoption of a control framework
D. Complete policies

Answer: A

Explanation:

Without defined objectives, a strategy—the plan to achieve objectives—cannot be developed. Time frames for delivery are important but not critical for inclusion in the strategy document. Similarly, the adoption of a control framework is not critical to having a successful information security strategy. Policies are developed subsequent to, and as a part of, implementing a strategy.

NEW QUESTION 64
Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

Answer: B

Explanation:

Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economics of scale. However, turnaround can be slower due to the lack of alignment with business units.

NEW QUESTION 66
A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BES T approach of the information security manager?

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

Answer: C

Explanation:

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

NEW QUESTION 68
Senior management commitment and support for information security can BEST be obtained through presentations that:

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

Answer: D

Explanation:

Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business

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

NEW QUESTION 69
Effective IT governance is BEST ensured by:

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

Answer: D

Explanation:

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

NEW QUESTION 74
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

A. review the functionalities and implementation requirements of the solutio
B. review comparison reports of tool implementation in peer companie
C. provide examples of situations where such a tool would be usefu
D. substantiate the investment in meeting organizational need

Answer: D

Explanation:

Any investment must be reviewed to determine whether it is cost effective and supports the organizational strategy. It is important to review the features and functionalities provided by such a tool, and to provide examples of situations where the tool would be useful, but that comes after substantiating the investment and return on investment to the organization.

NEW QUESTION 76
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

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

Answer: A

Explanation:

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

NEW QUESTION 78
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 80
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

A. establishing a periodic risk assessmen
B. promoting regulatory requirement

C. developing a business cas
D. developing effective metric

Answer: C

Explanation:

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

NEW QUESTION 85
Who is ultimately responsible for the organization's information?

A. Data custodian
B. Chief information security officer (CISO)
C. Board of directors
D. Chief information officer (CIO)

Answer: C

Explanation:

The board of directors is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. The data custodian is responsible for the maintenance and protection of data. This role is usually filled by the IT department. The chief information security officer (CISO) is responsible for security and carrying out senior management's directives. The chief information officer (CIO) is responsible for information technology within the organization and is not ultimately responsible for the organization's information.

NEW QUESTION 89
In order to highlight to management the importance of network security, the security manager should FIRST:

A. develop a security architectur
B. install a network intrusion detection system (NIDS) and prepare a list of attack
C. develop a network security polic
D. conduct a risk assessmen

Answer: D

Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

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 99
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

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

Answer: C

Explanation:

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

NEW QUESTION 104
Which of the following is MOST important in developing a security strategy?

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

Answer: B

Explanation:

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

NEW QUESTION 109
An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

A. Direct information security on what they need to do
B. Research solutions to determine the proper solutions
C. Require management to report on compliance
D. Nothing; information security does not report to the board

Answer: C

Explanation:

Information security governance is the responsibility of the board of directors and executive management. In this instance, the appropriate action is to ensure that a plan is in place for implementation of needed safeguards and to require updates on that implementation.

NEW QUESTION 112
In implementing information security governance, the information security manager is PRIMARILY responsible for:

A. developing the security strateg
B. reviewing the security strateg
C. communicating the security strateg
D. approving the security strategy

Answer: A

Explanation:

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

NEW QUESTION 115
What is the MOST important factor in the successful implementation of an enterprise wide information security program?

A. Realistic budget estimates
B. Security awareness
C. Support of senior management
D. Recalculation of the work factor

Answer: C

Explanation:

Without the support of senior management, an information security program has little chance of survival. A company's leadership group, more than any other group, will more successfully drive the program. Their authoritative position in the company is a key factor. Budget approval, resource commitments, and companywide participation also require the buy-in from senior management. Senior management is responsible for providing an adequate budget and the necessary resources. Security awareness is important, but not the most important factor. Recalculation of the work factor is a part of risk management.

NEW QUESTION 117
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

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

Answer: A

Explanation:

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

NEW QUESTION 119
Which of the following is the BEST justification to convince management to invest in an information security program?

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

Answer: D

Explanation:

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

NEW QUESTION 121
Which of the following should be the FIRST step in developing an information security plan?

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

Answer: B

Explanation:

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

NEW QUESTION 125
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 127
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 131
Which of the following should be included in an annual information security budget that is submitted for management approval?

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

Answer: A

Explanation:

A brief explanation of the benefit of expenditures in the budget helps to convey the context of how the purchases that are being requested meet goals and

objectives, which in turn helps build credibility for the information security function or program. Explanations of benefits also help engage senior management in the support of the information security program. While the budget should consider all inputs and recommendations that are received from the business, the budget that is ultimately submitted to management for approval should include only those elements that are intended for purchase. TC'O may be requested by management and may be provided in an addendum to a given purchase request, but is not usually included in an annual budget. Baseline comparisons (cost comparisons with other companies or industries) may be useful in developing a budget or providing justification in an internal review for an individual purchase, but would not be included with a request for budget approval.

NEW QUESTION 132
The data access requirements for an application should be determined by the:

A. legal departmen
B. compliance office
C. information security manage
D. business owne

Answer: D

Explanation:

Business owners are ultimately responsible for their applications. The legal department, compliance officer and information security manager all can advise, but do not have final responsibility.

NEW QUESTION 133
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 135
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 138
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 139
When developing an information security program, what is the MOST useful source of information for determining available resources?

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

Answer: D

Explanation:

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

NEW QUESTION 141
Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

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

Answer: A

Explanation:

The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

NEW QUESTION 143
Which of the following characteristics is MOST important when looking at prospective candidates for the role of chief information security officer (CISO)?

A. Knowledge of information technology platforms, networks and development methodologies
B. Ability to understand and map organizational needs to security technologies
C. Knowledge of the regulatory environment and project management techniques
D. Ability to manage a diverse group of individuals and resources across an organization

Answer: B

Explanation:

Information security will be properly aligned with the goals of the business only with the ability to understand and map organizational needs to enable security technologies. All of the other choices are important but secondary to meeting business security needs.

NEW QUESTION 147
Senior management commitment and support for information security can BEST be enhanced through:

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

Answer: C

Explanation:

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

NEW QUESTION 149
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 153
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 155
Information security projects should be prioritized on the basis of:

A. time required for implementatio
B. impact on the organizatio
C. total cost for implementatio
D. mix of resources require

Answer: BExplanation:

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

NEW QUESTION 160
An information security manager must understand the relationship between information security and business operations in order to:

A. support organizational objective
B. determine likely areas of noncomplianc
C. assess the possible impacts of compromis
D. understand the threats to the busines

Answer: A

Explanation:

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

NEW QUESTION 165
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks
C. Demonstrate that IT mitigating controls are in place
D. Suggest new IT controls to mitigate operational risk

Answer: B

Explanation:

The job of the information security officer on such a team is to assess the risks to the business operation. Choice A is incorrect because information security is not limited to IT issues. Choice C is incorrect because at the time a team is formed to assess risk, it is premature to assume that any demonstration of IT controls will mitigate business operations risk. Choice D is incorrect because it is premature at the time of the formation of the team to assume that any suggestion of new IT controls will mitigate business operational risk.

NEW QUESTION 169
The cost of implementing a security control should not exceed the:

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

Answer: C

Explanation:

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

NEW QUESTION 172
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

A. prepare a security budge
B. conduct a risk assessmen
C. develop an information security polic
D. obtain benchmarking informatio

Answer: B

Explanation:

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

NEW QUESTION 177
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

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

Answer: B

Explanation:

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

NEW QUESTION 180
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism
C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

Answer: B

Explanation:

A challenge .response mechanism prevents replay attacks by sending a different random challenge in each authentication event. The response is linked to that challenge. Therefore, capturing the authentication handshake and replaying it through the network will not work. Using hashes by itself will not prevent a replay. A WEP key will not prevent sniffing (it just takes a few more minutes to break the WEP key if the attacker does not already have it) and therefore will not be able to prevent recording and replaying an authentication handshake. HTTP Basic Authentication is clear text and has no mechanisms to prevent replay.

NEW QUESTION 183
Acceptable risk is achieved when:

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

Answer: A

Explanation:

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

NEW QUESTION 186
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

A. map the major threats to business objective
B. review available sources of risk informatio
C. identify the value of the critical asset
D. determine the financial impact if threats materializ

Answer: A

Explanation:

Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available

sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

NEW QUESTION 191
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 196
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 198
The BEST strategy for risk management is to:

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

Answer: B

Explanation:

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

NEW QUESTION 200
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

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

Answer: A

Explanation:

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

NEW QUESTION 201
When performing an information risk analysis, an information security manager should FIRST:

A. establish the ownership of asset
B. evaluate the risks to the asset
C. take an asset inventor
D. categorize the asset

Answer:

C

Explanation:

Assets must be inventoried before any of the other choices can be performed.

NEW QUESTION 203
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

A. Tree diagrams
B. Venn diagrams
C. Heat charts
D. Bar charts

Answer: C

Explanation:

Meat charts, sometimes referred to as stoplight charts, quickly and clearly show the current status of remediation efforts. Venn diagrams show the connection between sets; tree diagrams are useful for decision analysis; and bar charts show relative size.

NEW QUESTION 204
Previously accepted risk should be:

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

Answer: A

Explanation:

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

NEW QUESTION 208
Phishing is BEST mitigated by which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 211
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 212
A successful risk management program should lead to:

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

Answer: A

Explanation:

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

NEW QUESTION 215
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

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

Answer: A

Explanation:

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

NEW QUESTION 217
Which of the following BEST describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

Answer: B

Explanation:

Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

NEW QUESTION 221
In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

A. original cost to acquir
B. cost of the software store
C. annualized loss expectancy (ALE).
D. cost to obtain a replacemen

Answer: D

Explanation:

The value of the server should be based on its cost of replacement. The original cost may be significantly different from the current cost and, therefore, not as relevant. The value of the software is not at issue because it can be restored from backup media. The ALE for all risks related to the server does not represent the server's value.

NEW QUESTION 225
The recovery point objective (RPO) requires which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 229
An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

A. perform a comprehensive assessment of the organization's exposure to the hacker's technique
B. initiate awareness training to counter social engineerin
C. immediately advise senior management of the elevated ris

D. increase monitoring activities to provide early detection of intrusio

Answer: C

Explanation:

Information about possible significant new risks from credible sources should be provided to management along with advice on steps that need to be taken to counter the threat. The security manager should assess the risk, but senior management should be immediately advised. It may be prudent to initiate an awareness campaign subsequent to sounding the alarm if awareness training is not current. Monitoring activities should also be increased.

NEW QUESTION 231
Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

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

Answer: B

Explanation:

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

NEW QUESTION 236
A common concern with poorly written web applications is that they can allow an attacker to:

A. gain control through a buffer overflo
B. conduct a distributed denial of service (DoS) attac
C. abuse a race conditio
D. inject structured query language (SQL) statement

Answer: D

Explanation:

Structured query language (SQL) injection is one of the most common and dangerous web application vulnerabilities. Buffer overflows and race conditions are very difficult to find and exploit on web applications. Distributed denial of service (DoS) attacks have nothing to do with the quality of a web application.

NEW QUESTION 240
The recovery time objective (RTO) is reached at which of the following milestones?

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

Answer: C

Explanation:

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

NEW QUESTION 241
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 246
The MOST important reason for conducting periodic risk assessments is because:

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

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

Answer: B

Explanation:

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

NEW QUESTION 248
Which of the following is the MOST usable deliverable of an information security risk analysis?

A. Business impact analysis (BIA) report
B. List of action items to mitigate risk
C. Assignment of risks to process owners
D. Quantification of organizational risk

Answer: B

Explanation:

Although all of these are important, the list of action items is used to reduce or transfer the current level of risk. The other options materially contribute to the way the actions are implemented.

NEW QUESTION 249
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

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

Answer: B

Explanation:

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

NEW QUESTION 253
Which of the following would generally have the GREATEST negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services
C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

Answer: C

Explanation:

Although the theft of software, interruption of utility services and internal frauds are all significant, the loss of customer confidence is the most damaging and could cause the business to fail.

NEW QUESTION 257
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 260
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

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

Answer: A

Explanation:

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

NEW QUESTION 263
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 267
Which of the following attacks is BEST mitigated by utilizing strong passwords?

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

Answer: B

Explanation:

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

NEW QUESTION 271
The valuation of IT assets should be performed by:

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

Answer: D

Explanation:

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

NEW QUESTION 272
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

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

Answer: C

Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The

other choices, although relevant, would not be as important.

NEW QUESTION 277
For risk management purposes, the value of an asset should be based on:

A. original cos
B. net cash flo
C. net present valu
D. replacement cos

Answer: D

Explanation:

The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

NEW QUESTION 281
The MOST effective way to incorporate risk management practices into existing production systems is through:

A. policy developmen
B. change managemen
C. awareness trainin
D. regular monitorin

Answer: B

Explanation:

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

NEW QUESTION 284
Which of the following steps should be performed FIRST in the risk assessment process?

A. Staff interviews
B. Threat identification
C. Asset identification and valuation
D. Determination of the likelihood of identified risks

Answer: C

Explanation:

The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk. Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

NEW QUESTION 289
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

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

Answer: B

Explanation:

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

NEW QUESTION 294
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

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

Answer: C

Explanation:

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

NEW QUESTION 297
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

A. increase its customer awareness efforts in those region
B. implement monitoring techniques to detect and react to potential frau
C. outsource credit card processing to a third part
D. make the customer liable for losses if they fail to follow the bank's advic

Answer: B

Explanation:

While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk. Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

NEW QUESTION 298
When a significant security breach occurs, what should be reported FIRST to senior management?

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

Answer: B

Explanation:

When reporting an incident to senior management, the initial information to be communicated should include an explanation of what happened and how the breach was resolved. A summary of security logs would be too technical to report to senior management. An analysis of the impact of similar attacks and a business case for improving controls would be desirable; however, these would be communicated later in the process.

NEW QUESTION 300
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 304
Information security managers should use risk assessment techniques to:

A. justify selection of risk mitigation strategie
B. maximize the return on investment (RO
C. provide documentation for auditors and regulator
D. quantify risks that would otherwise be subjectiv

Answer: A

Explanation:

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

NEW QUESTION 307
When residual risk is minimized:

A. acceptable risk is probabl
B. transferred risk is acceptabl
C. control risk is reduce

D. risk is transferabl

Answer: A

Explanation:

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

NEW QUESTION 309
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

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

Answer: A

Explanation:

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

NEW QUESTION 313
Which of the following is the MOST appropriate use of gap analysis?

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

Answer: D

Explanation:

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

NEW QUESTION 314
The decision on whether new risks should fall under periodic or event-driven reporting
should be based on which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 318
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

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

Answer: C

Explanation:

Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Violation logs are detective and do not prevent unauthorized access. Baseline security standards do not prevent unauthorized access. Exit routines are dependent upon appropriate role-based access.

NEW QUESTION 322
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 327
Who can BEST advocate the development of and ensure the success of an information security program?

A. Internal auditor
B. Chief operating officer (COO)
C. Steering committee
D. IT management

Answer: C

Explanation:

Senior management represented in the security steering committee is in the best position to advocate the establishment of and continued support for an information security program. The chief operating officer (COO) will be a member of that committee. An internal auditor is a good advocate but is secondary to the influence of senior management. IT management has a lesser degree of influence and would also be part of the steering committee.

NEW QUESTION 328
For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method
to ensure that logging onto the network is secure?

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

Answer: D

Explanation:

Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

NEW QUESTION 329
When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSI.), confidentiality is MOST vulnerable to which of the following?

A. IP spoofing
B. Man-in-the-middle attack
C. Repudiation
D. Trojan

Answer: D

Explanation:

A Trojan is a program that gives the attacker full control over the infected computer, thus allowing the attacker to hijack, copy or alter information after authentication by the user. IP spoofing will not work because IP is not used as an authentication mechanism. Man-in-the-middle attacks are not possible if using SSL with client-side certificates. Repudiation is unlikely because client-side certificates authenticate the user.

NEW QUESTION 330
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 331
Which of the following is the MOST important risk associated with middleware in a client-server environment?

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

Answer: C

Explanation:

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

NEW QUESTION 335
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. corporate internal audito
B. System developers/analyst
C. key business process owner
D. corporate legal counse

Answer: C

Explanation:

Business process owners are in the best position to understand how new regulatory requirements may affect their systems. Legal counsel and infrastructure management, as well as internal auditors, would not be in as good a position to fully understand all ramifications.

NEW QUESTION 338
What is the MOST important item to be included in an information security policy?

A. The definition of roles and responsibilities
B. The scope of the security program
C. The key objectives of the security program
D. Reference to procedures and standards of the security program

Answer: C

Explanation:

Stating the objectives of the security program is the most important element to ensure alignment with business goals. The other choices are part of the security policy, but they are not as important.

NEW QUESTION 340
Which of the following is MOST important to the success of an information security program?

A. Security' awareness training
B. Achievable goals and objectives
C. Senior management sponsorship
D. Adequate start-up budget and staffing

Answer: C

Explanation:

Sufficient senior management support is the most important factor for the success of an information security program. Security awareness training, although important, is secondary. Achievable goals and objectives as well as having adequate budgeting and staffing are important factors, but they will not ensure success if senior management support is not present.

NEW QUESTION 341
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 346
A border router should be placed on which of the following?

A. Web server
B. IDS server
C. Screened subnet
D. Domain boundary

Answer: D

Explanation:

A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

NEW QUESTION 347
The MAIN advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workloa
B. increases security between multi-tier system
C. allows passwords to be changed less frequentl
D. reduces the need for two-factor authenticatio

Answer: A

Explanation:

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

NEW QUESTION 350
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 352
At what stage of the applications development process would encryption key management initially be addressed?

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

Answer: A

Explanation:

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

NEW QUESTION 357
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 359
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

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

Answer: C

Explanation:

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

NEW QUESTION 362
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

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

Answer: D

Explanation:

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

NEW QUESTION 364
The effectiveness of virus detection software is MOST dependent on which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 365
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

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

Answer: A

Explanation:

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

NEW QUESTION 367
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

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

Answer: B

Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and. second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

NEW QUESTION 372
When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

A. Centralizing security management
B. Implementing sanctions for noncompliance
C. Policy enforcement by IT management
D. Periodic compliance reviews

Answer: A

Explanation:

By centralizing security management, the organization can ensure that security standards are applied to all systems equally and in line with established policy. Sanctions for noncompliance would not be the best way to correct poor management practices caused by work overloads or insufficient knowledge of security practices. Enforcement of policies is not solely the responsibility of IT management. Periodic compliance reviews would not correct the problems, by themselves, although reports to management would trigger corrective action such as centralizing security management.

NEW QUESTION 377
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 I)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 379
Which of the following is a key area of the ISO 27001 framework?

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

Answer: D

Explanation:

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

NEW QUESTION 382
An extranet server 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 extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

NEW QUESTION 386
Which of the following is the MOST effective type of access control?

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

Answer: B

Explanation:

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

NEW QUESTION 391
Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

A. Regular review of access control lists
B. Security guard escort of visitors
C. Visitor registry log at the door
D. A biometric coupled with a PIN

Answer: A

Explanation:

A review of access control lists is a detective control that will enable an information security manager to ensure that authorized persons are entering in compliance with corporate policy. Visitors accompanied by a guard will also provide assurance but may not be cost effective. A visitor registry is the next cost-effective control. A biometric coupled with a PIN will strengthen the access control; however, compliance assurance logs will still have to be reviewed.

NEW QUESTION 392
The MOST important success factor to design an effective IT security awareness program is to:

A. customize the content to the target audienc
B. ensure senior management is represente
C. ensure that all the staff is traine
D. avoid technical content but give concrete example

Answer: A

Explanation:

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

NEW QUESTION 394
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 397
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 402
What is the MOST important reason for conducting security awareness programs throughout an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 407
In an organization, information systems security is the responsibility of:

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

Answer: A

Explanation:

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

NEW QUESTION 412
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

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

Answer: B

Explanation:

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

NEW QUESTION 413
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 414
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 417
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

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

Answer: A

Explanation:

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

NEW QUESTION 421
When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

A. right-to-terminate claus
B. limitations of liabilit
C. service level agreement (SLA).
D. financial penalties claus

Answer: C

Explanation:

Service level agreements (SLAs) provide metrics to which outsourcing firms can be held accountable. This is more important than a limitation on the outsourcing firm's liability, a right-to-terminate clause or a hold- harmless agreement which involves liabilities to third parties.

NEW QUESTION 423
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. ensure the confidentiality of sensitive materia
B. provide a high assurance of identit
C. allow deployment of the active director
D. implement secure sockets layer (SSL) encryptio

Answer: B

Explanation:

The primary purpose of a public key infrastructure (PKI) is to provide strong authentication. Confidentiality is a function of the session keys distributed by the PKI. An active directory can use PKI for authentication as well as using other means. Even though secure sockets layer (SSL) encryption requires keys to authenticate, it is not the main reason for deploying PKI.

NEW QUESTION 424
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

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

Answer: B

Explanation:

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

NEW QUESTION 425
In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

A. a strong authenticatio
B. IP antispoofing filterin
C. network encryption protoco
D. access lists of trusted device

Answer: A

Explanation:

Strong authentication will provide adequate assurance on the identity of the users, while IP antispoofing is aimed at the device rather than the user. Encryption protocol ensures data confidentiality and authenticity while access lists of trusted devices are easily exploited by spoofed identity of the clients.

NEW QUESTION 426
Security awareness training is MOST likely to lead to which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 428
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 430
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. messages displayed at every logo
B. periodic security-related e-mail message
C. an Intranet web site for information securit
D. circulating the information security polic

Answer: A

Explanation:

Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet web site does not force users to access it and read the information. Circulating the information security policy atone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

NEW QUESTION 432
Which of the following devices should be placed within a DMZ?

A. Proxy server
B. Application server
C. Departmental server
D. Data warehouse server

Answer: B

Explanation:

An application server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Data warehouse and departmental servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. A proxy server forms the

inner boundary of the DMZ but is not placed within it.

NEW QUESTION 437
An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RI P) is the:

A. references from other organization
B. past experience of the engagement tea
C. sample deliverabl
D. methodology used in the assessmen

Answer: D

Explanation:

Methodology illustrates the process and formulates the basis to align expectations and the execution of the assessment. This also provides a picture of what is required of all parties involved in the assessment. References from other organizations are important, but not as important as the methodology used in the assessment. Past experience of the engagement team is not as important as the methodology used. Sample deliverables only tell how the assessment is presented, not the process.

NEW QUESTION 439
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

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

Answer: A

Explanation:

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

NEW QUESTION 444
What is the BEST way to ensure that contract programmers comply with organizational security policies?

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

Answer: D

Explanation:

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

NEW QUESTION 447
The MOST important reason for formally documenting security procedures is to ensure:

A. processes are repeatable and sustainabl
B. alignment with business objective
C. auditability by regulatory agencie
D. objective criteria for the application of metric

Answer: A

Explanation:

Without formal documentation, it would be difficult to ensure that security processes are performed in the proper manner every time that they are performed. Alignment with business objectives is not a function of formally documenting security procedures. Processes should not be formally documented merely to satisfy an audit requirement. Although potentially useful in the development of metrics, creating formal documentation to assist in the creation of metrics is a secondary objective.

NEW QUESTION 449
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISM Practice Exam Features:

* CISM Questions and Answers Updated Frequently

* CISM Practice Questions Verified by Expert Senior Certified Staff

* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year