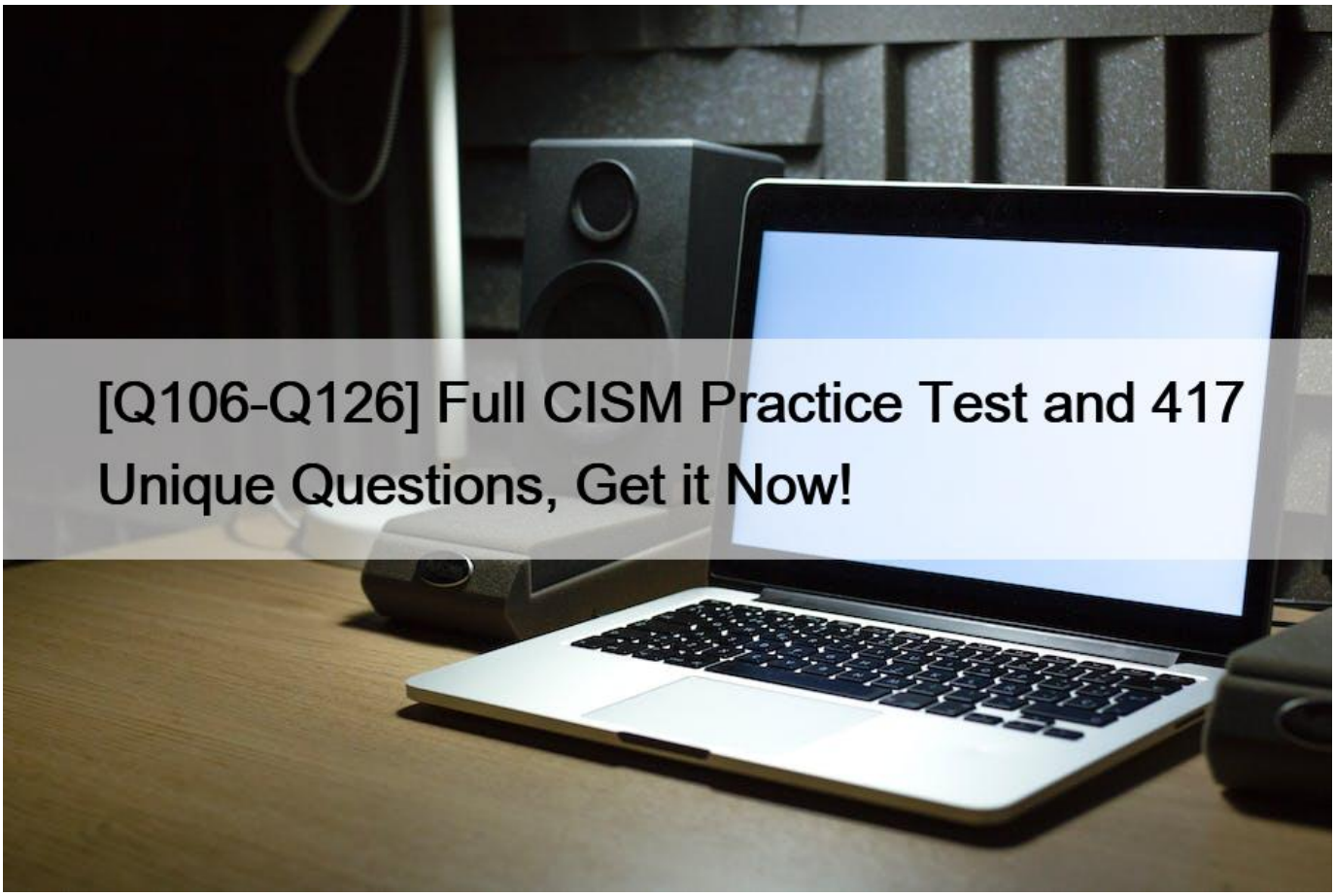
[Q106-Q126 Full CISM Practice Test and 417 Unique Questions, Get it Now!



Full CISM Practice Test and 417 Unique Questions, Get it Now!
The Best CISM Exam Study Material Premium Files and Preparation Tool

The CISM certification is recognized by many organizations and is highly valued in the information security industry. According to ISACA, CISM certification holders earn an average of 27% higher salaries than their non-certified counterparts. Certified Information Security Manager certification is also recognized by the US Department of Defense (DoD) as a prerequisite for certain job roles. Overall, the CISM certification is an excellent way for IT professionals to advance their careers in the field of information security management and increase their value to their organizations.

NO.106 Phishing is BEST mitigated by which of the following?
* Security monitoring software
* Encryption
* Two-factor authentication
* User awareness

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.

NO.107 Which of the following situations would MOST inhibit the effective implementation of security governance:
* The complexity of technology
* Budgetary constraints
* Conflicting business priorities
* High-level sponsorship

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.

NO.108 Which of the following would a security manager establish to determine the target for restoration of normal processing?
* Recover)’ time objective (RTO)
* Maximum tolerable outage (MTO)
* Recovery point objectives (RPOs)
* Services delivery objectives (SDOs)

Explanation/Reference:

Explanation:

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

NO.109 The MAIN goal of an information security strategic plan is to:
* develop a risk assessment plan.
* develop a data protection plan.
* protect information assets and resources.
* establish security governance.

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT

Explanation:

The main goal of an information security strategic plan is to protect information assets and resources.

Developing a risk assessment plan and H data protection plan, and establishing security governance refer to tools utilized in the security strategic plan that achieve the protection of information assets and resources.

NO.110 An online bank identifies a successful network attack in progress. The bank should FIRST:
* isolate the affected network segment.
* report the root cause to the board of directors.
* assess whether personally identifiable information (Pll) is compromised.
* shut down the entire network.

NO.111 An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

* A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
* Firewall policies are updated on the basis of changing requirements.
* inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
* The firewall is placed on top of the commercial operating system with all installation options.

Explanation

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners’ roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

NO.112 Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization’s information security requirements?

* The ability to audit the third-party supplier’s IT systems and processes
* An independent review report indicating compliance with industry standards
* Third-party security control self-assessment results
* Alive demonstration of the third-party supplier’s security capabilities

NO.113 Which of the following is a PRIMARY responsibility of an information security governance committee?

* Analyzing information security policy compliance reviews
* Approving the purchase of information security technologies
* Reviewing the information security strategy
* Approving the information security awareness training strategy

Section: INFORMATION SECURITY GOVERNANCE

NO.114 An information security manager is developing a new information security strategy. Which of the following functions would serve as the BEST resource to review the strategy and provide guidance for business alignment?

* The board of directors
* Internal audit
* The steering committee
* The legal department

NO.115 which of the following would BEST help an information security manager justify the implementation ofa security information and event management (SIEM) system?

* Results of a risk assessment
* Results of a cost-benefit analysis
* Security benchmarks
* Results of a business impact analysis (BIA)

NO.116 A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

* change the password policy to improve the customer experience
* research alternative secure methods of identity verification
* evaluate the impact of the customer’s experience on business revenue
* recommend implementing two-factor authentication

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

NO.117 Which of the following is MOST critical to review when preparing to outsource a data repository to a cloud-based solution?
* Disaster recovery plan
* Identity and access management
* Vendor s information security policy
* A risk assessment

NO.118 Planning for the implementation of an information security program is MOST effective when it:
* uses decision trees to prioritize security projects
* applies gap analysis to current and future business plans
* uses risk-based analysis for security projects
* applies technology-driven solutions to identified needs

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT

NO.119 In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?
* Applying patches
* Changing access rules
* Upgrading hardware
* Backing up files

Explanation/Reference:

Explanation:

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

NO.120 A recent audit has identified that security controls by the organization’s policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?
* Discuss the issue with the data owners to determine the reason for the exception
* Discuss the issue with data custodians to determine the reason for the exception
* Report the issue to senior management and request funding to fix the issue
* Deny access to the application until the issue is resolved

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

Explanation

NO.121 When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?
* Ensuring accessibility should a disaster occur
* Versioning control as plans are modified
* Broken hyperlinks to resources stored elsewhere
* Tracking changes in personnel and plan assets

Explanation

If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

NO.122 Which of the following results from the risk assessment process would BEST assist risk management decision making?

* Control risk
* Inherent risk
* Risk exposure
* Residual risk

Explanation

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

NO.123 Which of the following should be in place before a black box penetration test begins?
* IT management approval
* Proper communication and awareness training
* A clearly stated definition of scope
* An incident response plan

Explanation/Reference:

Explanation:

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

NO.124 A risk was identified during a risk assessment. The business process owner has chosen to accept the risk because the cost of remediation is greater than the projected cost of a worst-case scenario. What should be the information security manager’s NEXT course of action?
* Document and schedule a date to revisit the issue.
* Document and escalate to senior management.
* Shut down the business application.
* Determine a lower-cost approach to remediation.

NO.125 When developing security processes for handling credit card data on the business unit’s information system, the information security manager should
* review corporate policies regarding credit card information.
* implement the credit card companies’ security requirements.
* ensure that systems handle credit card data are segmented.
* review industry’s best practices for handling secure payments.

NO.126 Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?
* Availability of current infrastructure documentation
* Capability to take a snapshot of virtual machines
* Availability of web application firewall logs
* Capability of online virtual machine analysis

Section: INCIDENT MANAGEMENT AND RESPONSE

Get Instant Access to CISM Practice Exam Questions: https://www.test4engine.com/CISM_exam-latest-braindumps.html]