Practice Exam Questions

ISACA

CISM

Certified Information Security Manager

ISACA

Exam CISM

Certified Information Security Manager

Version: 35.0

[Total Questions: 258]

Question No : 1

To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls

Answer: A

Explanation: Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

Question No : 2

Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials

Answer: B

Question No : 3

Which of the following is the BEST way to obtain support for a new organization-wide information security program?

A. Benchmark against similar industry organizations

B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.

Answer: B

Explanation: Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

Question No : 4

Which of the following is MOST important to consider when determining asset valuation?

A. Asset recovery cost
B. Asset classification level
C. Cost of insurance premiums
D. Potential business loss

Answer: D

Question No : 5

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. results of exit interviews.
B. previous training sessions.
C. examples of help desk requests.
D. responses to security questionnaires.

Answer: C

Question No : 6

An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?

A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.

Answer: A

Question No : 7

Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?

A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents

Answer: C

Question No : 8

Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Business contingency plan

Answer: C

Question No : 9

Which of the following BEST enables staff acceptance of information security policies?

A. Strong senior management support

B. Gomputer-based training

C. Arobust incident response program

D. Adequate security funding

Answer: A

Question No : 10

Which of the following backup methods requires the MOST time to restore data for an application?

A. Full backup

B. Incremental

C. Differential

D. Disk mirroring

Answer: A

Explanation: The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

Question No : 11

Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?

A. Metrics to drive the information security program

B. Information security policies

C. A defined security organizational structure

D. An information security strategy

Answer: D

Question No : 12

If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:

A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.

Answer: B

Question No : 13

Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process

Answer: D

Explanation: An incident response plan is a critical component of an organization's overall security strategy, as it provides a framework for responding to security incidents in a timely and effective manner. To ensure that incidents are responded to by the appropriate individuals, it is essential to have a detailed incident notification process that clearly outlines who is responsible for responding to different types of incidents, how incidents should be reported and escalated, and who should be notified in the event of an incident. This helps to ensure that incidents are addressed promptly and effectively, and that the right resources are brought to bear to resolve the issue. Other important elements to include in an incident response plan include a clear definition of roles and responsibilities, a list of external resources to assist with incidents, and incident response procedures, such as steps to contain, assess, and recover from incidents.

Question No : 14

An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?

A. Conduct an information security audit.
B. Validate the relevance of the information.
C. Perform a gap analysis.
D. Inform senior management

Answer: B

Explanation: The first step the information security manager should take upon learning of the potential threat is to validate the relevance of the information. This should involve researching the threat to evaluate its potential impact on the organization and to determine the accuracy of the threat intelligence. Once the information is validated, the information security manager can then take action, such as informing senior management, conducting an information security audit, or performing a gap analysis.

Question No : 15

Which of the following is the BEST indication ofa successful information security culture?

A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.

Answer: B

Question No : 16

Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site

Answer: C

Question No : 17

Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards

Answer: A

Question No : 18

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

A. Business process owner
B. Business continuity coordinator
C. Senior management
D. Information security manager

Answer: A

Question No : 19

Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.

Answer: B

Question No : 20

Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?

A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats

Answer: B

Explanation: Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

Question No : 21

Which of the following would BEST ensure that security is integrated during application development?

A. Employing global security standards during development processes
B. Providing training on secure development practices to programmers
C. Performing application security testing during acceptance testing
D. Introducing security requirements during the initiation phase

Answer: B

Question No : 22

Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.

Answer: B