Free Questions for CISM by certscare

Shared by Glover on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?

Options:

A- Security requirements are included in the vendor contract

B- External security audit results are reviewed.

C- Service level agreements (SLAs) meet operational standards.

D- Business continuity contingency planning is provided

Answer:

A

Explanation:

Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.

https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations

https://www.sciencedirect.com/science/article/pii/S0378720616302166

Question 2

Question Type: **MultipleChoice**

After a recovery from a successful malware attack, instances of the malware continue to be discovered. Which phase of incident response was not successful?

Options:

A- Eradication

B Recovery

C- Lessons learned review

D- Incident declaration

Answer:

A

Explanation:

Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.

https://www.securitymetrics.com/blog/6-phases-incident-response-plan

https://www.atlassian.com/incident-management/incident-response

https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

Question 3

Question Type: **MultipleChoice**

Which of the following BEST enables an organization to effectively manage emerging cyber risk?

Options:

A- Periodic internal and external audits

B- Clear lines of responsibility

C- Sufficient cyber budget allocation

D- Cybersecurity policies

Answer:

D

Explanation:

Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-

9781119801948

Question 4

Question Type: MultipleChoice

Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

Options:

A- Return on investment (ROI)

B- Compliance requirements

C- Target audience

D- Criticality of information

Answer:

D

Explanation:

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question 5

Question Type: MultipleChoice

An organization is leveraging tablets to replace desktop computers shared by shift-based staff These tablets contain critical business data and are inherently at increased risk of theft Which of the following will BEST help to mitigate this risk"

Options:

A- Deploy mobile device management (MDM)

B- Implement remote wipe capability.

C- Create an acceptable use policy.

D- Conduct a mobile device risk assessment

Answer:

D

Explanation:

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question 6

Question Type: MultipleChoice

In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?

Options:

A- Ownership of security

B- Compliance with policies

C- Auditability of systems

D- Allocation of training resources

Answer:

A

Explanation:

Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks. Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

Question 7

Question Type: MultipleChoice

Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?

Options:

A- Conduct a cost-benefit analysis.

B- Consult corporate legal counsel

C- Update the information security policy.

D- Perform a gap analysis.

Answer:

D

Explanation:

When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question 8

Question Type: MultipleChoice

Which of the following is the BEST way lo monitor for advanced persistent threats (APT) in an organization?

Options:

A- Network with peers in the industry to share information.

B- Browse the Internet to team of potential events

C- Search for anomalies in the environment

D- Search for threat signatures in the environment.

Answer:

C

Explanation:

An advanced persistent threat (APT) is a stealthy and sophisticated attack that aims to compromise and maintain access to a target network or system over a long period of time, often for espionage or sabotage purposes. APTs are difficult to detect by conventional security tools, such as antivirus or firewalls, that rely on signatures or rules to identify threats. Therefore, the best way to monitor for APTs is to search for anomalies in the environment, such as unusual network traffic, user behavior, file activity, or system configuration changes, that may indicate a compromise or an ongoing attack. Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

Question 9

Question Type: MultipleChoice

A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?

Options:

A- Determine the required security controls for the new solution

B- Review the disaster recovery plans (DRPs) of the providers

C- Obtain audit reports on the service providers' hosting environment

D- Align the roles of the organization's and the service providers' stats.

Answer:

A

Explanation:

Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question 10

Question Type: MultipleChoice

Which of the following should be triggered FIRST when unknown malware has infected an organization's critical system?

Options:

A- Incident response plan

B- Disaster recovery plan (DRP)

C- Business continuity plan (BCP)

D- Vulnerability management plan

Answer:

A

Explanation:

The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization's critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating

the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

Question 11

Question Type: MultipleChoice

Which of the following should include contact information for representatives of equipment and software vendors?

Options:

A- Information security program charter

B- Business impact analysis (BIA)

C- Service level agreements (SLAs)

D- Business continuity plan (BCP)

Answer:

D

Explanation:

The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/business-continuity-management-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis