Check answer:

Which of the following is the MOST important for an information security manager to consider when developing a new information security policy?

1. Alignment with industry standards
2. Information security budget allocation
3. Organizational goals and objectives
4. Organizational culture and complexity

Ans: C

What should be ain information security’s manager’s FIRST step when developing a business case for a new intrusion detection system (IDS) solution?

1. Calculate the total cost of ownership (TCO).
2. Perform a cost-benefit analysis.
3. Conduct a feasibility study
4. Define the issues to be addressed.

Which of the following is a PRIMARY responsibility of an information security steering committee?

1. Drafting information security policities in line with business objectives
2. Updating the information security threat profile
3. Developing an information security architecture
4. Approving business cases for information security initiatives

Proposed : D

Which of the following defines the minimum security requirements that a specific system must meet?

1. Security procedure
2. Security baseline
3. Security guideline
4. Security policy

Ans: B Security baseline.

CISM All questions[QZ4050]

Which of the folliwng is the BEST control to minimize the risk associated with loss of information as a result of ransomware exploiting a zero-day vulnerability?

A A security operation centre

A Public key Infrastructure

A Patch management process

A data recovery process

Ans: A data recovery process.

An inexperienced information security manager is relying on its internal audit department to design and implement key security controls. Which of the following is the GREATEST risk?

1. Conflict of interest
2. Violation of the audit charter
3. Inadequate implementation of controls
4. Inadequate audit skills.

Ans: Conflict of interest

What is the Primary purpose of communicating business impact to an incident response team?

1. To enable effective prioritization of incidents
2. To facilitate resource allocation to preventive measures
3. To provide information for communication of incidents
4. To provide monetary values for post-incident review

Ans: A

1 The use of a business case to obtain funding for an information security investment is MOST

effective when the business case: [43901]

A: realigns information security objectives to organizational strategy.

B: articulates management's intent and information security directives in clear language.

C: relates the investment to the organization's strategic plan.

D: translates information security policies and standards into business requirements.

C 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43901

2 Which of the following metrics would be considered an accurate measure of a information security

program's performance? [43902]

A: A combination of qualitative and quantitative trends that enable decision making.

B: The number of key risk indications (KRIs) identified, monitored, and acted upon.

C: A single numeric score derived from various measures assigned to the security program.

D: A collection of qualitative indicators that accurately measure security exceptions.

B 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

F43902

3 Which of the following is the PRIMARY reason to conduct periodic business impact assessments?

[43903]

A: Improve the results of last business impact assessment

B: Update recovery objectives based on new risks

C: Decrease the recovery times

D: Meet the needs of the business continuity policy

B 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43903

4 The PRIMARY purpose of a security information and event management (SIEM) system is to:

[43904]

A: track ongoing incidents.

B: resolve incidents.

C: identify potential incidents.

D: provide status of incidents.

C 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43904

5 Which of the following would BEST demonstrate the maturity level of an organization's security

incident response program? [43905]

A: An increase in the number of reported incidents.

B: Ongoing review and evaluation of the incident response team.

C: A documented and live-tested incident response process.

D: A decrease in the number of reported incidents.

C 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43905

Page 1 of 102 03-Jul-2020

CISM All questions[QZ4050]

6 An information security manager has been made aware that some employees are discussing

confidential corporate business on social media sites. Which of the following is the BEST response

to this situation? [43906]

A: Scan social media sites for company-related information.

B: Block workplace access to social media sites and monitor employee usage.

C: Communicate social media usage requirements and monitor compliance.

D: Train employees how to set up privacy rules on social media sites.

C 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43906

7 An information security manager is reviewing the organization's incident response policy affected

by a proposed public cloud integration. Which of the following will be the MOST difficult to resolve

with the cloud service provider? [43907]

A: Accessing information security event data

B: Obtaining physical hardware for forensic analysis

C: Defining incidents and notification criteria

D: Regular testing of incident response plan

B 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43907

8 In a large organization, which of the following is the BEST source for identifying ownership of a PC?

[43908]

A: Identify management system

B: User ID register

C: Domain name server (DNS) records

D: Asset management register

D 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43908

9 A multinational organization has developed a bring your own device (BYOD) policy that requires

the installation of mobile device management (MDM) software on personally owned devices.

Which of the following poses the GREATEST challenge for implementing the policy? [43909]

A: Translation and communication of policy

B: Varying employee data privacy rights

C: Differences in corporate cultures

D: Differences in mobile OS platforms

B 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43909

10 To minimize security exposure introduced by changes to the IT environment, which of the

following is MOST important to implement as part of change management? [43910]

A: Conducting a security risk assessment prior to go-live

B: Requiring approval by senior management

C: Performing post-change reviews before closing change tickets

D: Performing a business impact analysis (BIA) prior to implementation

D 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43910

Page 2 of 102 03-Jul-2020

CISM All questions[QZ4050]

11 Which of the following is the BEST strategy to implement an effective operational security posture?

[43911]

A: Defense in depth

B: Threat management

C: Vulnerability management

D: Increased security awareness

D 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43911

12 A legacy application does not comply with new regulatory requirements to encrypt sensitive data

at rest, and remediating this issue would require significant investment. What should the

information security manager do FIRST? [43912]

A: Determine the cost to remediate the noncompliance.

B: Present the noncompliance risk to senior management.

C: Investigate alternative options to remediate the noncompliance.

D: Assess the business impact to the organization.

D 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43912

13 The MOST important reason to maintain key risk indicators (KRIs) is that: [43913]

A: threat and vulnerabilities continuously evolve.

B: they are needed to verify compliance with laws and regulations.

C: management uses them to make informed business decisions.

D: they help assess the performance of the security program.

A 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43913

14 The BEST way to encourage good security practices is to: [43914]

A: schedule periodic compliance audits.

B: discipline those who fail to comply with the security policy.

C: recognize appropriate security behavior by individuals.

D: publish the information security policy.

A 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43914

15 Which of the following would be MOST effective in preventing malware from being launched

through an email attachment? [43915]

A: Up-to-date security policies

B: Security awareness training

C: Placing the e-mail serve on a screened subnet

D: A network intrusion detection system (NIDS)

B 4

Cat: 1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43915

Page 3 of 102 03-Jul-2020

|  |
| --- |
| 56. An organization enacted several information security policies to satisfy regulatory requirements. Which of the following situations would MOST likely increase the probability of noncompliance to these requirements? A: Availability of security policy documents a public website B: Lack of training for end users on security policies C: Lack of training for end users on security policies D: Inadequate buy-in from system owners to support the policies  Answer:D |
| 93. Which of the following is the BEST reason to develop comprehensive information security policies? A: To comply with external industry and government regulations B: To gain senior management support for the information security program C: To align the information security program to organizational strategy D: To support development of effective risk indicators  Answer:C |
| 61. When implementing security architecture, an information security manager MUST ensure that security controls: A: are transparent. B: form multiple barriers against threats. C: form multiple barriers against threats. D: are communicated through security policies.  Answer:C |
| 84. A security team is conducting its annual disaster recovery test. Post-restoration testing shows the system response time is significantly slower due to insufficient bandwidth for internet connectivity at the recovery center. Which of the following is the security manager's BEST course of action? A: Document the deficiency for review by business leadership. B: Pursuer risk acceptance for the slower response time. C: Pursuer risk acceptance for the slower response time. D: Reduce the number of applications marked as critical.  Answer:A |
| 55. Which of the following techniques is MOST useful when an incident response team needs to external attacks on multiple corporate network devices? A: Vulnerability assessment of network devices B: Penetration testing of network devices C: Security event correlation analysis D: Endpoint baseline configuration analysis  Answer:C |
| 63. Which of the following is the BEST approach for an information security manager to effectively manage third-party risk? A: Ensure senior management has approved the vendor relationship. B: Ensure risk management efforts are commensurate with risk exposure. C: Ensure vendor governance controls are in place. /  D: Ensure controls are implemented to address changes in risk.  Answer:D |
| 2. What should the information security manager recommend to support the development of a new web application that will allow retail customers to view inventory and order products? A: Implementation of secure transmission protocols B: Request customers adhere to baseline security standards C: Request customers adhere to baseline security standards D: Building an access control matrix  Answer:A |
| . Which of the following provides the BEST evidence that the information security program is aligned to the business strategy? A: The information security team is able to provide key performance indicators (KPIs) to senior management. B: Information security initiatives are directly correlated to business processes. C: Information security initiatives are directly correlated to business processes. D: The information security program manages risk within the business's risk tolerance.  Answer:C |
| . Which of the following MOST effectively helps an organization to align information security governance with corporate governance? A: Developing security performance metrics B: Adopting global security standards to achieve business goals C: Adopting global security standards to achieve business goals D: Prioritizing security initiatives based on IT strategy  Answer:B |
| 17. Which of the following is MOST important for effective communication during incident response? A: Establishing a recovery time objective (RTO) B: Maintaining a  C: Maintaining a relationship with media and law enforcement D: Establishing a mean time to resolve (MTTR) metric  Answer:B |
| 6. An organization recently rolled out a new procurement program that does not include any security requirements. Which of the following should the information security manager do FIRST? A: Conduct security assessments of vendors based on value of annual spend with each vendor. B: Escalate the procurement program gaps to the compliance department in case of noncompliance issues. C: Escalate the procurement program gaps to the compliance department in case of noncompliance issues. D: Ask internal audit to conduct an assessment of the current state of third-party security controls.  Answer:C |
| 40. Which of the following is MOST important for an information security manager to ensure is included in a business case for a new security system? A: Audit-logging capabilities B: Benchmarking results C: Benchmarking results D: Risk reduction associated with the system  Answer:D |
| 45. Which of the following is MOST important to building an effective information security program? A: Logical assess controls for information systems B: Relevant and timely content included in awar ness programs C: Management support for information security D: Information security architecture to increase monitoring activities  Answer:B |
| 39. Which of the following is the BEST reason to separate short-term from long-term plans within an information security roadmap? A: To allocate resources for initiatives B: To allow for reactive initiatives C: To allow for reactive initiatives D: To facilitate business plan reporting to management  Answer:A |
| 49. Which of the following is MOST helpful for prioritizing the recovery of IT assets during a disaster? A: Cost-benefit analysis B: Risk assessment C: Risk assessment D: Business impact analysis (BIA)  Answer:D |
| 34. Recovery time objectives (RTOs) are an output of which of the following? A: Business continuity plan (BCP) B: Disaster recovery plan (DRP) C: Business impact analysis (BIA) D: Service level agreement (SLA)  Answer:B |
| 28. Which of the following has the GREATEST impact on efforts to improve an organization's security posture? A: Well-documented security policies and procedures B: Automation of security controls C: Regular reporting to senior management D: Supportive tone at the top regarding security  Answer:B |
| 30. After adopting an information security framework, an information security manager is working with senior management to change the organization-wide perception that information security is solely the responsibility of the information security department. To achieve this objective, which should be the information security manager's FIRST initiative? A: Develop an information security awareness campaign with senior management's support. B: Document and publish the respobsibilities of the information security department. C: Document and publish the respobsibilities of the information security department. D: Implement a formal process to conduct periodic compliance reviews.  Answer:A |