CISM Q&As

Certified Information Security Manager

Pass Isaca CISM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/cism.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included.

Which of the following is the BEST course of action for the information security manager?

A. Instruct IT to deploy controls based on urgent business needs.

B. Present a business case for additional controls to senior management.

C. Solicit bids for compensating control products.

D. Recommend a different application.

Correct Answer: B

The information security manager should present a business case for additional controls to senior management, as this is the most effective way to communicate the risk and the need for mitigation. The information security manager should not instruct IT to deploy controls based on urgent business needs, as this may not align with the business objectives and may cause unnecessary costs and delays. The information security manager should not solicit bids for compensating control products, as this may not address the root cause of the risk and may not be the best solution. The information security manager should not recommend a different application, as this may not be feasible or desirable for the business. References: CISM Review Manual 2023, page 711; CISM Review Questions, Answers and Explanations Manual 2023, page 252

QUESTION 2

Which of the following is the BEST way to determine if an information security program aligns with corporate governance?

A. Evaluate funding for security initiatives

B. Survey end users about corporate governance

C. Review information security policies

D. Review the balanced scorecard

Correct Answer: C

One of the most important aspects of the action plan to execute the strategy is to create or modify, as needed, policies and standards. Policies are one of the primary elements of governance and each policy should state only one general security mandate. The road map should show the steps and the sequence, dependencies, and milestones.

QUESTION 3

Which of the following is MOST helpful in integrating information security governance with corporate governance?

A. Assigning the implementation of information security governance to the steering committee.

B. Including information security processes within operational and management processes.

C. Providing independent reports of information security efficiency and effectiveness to the board.

D. Aligning the information security governance to a globally accepted framework.

Correct Answer: B

QUESTION 4

Of the following, who is accountable for data loss in the event of an information security incident at a third-party provider?

A. The information security manager

B. The service provider that hosts the data

C. The incident response team

D. The business data owner

Correct Answer: D

The business data owner is accountable for data loss in the event of an information security incident at a third-party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third- party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume- 1/dataownership-and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

QUESTION 5

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

Correct Answer: A

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.

QUESTION 6

Which of the following is MOST important for an information security manager to regularly report to senior management?

A. Results of penetration tests

B. Audit reports

C. Impact of unremediated risks

D. Threat analysis reports

Correct Answer: C

QUESTION 7

Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness.

B. It is easier to manage and control.

C. It is more responsive to business unit needs.

D. It provides a faster turnaround for security requests.

Correct Answer: B

It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization. Decentralization allows you to use field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

QUESTION 8

Which of the following is MOST important to have in place to help ensure an organization\\'s cybersecurity program meets the needs of the business?

A. Risk assessment program

B. Information security awareness training

C. Information security governance

D. Information security metrics

Correct Answer: C

Information security governance is the process of establishing and maintaining the policies, standards, frameworks, and

best practices that guide the information security program of an organization. Information security governance helps to ensure that the information security program meets the needs of the business by aligning it with the organization\\'s risk appetite, objectives, and strategy. Information security governance also helps to coordinate and integrate various assurance functions, such as risk management, compliance, audit, and incident response, to provide a holistic view of the information security posture. Information security governance is essential for achieving a positive return on investment (ROI) from information security investments, as well as for enhancing the trust and confidence of internal and external stakeholders. References: CISM Review Manual (Digital Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management1. CISM Review Manual (Print Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management2. CISM ITEM DEVELOPMENT GUIDE, Domain 1: Information Security Governance, Task Statement 1.1, p. 193. Information security governance is MOST important to have in place to help ensure an organization\\'s cybersecurity program meets the needs of the business. This is because information security governance provides the strategic direction, oversight and accountability for the cybersecurity program. It also ensures that the program aligns with the business objectives, risk appetite and compliance requirements of the organization. Information security governance involves defining roles and responsibilities, establishing policies and standards, setting goals and metrics, allocating resources and monitoring performance of the cybersecurity program.

QUESTION 9

Which of the following BEST helps to ensure a risk response plan will be developed and executed in a timely manner?

A. Establishing risk metrics

B. Training on risk management procedures

C. Reporting on documented deficiencies

D. Assigning a risk owner

Correct Answer: D

Assigning a risk owner is the best way to ensure a risk response plan will be developed and executed in a timely manner, because a risk owner is responsible for monitoring, controlling, and reporting on the risk, as well as implementing the appropriate risk response actions. A risk owner should have the authority, accountability, and resources to manage the risk effectively. Establishing risk metrics, training on risk management procedures, and reporting on documented deficiencies are all important aspects of risk management, but they do not guarantee that a risk response plan will be executed promptly and properly. Risk metrics help to measure and communicate the risk level and performance, but they do not assign any responsibility or action. Training on risk management procedures helps to increase the awareness and competence of the staff involved in risk management, but it does not ensure that they will follow the procedures or have the authority to do so. Reporting on documented deficiencies helps to identify and communicate the gaps and weaknesses in the risk management process, but it does not provide any solutions or corrective actions. References: CISM Review Manual, 16th Edition, ISACA, 2021, pages 125-126, 136-137.

QUESTION 10

Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?

A. Information security management costs will be optimized.

B. Information security strategy will be in line with industry best practice.

C. Gaps between current and desirable levels will be addressed.

D. Staff awareness of information security compliance will be promoted.

Correct Answer: C

QUESTION 11

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. rebuild the server from the last verified backup.

B. place the web server in quarantine.

C. shut down the server in an organized manner.

D. rebuild the server with original media and relevant patches.

Correct Answer: D

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

QUESTION 12

Which of the following should be the PRIMARY focus of a post-incident review following a successful response to a cybersecurity incident?

A. Which control failures contributed to the incident

B. How incident response processes were executed

C. What attack vectors were utilized

D. When business operations were restored

Correct Answer: D

QUESTION 13

There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

A. Identify the vulnerable systems and apply compensating controls

B. Minimize the use of vulnerable systems

C. Communicate the vulnerability to system users

D. Update the signatures database of the intrusion detection system (IDS)

Correct Answer: A

The best protection is to identify the vulnerable systems and apply compensating controls until a patch is installed. Minimizing the use of vulnerable systems and communicating the vulnerability to system users could be compensating controls but would not be the first course of action. Choice D does not make clear the timing of when the intrusion detection system (IDS) signature list would be updated to accommodate the vulnerabilities that are not yet publicly known. Therefore, this approach should not always be considered as the first option.

QUESTION 14

When determining an acceptable risk level, which of the following is the MOST important consideration?

A. Threat profiles

B. System criticalities

C. Vulnerability scores

D. Risk matrices

Correct Answer: B

QUESTION 15

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

Correct Answer: C

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.