ISACA

CISM

Certified Information Security Manager (CISM)

https://killexams.com/pass4sure/exam-detail/CISM

Question #436 Topic 2

Inadvertent disclosure of internal business information on social media is BEST minimized by which of the following?

- A. Developing social media guidelines
- B. Educating users on social media risks
- C. Limiting access to social media sites
- D. Implementing data loss prevention (DLP) solutions

Answer: D

Question #437 Topic 2

Which of the following is the MOST important security consideration when using Infrastructure as a Service (IaaS)?

- A. Backup and recovery strategy
- B. Compliance with internal standards
- C. User access management
- D. Segmentation among tenants

Answer: C

Question #438 Topic 2

An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?

- A. Control owner responses based on a root cause analysis
- B. The impact of noncompliance on the organization's risk profile
- C. An accountability report to initiate remediation activities
- D. A plan for mitigating the risk due to noncompliance

Answer: B

Question #439 Topic 2

An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?

- A. Report the noncompliance to the board of directors.
- B. Inform respective risk owners of the impact of exceptions
- C. Design mitigating controls for the exceptions.
- D. Prioritize the risk and implement treatment options.

Answer: D

Question #440 Topic 2

Which of the following models provides a client organization with the MOST administrative control over a cloud-hosted environment?

- A. Storage as a Service (SaaS)
- B. Platform as a Service (PaaS)
- C. Software as a Service (SaaS)
- D. Infrastructure as a Service (IaaS)

Answer: D

Question #441 Topic 2

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?

- A. Communicate social media usage requirements and monitor compliance.
- B. Block workplace access to social media sites and monitor employee usage.
- C. Train employees how to set up privacy rules on social media sites.
- D. Scan social media sites for company-related information.

Answer: C

Question #442 Topic 2

Which of the following is the BEST
indication that an information security control is no longer relevant?

- A. Users regularly bypass or ignore the control.
- B. The control does not support a specific business function.
- C. IT management does not support the control.
- D. Following the control costs the business more than not following it.

Answer: B

Question #443 Topic 2

Which of the following metrics provides the BEST indication of the effectiveness of a security awareness campaign?

- A. The number of reported security events
- B. Quiz scores for users who took security awareness classes
- C. User approval rating of security awareness classes
- D. Percentage of users who have taken the courses

Answer: A

Question #444 Topic 2

An employee is found to be using an external cloud storage service to share corporate information with a third-party consultant, which is against company policy.
Which of the following should be the information security manager's FIRST course of action?

- A. Determine the classification level of the information.
- B. Seek business justification from the employee.
- C. Block access to the cloud storage service.
- D. Inform higher management a security breach.

Answer: A

Question #445 Topic 2

When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?

- A. Recommendations from senior management
- B. The business continuity plan (BCP)
- C. Business impact analysis (BIA) results

D. Vulnerability assessment results

Answer: C

Question #446 Topic 2

An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's FIRST course of action?

- A. Shut down the server in an organized manner.
- B. Validate that there has been an incident.
- C. Inform senior management of the incident.
- D. Notify the business process owner.

Answer: B

Question #447 Topic 2

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?

- A. Accessing information security event data
- B. Regular testing of incident response plan
- C. Obtaining physical hardware for forensic analysis
- D. Defining incidents and notification criteria

Answer: A

Question #448 Topic 2

The head of a department affected by a recent security incident expressed concern about not being aware of the actions taken to resolve the incident. Which of the following is the BEST way to address this issue?

- A. Ensure better identification of incidents in the incident response plan.
- B. Discuss the definition of roles in the incident response plan.
- C. Require management approval of the incident response plan.
- D. Disseminate the incident response plan throughout the organization.

Answer: B

Question #449 Topic 2

The PRIMARY reason for implementing scenario-based training for incident response is to:

- A. help incident response team members understand their assigned roles.
- B. verify threats and vulnerabilities faced by the incident response team.
- C. ensure staff knows where to report in the event evacuation is required.
- D. assess the timeliness of the incident team response and remediation.

Answer: D

Question #450 Topic 2

What should an information security manager do FIRST when a service provider that stores the organization's confidential customer data experiences a breach in its data center?

- A. Engage an audit of the provider's data center.
- B. Recommend canceling the outsourcing contract.
- C. Apply remediation actions to counteract the breach.

- D. Determine the impact of the breach.

Answer: D

Question #451 Topic 2

An organization was forced to pay a ransom to regain access to a critical database that had been encrypted in a ransomware attack. What would have BEST prevented the need to make this ransom payment?

- A. Storing backups on a segregated network
- B. Training employees on ransomware
- C. Ensuring all changes are approved
- D. Verifying the firewall is configured properly

Answer: A

KILL EXAMS
Questions & Answ
Killexams Inc.
KILL EXAMS
Test Engine V.5.3
Killexams Inc