QUESTION 1533
What should be the FIRST step when developing an asset management program?

A. Create a configuration management database
B. Encrypt assets containing sensitive data.
C. Classify assets according to risk.
D. Create an asset inventory.

Answer: D

QUESTION 1534
In the development of an information security strategy, recovery time objectives (RTOs) will serve as indicators of:

A. senior management support.
B. risk tolerances.
C. maturity levels.
D. open vulnerabilities.

Answer: B

QUESTION 1535
Who within an organization is accountable for ensuring incident notification and escalation processes are in place?

A. Data owner
B. Senior management
C. Information security manager
D. Security operations center management

Answer: B

QUESTION 1536
Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?

A. Root cause analysis results
B. Adverse effects on the business
C. Availability of resources
D. Legal and regulatory requirements

Answer: A

QUESTION 1537
Which of the following is the GREATEST risk associated with the installation of an intrusion prevention system (IPS)?

A. Staff may not be able to access the Internet.
B. Critical business processes may be blocked.
C. Data links can no longer be encrypted end-to-end.
D. IPS logfiles may become too large to process.

Answer: B

QUESTION 1538
When outsourcing sensitive data to a cloud service provider, which of the following should be the information security manager's MOST important.....

A. Data stored at the cloud service provider is not co-hosted.
B. The cloud service provider contract includes right to audit.
C. Access authorization includes biometric security verification.
D. Roles and responsibilities have been defined for the service provider.

Answer: B

QUESTION 1539
Which of the following is MOST important for the alignment of an information security program with the information security strategy?

A. Input from senior management
B. Adoption of an industry recognized framework
C. Benchmarking against industry peers
D. Identification of business-specific risk factors

Answer: A

QUESTION 1540
Which of the following should be the GREATEST concern when considering launching a counterattack in response to a network attack?

A. Incident impact escalation
B. Digital evidence contamination
C. Denial of service attacks on the external source
D. Legal ramifications

Answer: D

QUESTION 1541
What is the BEST approach for the information security manager to reduce the impact on a security program due to turnover within the security staff?

A. Recruit certified staff.
B. Revise the information security program.
C. Ensure everyone is trained in their roles.
D. Document security procedures.

CISM Exam Dumps CISM Exam Questions CISM PDF Dumps CISM VCE Dumps

https://www.braindump2go.com/cism.html

Answer: D

QUESTION 1542
An internal security audit has reported that authentication controls are not operating effectively. Which of the following is MOST important to c management?

A. The impact of the control weakness on the risk profile of the organization
B. The results of a business impact analysis (BIA)
C. A business case for implementing stronger authentication controls
D. An analysis of the impact of this type of control weakness on other organizations

Answer: A

QUESTION 1543
Which of the following is MOST important for an information security manager to present to senior management on a regular basis?

A. Details of reported vulnerabilities
B. Changes to the organization's threat environment
C. False positives found on the intrusion prevention system
D. Security controls in place to prevent the threats

Answer: B

QUESTION 1544
A business impact analysis (BIA) should be periodically executed PRIMARILY to:

A. analyze the importance of assets.
B. check compliance with regulations.
C. verify the effectiveness of controls
D. validate vulnerabilities on environmental changes.

Answer: C

QUESTION 1545
Which of the following is the MOST important consideration when updating procedures for managing security devices?

A. Updates based o the organization's security framework
B. Updates based on changes in risk, technology, and process
C. Review and approval of procedures by management
D. Notification to management of the procedural changes

Answer: A

QUESTION 1546
Which of the following is the PRIMARY reason to include message templates for communications with external parties in an incident response plan?

A. To ensure that messages to external parties are complete and accurate
B. To communicate efficiently and consistently
C. To eliminate reliance on a communications specialist
D. To automate communication with external parties without delay

Answer: B

CISM Exam Dumps CISM Exam Questions CISM PDF Dumps CISM VCE Dumps

https://www.braindump2go.com/cism.html

QUESTION 1547
Which of the following is the MOST effective way to help ensure information security programs are aligned with business objectives?

A. Implement information security awareness campaigns for business units.
B. Include business unit representation in the information security steering committee.
C. Develop information security policies based on laws and regulations.
D. Establish and monitor information security performance metrics for the business.

Answer: B

QUESTION 1548
Which of the following is MOST important when developing a security strategy?

A. Management direction on security
B. A well-defined security organization
C. Sufficient resource allocation by management
D. A risk-aware security culture

Answer: A