

➤ **Vendor: Isaca**

➤ **Exam Code: CISM**

➤ **Exam Name: Certified Information Security Manager**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [January/2021](#))**

**[Visit Braindump2go and Download Full Version CISM Exam Dumps](#)**

**QUESTION 1571**

Which of the following is MOST likely to result from a properly conducted post-incident review?

- A. Breach information is provided to the organization's key stakeholders and users.
- B. The cause of the incident is discovered and remediated.
- C. Forensic evidence is reviewed and provided to law enforcement
- D. The incident response team discovers inefficiencies in the recovery process.

**Answer: D**

**QUESTION 1572**

Labeling information according to its security classification:

- A. affects the consequences if information is handled insecurely,
- B. induces the number and type of counter measures required
- C. enhances the likelihood of people handling information securely,
- D. reduces the need to identify baseline controls for each classification.

**Answer: B**

**QUESTION 1573**

Which of the following is MOST likely to result from a properly conducted post-incident review?

- A. Breach information is provided to the organization's key stakeholders and users.
- B. The cause of the incident is discovered and remediated.
- C. Forensic evidence is reviewed and provided to law enforcement
- D. The incident response team discovers inefficiencies in the recovery process.

**Answer: D**

**QUESTION 1574**

Which of the following would provide senior management with the BEST overview of the performance of information security risk treatment options?

- A. Before-and-after heat maps
- B. Analysis of recent incident
- C. Detailed risk analysis of the treatments
- D. individual risk assessments

[CISM Exam Dumps](#) [CISM Exam Questions](#) [CISM PDF Dumps](#) [CISM VCE Dumps](#)

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

**Answer: A**

**QUESTION 1575**

Which of the following should be reviewed to obtain a structured overview of relevant information about an information security investment?

- A. Security balanced scorecard
- B. Information security strategy
- C. Business case
- D. Quantitative risk analysis report

**Answer: C**

**QUESTION 1576**

Which of the following is MOST important for an information security manager to communicate to senior management regarding the security program?

- A. User roles and responsibilities
- B. Potential risks and exposures
- C. Security architecture changes
- D. Impact analysis results

**Answer: B**

**QUESTION 1577**

When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure that the:

- A. forensic investigation software is loaded on the server.
- B. server is unplugged from power.
- C. integrity of evidence is preserved.
- D. server is backed up to the network.

**Answer: D**

**QUESTION 1578**

Which of the following is the MOST effective method to help ensure information security incidents are reported?

- A. Integrating information security language in corporate compliance rules
- B. Providing information security awareness training to employees
- C. Implementing an incident management system
- D. Integrating information security language in conditions of employment

**Answer: B**

**QUESTION 1579**

Which of the following should be the FIRST step when creating an organization's bring your own device (BYOD) program?

- A. identify data to be stored on the device
- B. Develop an acceptable use policy.
- C. Develop employee training.
- D. Pretest approved devices

**Answer: B**

**QUESTION 1580**

Which of the following is the BEST evidence of an effectively designed key risk indicator (KRI)?

- A. The KRI is quantitative
- B. The KRI measures inherent risk.
- C. The KRI predicts threats
- D. The KRI incorporates risk appetite

**Answer: B**

**QUESTION 1581**

Which of the following is the MOST important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

- A. The ability to restrict unapproved applications
- B. The ability to classify types of devices
- C. The ability to remotely locate devices
- D. The ability to centrally manage devices

**Answer: D**

**QUESTION 1582**

The MOST important reason to maintain metrics for incident response activities is to?

- A. support continual process improvement.
- B. analyze security incident trends
- C. ensure that evidence collection and preservation are standardized
- D. prevent incidents from reoccurring.

**Answer: A**

**QUESTION 1583**

Which of the following is the MOST effective way for an Information security manager to ensure that security is incorporated into an organization's project development processes?

- A. Participate in project initiation, approval, and funding.
- B. Develop good communications with the project management office
- C. Integrate organization's security requirements into project management.
- D. Conduct security reviews during design, testing and implementation

**Answer: C**

**QUESTION 1584**

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

- A. Senior management support
- B. Results of a cost-benefit analysis
- C. Results of a risk assessment
- D. Impact on the risk profile

**Answer: A**

**QUESTION 1585**

When scoping a risk assessment assets need to be classified by?

- A. redundancy and recoverability
- B. sensitivity and critically
- C. threats and opportunities
- D. likelihood and impact.

**Answer: B**

**QUESTION 1586**

Which of the following is MOST important to track for determining the effectiveness of an information security program?

- A. Return on investment (ROI)
- B. Key performance indicators (KPIs)
- C. Service level agreements (SLAs)
- D. Key risk indicators (KRIs)

**Answer: B**

**QUESTION 1587**

Which of the following is the MOST effective preventive control?

- A. Review of audit logs
- B. Segregation of duties
- C. Warning banners on login screens
- D. Restoration of a system from backup

**Answer: B**

**QUESTION 1588**

Which of the following BEST supports effective information security governance?

- A. A steering committee is established
- B. A baseline risk assessment is performed.
- C. Compliance with regulations is demonstrated.
- D. The information security manager develops the strategy

**Answer: A**

**QUESTION 1589**

Which of the following is MOST likely to occur following a security awareness campaign?

- A. An increase in the number of viruses detected in incoming email
- B. An increase in reported social engineering attempts
- C. A decrease in number of account lockouts
- D. A decrease in user-reported false positive incidents

**Answer: D**

**QUESTION 1590**

Which of the following is the BEST way for an information security manager to promote the integration of information security considerations into key business processes?

[CISM Exam Dumps](#) [CISM Exam Questions](#) [CISM PDF Dumps](#) [CISM VCE Dumps](#)

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

- A. Provide information security awareness training.
- B. Conduct a business impact analysis (BIA).
- C. Facilitate the creation of an information security steering group
- D. Conduct information security briefings for executives

**Answer: C**

**QUESTION 1591**

When responding to an incident, which of the following is required to ensure evidence remains legally admissible in court?

- A. Law enforcement oversight
- B. Chain of custody
- C. A documented incident response plan
- D. Certified forensics examiners

**Answer: B**