Vendor: (ISC)2

Exam Code: CISSP-ISSMP

Exam Name: Information Systems Security Management Professional

Version: DEMO

QUESTION 1
During a tabletop exercise, participants discuss their roles and responses to a simulated incident without actually activating systems. This is an example of which testing type?

A. Full interruption test
B. Parallel test
C. Structured walkthrough (tabletop) test
D. Simulation test

Answer: C
Explanation:
A tabletop/structured walkthrough is a discussion-based exercise where team members review procedures verbally without operational disruption. Answer options A and B involve actual system activity; D typically involves acting out response steps more actively than a tabletop but still short of live systems.

QUESTION 2
An organization discovers that an employee has been exfiltrating data slowly over several months to avoid detection thresholds. This is an example of which type of threat?

A. Advanced Persistent Threat (APT)
B. Insider threat
C. Script kiddie attack
D. Zero-day exploit

Answer: B
Explanation:
The scenario describes a malicious or negligent employee - an insider threat - regardless of the technique's sophistication. Answer option A is incorrect because APT specifically refers to a sustained, sophisticated external adversary campaign, not necessarily an employee.

QUESTION 3
Which document formally authorizes a project or security initiative and grants the project manager authority to apply organizational resources?

A. Statement of Work (SOW)
B. Project Charter
C. Risk Register
D. Business Case

Answer: B
Explanation:
The project charter formally authorizes the project's existence and gives the PM authority to use resources. Answer option A describes the work to be done; C tracks risks; D justifies the investment but doesn't grant authority.

QUESTION 4
Which of the following is the PRIMARY reason organizations classify data (e.g., Public, Internal, Confidential, Restricted)?

A. To simplify storage costs

B. To apply appropriate handling and protection controls based on sensitivity
C. To comply with backup schedules
D. To determine employee salaries

Answer: B
Explanation:
Data classification ensures resources are protected proportionally to their sensitivity and value, guiding access control, encryption, and handling requirements.

QUESTION 5
Sarah, a CISO, wants to measure how quickly her SOC detects and responds to incidents. Which metrics should she track?

A. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)
B. Number of employees trained
C. Number of open vulnerabilities
D. Annual security budget

Answer: A
Explanation:
MTTD and MTTR are standard operational metrics for evaluating detection and response efficiency. Answer options B, C, and D measure other program aspects, not response speed.

QUESTION 6
Which of the following BEST describes "separation of duties" as a control?

A. Ensuring only one person has access to critical systems for accountability
B. Dividing critical tasks among multiple people to prevent fraud or error by a single individual
C. Rotating employees between departments annually
D. Requiring dual approval for all emails

Answer: B
Explanation:
Separation of duties prevents any single individual from having enough control to commit fraud or cause significant harm undetected. Answer option A actually describes the opposite risk that this control mitigates.

QUESTION 7
During contract negotiation with a cloud service provider, which clause is MOST important for ensuring the organization can retrieve its data upon contract termination?

A. Indemnification clause
B. Data portability / exit clause
C. Non-compete clause
D. Force majeure clause

Answer: B
Explanation:
An exit/data portability clause ensures the organization can retrieve or transfer its data in a usable format when the relationship ends, preventing vendor lock-in or data loss.

QUESTION 8
Which of the following is the correct order of the classic risk management process?

A. Identify → Analyze → Evaluate → Treat → Monitor
B. Treat → Identify → Monitor → Analyze
C. Monitor → Identify → Treat → Analyze
D. Analyze → Treat → Identify → Evaluate

Answer: A
Explanation:
The standard risk management lifecycle (per ISO 31000 and similar frameworks) begins with identification, followed by analysis, evaluation, treatment, and ongoing monitoring/review.

QUESTION 9
Which of the following is generally the LEAST effective control type on its own for mitigating insider threats?

A. Technical (DLP, access controls)
B. Administrative (background checks, policy)
C. Physical (badge access)
D. A single control type used alone, regardless of category

Answer: D
Explanation:
ISSMP emphasizes defense-in-depth - insider threat mitigation requires a layered combination of administrative, technical, and physical controls; relying on any single category alone leaves gaps.

QUESTION 10
Which of the following BEST defines "risk appetite"?

A. The specific dollar amount allocated to security tools
B. The level of risk an organization is willing to accept in pursuit of its objectives
C. The maximum number of vulnerabilities allowed in production
D. The insurance premium a company is willing to pay

Answer: B
Explanation:
Risk appetite is a strategic, board-level concept describing the amount and type of risk an organization is willing to pursue or retain. Answer options A, C, and D are operational or financial specifics, not the governance-level definition.

QUESTION 11
A security manager wants to ensure that critical business functions can continue during a disruption with minimal manual intervention. Which BCP strategy addresses this BEST?

A. Manual workaround procedures
B. Redundant/failover systems with automated switchover
C. Employee cross-training

D. Annual tabletop exercises

Answer: B
Explanation:
Automated redundancy/failover minimizes downtime and manual intervention during disruption. Answer options A, C, and D support resilience but don't directly provide continuous automated operation.

QUESTION 12
Which of the following is the PRIMARY difference between a vulnerability assessment and a penetration test?

A. Vulnerability assessments are always more expensive
B. A vulnerability assessment identifies weaknesses; a penetration test actively exploits them to demonstrate impact
C. Penetration tests only apply to web applications
D. There is no meaningful difference

Answer: B
Explanation:
Vulnerability assessments are typically passive/scanning-based identification of weaknesses, while pentests actively attempt exploitation to prove real-world risk and impact.

QUESTION 13
An organization's disaster recovery plan specifies an RPO of 4 hours for its ERP system. Which backup strategy would BEST support this requirement?

A. Weekly full backups only
B. Backups every 4 hours or continuous data replication
C. Annual backups
D. Backups only after major releases

Answer: B
Explanation:
RPO defines the maximum tolerable data loss measured in time; to meet a 4-hour RPO, backups/replication must occur at least that frequently. Answer options A, C, and D would result in far greater data loss than acceptable.

QUESTION 14
Which of the following BEST describes "due care" versus "due diligence"?

A. Due care is a one-time act; due diligence is ongoing research and investigation to maintain that standard
B. They are legally identical terms
C. Due diligence applies only to financial audits
D. Due care applies only to physical security

Answer: A
Explanation:
Due care refers to the reasonable steps taken to protect assets/prevent harm (the "prudent person" standard); due diligence refers to the ongoing investigation and research to identify and

understand risks before/while exercising due care.

QUESTION 15
During an incident, which role is typically responsible for making the final decision to invoke the disaster recovery plan?

A. Help desk technician
B. Emergency management team / senior management
C. Software team
D. Off-site storage team

Answer: B
Explanation:
Plan invocation is a business decision made by those with authority over organizational impact, typically emergency management or senior leadership, not technical teams who execute the response.

QUESTION 16
Which of the following laws primarily addresses the security and privacy of financial institution customer data in the United States?

A. HIPAA
B. Gramm-Leach-Bliley Act (GLBA)
C. FERPA
D. COPPA

Answer: B
Explanation:
GLBA requires financial institutions to explain information-sharing practices and safeguard sensitive customer data. HIPAA covers healthcare, FERPA covers education records, COPPA covers children's online privacy.

QUESTION 17
A security governance framework primarily helps ensure which of the following?

A. Technical staff can bypass policy for efficiency
B. Security decisions align with organizational objectives and are subject to appropriate oversight
C. All risk is eliminated
D. Compliance replaces the need for risk management

Answer: B
Explanation:
Governance frameworks establish accountability, decision rights, and alignment between security activities and business objectives - they don't eliminate risk or replace risk management.

QUESTION 18
Which of the following BEST describes the purpose of a "war room" during a major incident?

A. A physical/virtual space for centralized coordination and decision-making during response
B. A location for storing backup tapes

C. A room dedicated to employee training
D. A secure facility for destroying evidence

Answer: A
Explanation:
A war room centralizes communication and coordination among response teams and stakeholders during a significant incident, improving situational awareness and decision speed.

QUESTION 19
Which of the following is TRUE regarding the relationship between policies, standards, procedures, and guidelines?

A. Guidelines are mandatory; policies are optional
B. Policies are high-level and mandatory; standards support policies with specific mandatory requirements; procedures give step-by-step instructions; guidelines are recommended
C. Procedures are the highest-level governing document
D. Standards and guidelines are interchangeable terms

Answer: B
Explanation:
This is the standard hierarchy in security governance: Policy (mandatory, high-level) → Standards (mandatory, specific) → Procedures (mandatory, step-by-step) → Guidelines (recommended, flexible).

QUESTION 20
An organization wants to reduce the likelihood of a successful phishing attack. Which combination of controls represents defense-in-depth?

A. Email filtering only
B. Email filtering + security awareness training + endpoint detection + incident response plan
C. Firewall rules only
D. Annual policy review only

Answer: B
Explanation:
Defense-in-depth layers multiple, complementary controls (technical, administrative, and procedural) so that failure of one layer doesn't result in total compromise.

QUESTION 21
Which of the following BEST describes a "single point of failure" in the context of business continuity?

A. A redundant system with automatic failover
B. A component whose failure would disrupt the entire system or process with no alternative
C. A backup power generator
D. A geographically distributed data center

Answer: B
Explanation:
A single point of failure is a critical dependency lacking redundancy; its failure causes total disruption. BCP efforts specifically aim to identify and eliminate these.

QUESTION 22
Which of the following roles is typically responsible for developing and maintaining the organization's overall security awareness training program?

A. Chief Financial Officer
B. Security Awareness/Training Manager (often under CISO)
C. External auditor
D. Legal counsel

Answer: B
Explanation:
Security awareness and training is typically owned within the security organization, often reporting to the CISO, as part of the human risk management function.

QUESTION 23
When evaluating a third-party vendor's security posture, which of the following provides the MOST independent and standardized assurance?

A. Vendor's self-reported questionnaire only
B. SOC 2 Type II report from an independent auditor
C. Marketing materials
D. A verbal assurance from the vendor's sales team

Answer: B
Explanation:
A SOC 2 Type II report provides independent, third-party verified evidence of controls operating effectively over a period of time, offering stronger assurance than self-attestation or informal claims.

QUESTION 24
Which of the following is the PRIMARY purpose of a security metrics dashboard presented to the board of directors?

A. To show granular technical logs
B. To communicate security posture and risk in business-relevant, digestible terms
C. To replace the need for an annual audit
D. To list every open vulnerability by CVE number

Answer: B
Explanation:
Board-level reporting should translate technical detail into business risk context (trends, exposure, program maturity) rather than raw technical data.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**