CISSP-ISSMP isc

Number: CISSP-ISSMP
Passing Score: 800
Time Limit: 120 min

Exam A

QUESTION 1
A company has asked its security analyst to draft a document describing due diligence practices an employee should follow when traveling for company business purposes. Which of the following combinations of information security practices is MOST effective for the "road warrior"?

A. Hard disk encryption, shredding, and awareness of environment
B. Laptop cable locks, encrypted thumb drives to transport data, and paper shredding
C. Using File Transfer Protocol (FTP) to transport data back to the office, shredding CD-ROMs, and removing the hard drive from the laptop
D. Using only paper, cell phones, and Internet email to conduct company business

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures to specific individuals?

A. Role-based access control
B. Biometric access control
C. Two-factor authentication
D. Application hardening

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
International Standards Organization (ISO) 27002 provides a framework for establishing information security

A. development.
B. procurement.
C. management.
D. analysis.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which trusted third-party authenticates public encryption keys?

A. Public Key Infrastructure (PKI)
B. Certificate Authority (CA)
C. Key Distribution Center (KDC)
D. Certificate Revocation List (CRL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which one of the following is the MAIN goal of a security awareness program when addressing senior management?

A. To provide a way to communicate security procedures
B. To provide a clear understanding of potential risk and exposure
C. To provide an opportunity to disclose exposures and risk analysis
D. To provide a forum to communicate user responsibilities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Information security policies are written to describe

A. security controls.
B. guidelines for users.
C. specific system restrictions.
D. goals of the security program.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following is the FIRST step in a successful security risk analysis?

A. Performing a network security scan

B. Verifying inventory
C. Confirm firewall rules
D. Reviewing the Intrusion Detection System (IDS) logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
The BEST solution an organization can implement to assure unauthorized employees do not remove servers from the server room is

A. a security awareness program.
B. restricted work areas.
C. a staff evaluation program.
D. closed-Circuit Television (CCTV)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A newly assigned Risk Manager requests access to a file share containing corporate financial records. The access request is reviewed by the Chief Financial Officer (CFO) who determines that access will be granted to only three files for one month. The principle is referred to as

A. job rotation.
B. least privilege.
C. special privilege.
D. separation of duties.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following helps to assure alignment of security functions and the organization's goals, missions and objectives?

A. Governance oversight
B. System security oversight
C. Human Resource (HR) oversight
D. Business service oversight

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following are attributes provided by a digital signature?

A. Confidentiality and availability
B. Confidentiality and integrity
C. Non-repudiation and availability
D. Non-repudiation and integrity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Risk avoidance is a strategy that attempts to

A. prevent the risk from being realized.
B. shift the risk to other entities.
C. reduce the impact caused by the vulnerability through planning and preparation.
D. avoid any actions to be taken to prevent the vulnerability.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements:

A. People, technology, and operations.
B. End point, network, and Demilitarized Zone (DMZ) security.
C. Confidentiality, authenticity, and identity.
D. Policies, standards, and procedures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Project sponsorship for evaluating outsourcing of IT services should be obtained from the

A. IT Services Manager.
B. Project Management Office (PMO).
C. Executive Management.
D. Legal and Compliance Department.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A background check is an example of which of the following security controls?

A. Administrative
B. Physical
C. Logical
D. Technical

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
An organization has deployed a large-scale Public Key Infrastructure (PK1) and has just issued a Certificate Authority (CA) revocation list. This list is used to revoke the

A. public key certificate for all entities within a CA.
B. private key certificate for all CAs and their entities.
C. private key certificate of the root CA only.
D. public-key certificates of other CAs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The MOST severe risk posed by an unauthorized Universal Serial Bus (USB) storage device found attached to a standalone workstation is

A. the loss or theft of sensitive data
B. the compromise of the corporate network security perimeter.
C. a Man-in-the-Middle (MITM) attack.
D. a Denial of Service (DoS) attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Most attacks against cryptosystems are successful due to

A. cryptanalysis.
B. poor algorithms.
C. brute force attacks.
D. weak implementations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
One reason to compute a hash for data that is sent to a user and later returned is to

A. mitigate side-channel leakage
B. protect the secrecy of the data.
C. validate the integrity of the data
D. prevent timing channel attacks.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Deployment of a "default deny" security strategy is a key component in which of the following?

A. Sandbox Security
B. Negative Security
C. Positive Security
D. Authentication Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An effective method used to detect compromised software includes

A. comparing file hashes.
B. verifying file sizes.
C. viewing contents in text form.
D. clearing alternate data streams.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A Domain Name Server (DNS) caches information mapping host names into Internet Protocol (IP) addresses. If an attacker is able to "poison" a DNS cache by

inserting a false IP address with a name, this will cause a host to route connections to another host incorrectly. This problem would be addressed by which of the following design principles?

A. Least Common Mechanism
B. Complete Mediation
C. Economy of Mechanism
D. Separation of Privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
The initial phase of the system development life cycle would normally include

A. cost-benefit analysis.
B. system design review.
C. executive project approval.
D. project status summary.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Programmed procedures which ensure that valid transactions are processed accurately and only once are referred to as

A. data installation controls.
B. application controls.
C. operation controls.
D. physical controls.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which one of the following identifies the first phase of a Distributed Denial-of-Service (DDoS) attack?

A. Establishing communications between the handler and agent
B. Disrupting the normal traffic to the host
C. Disabling the router so it cannot filter traffic
D. Compromising as many machines as possible

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
The ISO 15408 Common Criteria (CC) Protection Profile (PP) is used to provide

A. an implementation-independent set of security requirements for a category of products or systems.
B. an implementation-independent set of security answers for a category of products or systems.
C. a set of security requirements and specifications used as the basis of evaluation of an identified product or systems.
D. a set of security answers and features used as the basis of evaluation of an identified product or systems.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Software development managers can leverage program modules that have had corrective actions taken to fix known bugs through the use of

A. tested units.
B. pptimized code.
C. reusable code.
D. acceptance units.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Threat modeling should begin during which phase of the Systems Development Life Cycle (SDLC)?

A. Requirements Gathering
B. Development
C. Design
D. Testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
An attacker wants to be able to attempt to discover vulnerabilities in a new software application. The only information available for breaking this new application is the program disk received from a friend. What method can the developer of the application use to make the binary code difficult to decompile or return to the original programming language?

A. Parsing
B. Obfuscation
C. Encryption
D. Factoring

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
When a vulnerability becomes publicly known and the weakness is exploited before a patch is available, this

A. Denial of Service DOS
B. SQL Slammer
C. iiscrack
D. zero-day

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
The risk elements that should be considered when designing a vulnerability test are vulnerability,

A. asset, and threat.
B. ease of use, and budget.
C. revenue, and threat.
D. ease of use, and revenue.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following should be considered during the execution of a vulnerability test?

A. Information security policy maintenance
B. Manual and automated testing
C. Separation of duties and job rotation
D. User accepted testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
One of the greatest risks in relying on an Intrusion Detection System (IDS) to defend against malicious traffic is

A. there are too many serious attacks to effectively monitor them all.
B. many security incidents fit into normal traffic rules.
C. the IDS causes a bottleneck when required to decrypt packets.
D. the risk of causing a Denial of Service (DoS) by dropping packets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Security authorizations of an information system are the processes to

A. validate the cost for the development of the system.
B. assess and accept the risks to operating the system.
C. determine the security architecture of the system.
D. increase user's security awareness of the system.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which is the FIRST step that should be considered in a penetration test?

A. The approval of change control management
B. The development of a detailed test plan
C. The formulation of specific management objectives
D. The communication process among team members

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What is the MAIN purpose of a Configuration Management System (CMS)?

A. To provide versioned documentation of a computer system
B. To avoid problems that could impact a computer system
C. To determine the cause of a system problem
D. To track changes to a computer system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What attack can be avoided by verifying that each session is required to change slightly from one session to the next?

A. Impersonation
B. Playback
C. Eavesdropping
D. Teardrop

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which department assures that vendors are fulfilling their contractual security obligations?

A. Human Resources (HR) department
B. Information Technology (IT) department
C. Internal audit department
D. Compliance department

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following would be considered a significant change to a system and therefore, would most likely require the reinitiation of the security authorization process prior to the date established for reauthorization?

A. Changing the database management system (DBMS)
B. Changing the security steward
C. Updating corporate security policy
D. Minor point upgrade of the application code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
What type of assessment tests the ability of an organization to know who, what, where, and when devices are connected to the network?

A. Infrastructure
B. Initial technical
C. Access control
D. Change impact

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Audit evidence for compliance should be

A. kept three to seven years.
B. deleted after the audit is complete.
C. kept according to the retention schedule.
D. stored indefinitely.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A system administrator is asked to perform an operating system (OS) upgarde on a production server OS that is no longer supported by the vendor. In this situation what must also be included along with the request to ensure risks are controlled during the upgrade?

A. Management authorization
B. Auditor authorization
C. Physical controls
D. Access controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A former employee continues to access corporate systems in violation of the organization's policies. This is a failure of

A. user entitlement.
B. intrusion detection and prevention.
C. identity and access provisioning.
D. federated identity management.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
During maintenance of deployed software, which of the following is the BEST method to assure that vulnerabilities are not introduced to updated code using

A. penetration testing.
B. code module reviews.
C. requirements analysis.
D. user acceptance testing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A system using Discretionary Access Control (DAC) is vulnerable to which one of the following direct attacks?

A. Trojan horse
B. Phreaking
C. Denial of Service (DoS)
D. SYN flood

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
When defining a user's roles from an IT security standpoint it is important to include

A. job experience.
B. targeted system privileges.
C. management chain.
D. office location.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is determined by a Business Impact Analysis (BIA)?

A. The identification of the people needed for recovery
B. The classification of the most sensitive data
C. The value of insurance required for facilities
D. The maximum-tolerable downtime for business processes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
When is the BEST time to test a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP)?

A. During a convenient time for customers
B. During a convenient time for the testing team
C. During a convenient time based on schedule and cost
D. During a convenient time based on scope and impact

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
The detailed response procedures for incident response teams should include the agreed upon meeting place for the teams, the activation and mobilization plan, and which of the following procedures?

A. Recovery

B. Business Impact Analysis (BIA)
C. Restoration
D. Information gathering and reporting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Fault tolerance requirements are based on the

A. Mean Time Between Failures (MTBF).
B. Memorandum of Understanding (MOU).
C. Maximum Tolerable Downtime (MTD).
D. Mandatory Access Control (MAC).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
What actions should be taken to restore a system's operational capability and data files after a system failure?

A. Implement recovery procedures
B. Synchronize system programs
C. Execute risk management
D. Recover storage media

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

When purchasing proprietary software from a vendor, source code escrow is BEST used to protect against

A. system data loss.

B. vendor bankruptcy.

C. copyright violation.

D. legal liability.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

A critical application that processes an organization's financial data relies on an authentication server to validate user permissions. The authentication server has experienced a catastrophic hard drive failure. There was no backup or failover for the authentication server. Which of the following is the best implementation to prevent the loss of access to the financial data?

A. Data replication to a disaster recovery site

B. High availability clustering

C. Implementing a Storage Area Network (SAN)

D. Redundant financial application servers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

The BEST motivators for an employee to understand and follow the corporation's Business Continuity Plan (BCP) are: job advancement, benefits, and

A. corporate loyalty.

B. disciplinary action.
C. compensation.
D. personal reputation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is a potential problem when creating a Message Digest (MD) for forensic purposes?

A. The process is very slow
B. The file's last access time is changed
C. The MD is almost as long as the data string
D. One-way hashing technology invalidates MD processing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A malware incident response plan

A. should focus on the active attack.
B. needs to focus primarily on the payload left behind.
C. lists acceptable websites that employees can access.
D. should include anti-virus update cycle times.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Honeynet analysis is undertaken for the purpose of

A. responding to an immediate threat.
B. discovering the characteristics of the existing threat in the network
C. discovering fraud and abuse of internal resources
D. blocking known perpetrators for entry into the local network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
The steps involved in handling a security incident are categorized into which of the following stages?

A. Identification of the critical business function, define recovery objectives, ensure administrative control, containment of the problem, and follow-up analysis
B. Establishment of processes, conducting security education, reporting the issue to management, eradication of the problem, and follow-up analysis
C. Establishment of processes, identification of the problem, eradication of the problem, recovering from the incident, and the follow-up analysis
D. Identification of the problem, containment of the problem, eradication of the problem, recovering from the incident, and the follow-up analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
When commencing a computer forensics investigation, the investigator must FIRST

A. notify law enforcement.
B. identify the issue.

C. verify if any rules or policies have been broken.
D. seize all related evidence.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is a canon of the (ISC)2 code of ethics?

A. Provide volunteer services to any of the security organizations
B. Provide diligent and competent service to principals
C. Do not misuse the (ISC)2 logo and follow (ISC)2 logo guidelines
D. Maintain the required Continued Professional Education (CPE) credits for the (ISC)2 certification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
What is the BEST example of a multi-national statement on criminal activity on the Internet?

A. Council of Europe Cybercrime Convention
B. United Nations Declaration on Friendly Relations
C. Vienna Declaration on Crime and Justice

D. United Nations Congress on the Prevention of Crime

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
In a system where security has potentially been compromised, non-repudiation of the origin of data is achieved through the use of digital signatures and

A. stream-based ciphers.
B. end-to-end encryption.
C. trusted third parties.
D. stenography.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: