



Reference Solution for CISSP.exam.64q CISSP

CISSP

Certified Information Systems Security Professional

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (64 questions)

Question 1

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

- ☒ Transport layer
- ☐ Application layer
- ☐ Network layer
- ☐ Session layer

Question 2

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

- ☒ System acquisition and development
- ☐ System operations and maintenance
- ☐ System initiation
- ☐ System implementation

Explanation:

Reference <https://online.concordia.edu/computer-science/system-development-life-cycle-phases/>

Question 3

Which of the following is an advantage of on-premise Credential Management Systems?

- ☐ Lower infrastructure capital costs
- ☒ Control over system configuration
- ☐ Reduced administrative overhead
- ☐ Improved credential interoperability

Question 4

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

- ☐ Continuously without exception for all security controls
- ☒ Before and after each change of the control
- ☐ At a rate concurrent with the volatility of the security control
- ☐ Only during system implementation and decommissioning

Question 5

A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

- ☐ Ignore the request and do not perform the change.
- ☐ Perform the change as requested, and rely on the next audit to detect and report the situation.
- ☐ Perform the change, but create a change ticket regardless to ensure there is complete traceability.
- ☒ Inform the audit committee or internal audit directly using the corporate whistleblower process.

Question 6

An organization's information security strategic plan MUST be reviewed

- ☐ whenever there are significant changes to a major application.
- ☐ quarterly, when the organization's strategic plan is updated.
- ☒ whenever there are major changes to the business.
- ☐ every three years, when the organization's strategic plan is updated.

Question 7

Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

- ☒ Hashing the data before encryption
- ☐ Hashing the data after encryption
- ☐ Compressing the data after encryption
- ☐ Compressing the data before encryption

Question 8

Which of the following mobile code security models relies only on trust?

- ☒ Code signing
- ☐ Class authentication
- ☐ Sandboxing
- ☐ Type safety

Explanation:

Reference: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/t09.pdf> (11)

Question 9

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- ☐ Use a web scanner to scan for vulnerabilities within the website.
- ☐ Perform a code review to ensure that the database references are properly addressed.
- ☐ Establish a secure connection to the web server to validate that only the approved ports are open.
- ☒ Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Question 10

An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

- ☐ Implement packet filtering on the network firewalls
- ☐ Install Host Based Intrusion Detection Systems (HIDS)
- ☐ Require strong authentication for administrators
- ☒ Implement logical network segmentation at the switches

Question 11

Intellectual property rights are PRIMARY concerned with which of the following?

- ☐ Owner's ability to realize financial gain
- ☐ Owner's ability to maintain copyright
- ☐ Right of the owner to enjoy their creation
- ☒ Right of the owner to control delivery method

Question 12

What is an advantage of Elliptic Curve Cryptography (ECC)?

- ☐ Cryptographic approach that does not require a fixed-length key
- ☐ Military-strength security that does not depend upon secrecy of the algorithm
- ☒ Opportunity to use shorter keys for the same level of security
- ☐ Ability to use much longer keys for greater security

Question 13

Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

- ☐ Lightweight Directory Access Protocol (LDAP)
- ☒ Security Assertion Markup Language (SAML)
- ☐ Internet Mail Access Protocol
- ☐ Transport Layer Security (TLS)

Question 14

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

- ☐ Acoustic sensor
- ☐ Motion sensor
- ☒ Shock sensor
- ☐ Photoelectric sensor

Question 15

In which identity management process is the subject's identity established?

- ☐ Trust
- ☐ Provisioning
- ☐ Authorization
- ☒ Enrollment

Question 16

What does the Maximum Tolerable Downtime (MTD) determine?

- ☐ The estimated period of time a business critical database can remain down before customers are affected.
- ☐ The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
- ☒ The estimated period of time a business can remain interrupted beyond which it risks never recovering
- ☐ The fixed length of time in a DR process before redundant systems are engaged

Question 17

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

- ☒ Enterprise asset management framework
- ☐ Asset baseline using commercial off the shelf software
- ☐ Asset ownership database using domain login records
- ☐ A script to report active user logins on assets

Question 18

Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

- ☐ Senior management
- ☐ Information security department
- ☒ Audit committee
- ☐ All users

Question 19

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

- ☐ Examines log messages or other indications on the system.
- ☐ Monitors alarms sent to the system administrator
- ☒ Matches traffic patterns to virus signature files
- ☐ Examines the Access Control List (ACL)

Question 20

When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

- ☐ Into the options field
- ☒ Between the delivery header and payload
- ☐ Between the source and destination addresses
- ☐ Into the destination address

Question 21

Which of the following BEST represents the concept of least privilege?

- ☒ Access to an object is denied unless access is specifically allowed.
- ☐ Access to an object is only available to the owner.
- ☐ Access to an object is allowed unless it is protected by the information security policy.
- ☐ Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Question 22

Which of the following is MOST important when deploying digital certificates?

- ☐ Validate compliance with X.509 digital certificate standards
- ☒ Establish a certificate life cycle management framework
- ☐ Use a third-party Certificate Authority (CA)
- ☐ Use no less than 256-bit strength encryption when creating a certificate

Question 23

A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

- ☒ Administrator should request data owner approval to the user access
- ☐ Administrator should request manager approval for the user access
- ☐ Administrator should directly grant the access to the non-sensitive files
- ☐ Administrator should assess the user access need and either grant or deny the access

Question 24

What is the purpose of an Internet Protocol (IP) spoofing attack?

- ☐ To send excessive amounts of data to a process, making it unpredictable
- ☐ To intercept network traffic without authorization
- ☐ To disguise the destination address from a target's IP filtering devices
- ☒ To convince a system that it is communicating with a known entity

Question 25

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

- ☐ Notification tool
- ☐ Message queuing tool
- ☒ Security token tool
- ☐ Synchronization tool

Question 26

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

- ☐ Topology diagrams
- ☐ Mapping tools
- ☐ Asset register
- ☒ Ping testing

Question 27

Which of the following is a PRIMARY advantage of using a third-party identity service?

- ☐ Consolidation of multiple providers
- ☐ Directory synchronization
- ☐ Web based logon
- ☒ Automated account management

Question 28

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

- ☐ Reversal
- ☒ Gray box
- ☐ Blind
- ☐ White box

Question 29

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- ☒ Asset Management, Business Environment, Governance and Risk Assessment
- ☐ Access Control, Awareness and Training, Data Security and Maintenance
- ☐ Anomalies and Events, Security Continuous Monitoring and Detection Processes
- ☐ Recovery Planning, Improvements and Communications

Question 30

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

- ☐ Temporal Key Integrity Protocol (TKIP)
- ☒ Secure Hash Algorithm (SHA)
- ☐ Secure Shell (SSH)
- ☐ Transport Layer Security (TLS)

Question 31

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

- ☒ Add a new rule to the application layer firewall
- ☐ Block access to the service
- ☐ Install an Intrusion Detection System (IDS)
- ☐ Patch the application source code

Question 32

When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

- ☐ To force the software to fail and document the process
- ☐ To find areas of compromise in confidentiality and integrity
- ☒ To allow for objective pass or fail decisions
- ☐ To identify malware or hidden code within the test results

Question 33

What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

- ☐ Disable all unnecessary services
- ☐ Ensure chain of custody
- ☐ Prepare another backup of the system
- ☒ Isolate the system from the network

Question 34

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

- ☐ Provide vulnerability reports to management.
- ☒ Validate vulnerability remediation activities.
- ☐ Prevent attackers from discovering vulnerabilities.
- ☐ Remediate known vulnerabilities.

Question 35

Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

- ☐ clear-text attack.
- ☐ known cipher attack.
- ☒ frequency analysis.
- ☐ stochastic assessment.

Question 36

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

- ☐ Tactical, strategic, and financial
- ☒ Management, operational, and technical
- ☐ Documentation, observation, and manual
- ☐ Standards, policies, and procedures

Question 37

Backup information that is critical to the organization is identified through a

- ☐ Vulnerability Assessment (VA).
- ☐ Business Continuity Plan (BCP).
- ☐ Business Impact Analysis (BIA).
- ☒ data recovery analysis.

Question 38

Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

- ☐ VPN bandwidth
- ☒ Simultaneous connection to other networks
- ☐ Users with Internet Protocol (IP) addressing conflicts
- ☐ Remote users with administrative rights

Question 39

Which of the following BEST describes a chosen plaintext attack?

- ☒ The cryptanalyst can generate ciphertext from arbitrary text.
- ☐ The cryptanalyst examines the communication being sent back and forth.
- ☐ The cryptanalyst can choose the key and algorithm to mount the attack.
- ☐ The cryptanalyst is presented with the ciphertext from which the original message is determined.

Question 40

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

- ☐ Implementation Phase
- ☐ Initialization Phase
- ☐ Cancellation Phase
- ☒ Issued Phase

Question 41

Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

- ☐ Transference
- ☐ Covert channel
- ☐ Bleeding
- ☒ Cross-talk

Question 42

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

- ☐ Alert data
- ☐ User data
- ☐ Content data
- ☒ Statistical data

Question 43

When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

- ☒ Only when assets are clearly defined
- ☐ Only when standards are defined
- ☐ Only when controls are put in place
- ☐ Only procedures are defined

Question 44

Which of the following is needed to securely distribute symmetric cryptographic keys?

- ☐ Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
- ☐ Officially approved and compliant key management technology and processes
- ☒ An organizationally approved communication protection policy and key management plan
- ☐ Hardware tokens that protect the user's private key.

Question 45

Reciprocal backup site agreements are considered to be

- ☐ a better alternative than the use of warm sites.
- ☒ difficult to test for complex systems.
- ☐ easy to implement for similar types of organizations.
- ☐ easy to test and implement for complex systems.

Question 46

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

- ☐ Purchase software from a limited list of retailers
- ☐ Verify the hash key or certificate key of all updates
- ☐ Do not permit programs, patches, or updates from the Internet
- ☒ Test all new software in a segregated environment

Question 47

Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

- ☐ Common Vulnerabilities and Exposures (CVE)
- ☒ Common Vulnerability Scoring System (CVSS)
- ☐ Asset Reporting Format (ARF)
- ☐ Open Vulnerability and Assessment Language (OVAL)

Question 48

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

- ☒ SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
- ☐ SSL and TLS provide nonrepudiation by default.
- ☐ SSL and TLS do not provide security for most routed protocols.
- ☐ SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Question 49

In order to assure authenticity, which of the following are required?

- ☐ Confidentiality and authentication
- ☐ Confidentiality and integrity
- ☐ Authentication and non-repudiation
- ☒ Integrity and non-repudiation

Question 50

An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

- ☒ organization policy.
- ☐ industry best practices.
- ☐ industry laws and regulations.
- ☐ management feedback.

Question 51

Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

- ☐ Intrusion Prevention Systems (IPS)
- ☐ Intrusion Detection Systems (IDS)
- ☐ Stateful firewalls
- ☒ Network Behavior Analysis (NBA) tools

Question 52

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

- ☐ Link layer
- ☐ Physical layer
- ☐ Session layer
- ☒ Application layer

Question 53

When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

- ☐ After the system preliminary design has been developed and the data security categorization has been performed
- ☐ After the vulnerability analysis has been performed and before the system detailed design begins
- ☒ After the system preliminary design has been developed and before the data security categorization begins
- ☐ After the business functional analysis and the data security categorization have been performed

Question 54

Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

- ☒ Addresses and protocols of network-based logs are analyzed.
- ☐ Host-based system logging has files stored in multiple locations.
- ☐ Properly handled network-based logs may be more reliable and valid.
- ☐ Network-based systems cannot capture users logging into the console.

Question 55

Which of the following is the MOST important goal of information asset valuation?

- ☐ Developing a consistent and uniform method of controlling access on information assets
- ☐ Developing appropriate access control policies and guidelines
- ☐ Assigning a financial value to an organization's information assets
- ☒ Determining the appropriate level of protection

Question 56

Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

- ☐ To verify that only employees have access to the facility.
- ☐ To identify present hazards requiring remediation.
- ☐ To monitor staff movement throughout the facility.
- ☒ To provide a safe environment for employees.

Question 57

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

- ☐ Install mantraps at the building entrances
- ☐ Enclose the personnel entry area with polycarbonate plastic
- ☐ Supply a duress alarm for personnel exposed to the public
- ☒ Hire a guard to protect the public area

Question 58

Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

- ☐ The dynamic reconfiguration of systems
- ☐ The cost of downtime
- ☒ A recovery strategy for all business processes
- ☐ A containment strategy

Question 59

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

- ☒ Length of Initialization Vector (IV)
- ☐ Protection against message replay
- ☐ Detection of message tampering
- ☐ Built-in provision to rotate keys

Question 60

What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

- ☐ Radio Frequency (RF) attack
- ☒ Denial of Service (DoS) attack
- ☐ Data modification attack
- ☐ Application-layer attack

Question 61

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

- ☐ Guaranteed recovery of all business functions
- ☐ Minimization of the need decision making during a crisis
- ☐ Insurance against litigation following a disaster
- ☒ Protection from loss of organization resources

Question 62

In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

- ☒ Reduced risk to internal systems.
- ☐ Prepare the server for potential attacks.
- ☐ Mitigate the risk associated with the exposed server.
- ☐ Bypass the need for a firewall.

Question 63

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

- ☐ Take the computer to a forensic lab
- ☐ Make a copy of the hard drive
- ☒ Start documenting
- ☐ Turn off the computer

Question 64

Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

- ☐ Transport and Session
- ☒ Data-Link and Transport
- ☐ Network and Session
- ☐ Physical and Data-Link