



Reference Solution for CISSP.examcollection.premium.exam.289

q
CISSP

CISSP

Certified Information Systems Security Professional

Version 3.1

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (289 questions)

Question 1

Which of the following is considered best practice for preventing e-mail spoofing?

- ☒ Cryptographic signature
- ☐ Uniform Resource Locator (URL) filtering
- ☐ Spam filtering
- ☐ Reverse Domain Name Service (DNS) lookup

Question 2

What is the PRIMARY role of a scrum master in agile development?

- ☐ To choose the primary development language
- ☐ To choose the integrated development environment
- ☐ To match the software requirements to the delivery plan
- ☒ To project manage the software delivery

Question 3

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 4

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 5

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

- ☐ Job rotation
- ☒ Separation of duties
- ☐ Least privilege
- ☐ Mandatory vacations

Question 6

Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

- ☐ End-to-end data encryption for data in transit
- ☐ Continuous monitoring of potential vulnerabilities
- ☐ A strong breach notification process
- ☒ Limited collection of individuals' confidential data

Question 7

As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

- ☐ Data classification policy
- ☒ Software and hardware inventory
- ☐ Remediation recommendations
- ☐ Names of participants

Question 8

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 9

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

- ☐ require an update of the Protection Profile (PP).
- ☒ require recertification.
- ☐ retain its current EAL rating.
- ☐ reduce the product to EAL 3.

Question 10

DRAG DROP

Match the access control type to the example of the control type.

Drag each access control type net to its corresponding example.

<u>Access Control Type</u>		<u>Example</u>
Administrative		Labeling of sensitive data
Technical		Biometrics for authentication
Logical		Constrained user interface
Physical		Radio Frequency Identification (RFID) badge

Solution:

<u>Access Control Type</u>		<u>Example</u>
Administrative	Administrative	Labeling of sensitive data
Technical	Logical	Biometrics for authentication
Logical	Technical	Constrained user interface
Physical	Physical	Radio Frequency Identification (RFID) badge

Question 11

DRAG DROP

Match the functional roles in an external audit to their responsibilities.
Drag each role on the left to its corresponding responsibility on the right.

Role		Responsibility
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

Solution:

Role		Responsibility
Executive management	Executive management	Approve audit budget and resource allocation.
Audit committee	Audit committee	Provide audit oversight.
Compliance officer	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

Question 12

Which of the following **MUST** be part of a contract to support electronic discovery of data stored in a cloud environment?

- ☒ identification of data location
- ☐ integration with organizational directory services for authentication
- ☐ accommodation of hybrid deployment models
- ☐ tokenization of data

Question 13

Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

- ☐ Transport layer handshake compression
- ☐ Application layer negotiation
- ☒ Peer identity authentication
- ☐ Digital certificate revocation

Question 14

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 15

Which of the following represents the GREATEST risk to data confidentiality?

- ☐ Network redundancies are not implemented
- ☐ Security awareness training is not completed
- ☒ Backup tapes are generated unencrypted
- ☐ Users have administrative privileges

Question 16

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

- ☐ Countermeasure effectiveness
- ☐ Type of potential loss
- ☒ Incident likelihood
- ☐ Information ownership

Question 17

How does Encapsulating Security Payload (ESP) in transport mode affect in the Internet Protocol (IP)?

- ☐ Authenticates the IP payload and selected portions of the IP header
- ☐ Encrypts and optionally authenticates the complete IP packet
- ☐ Encrypts and optionally authenticates the IP header, but not the IP payload
- ☒ Encrypts and optionally authenticates the IP payload, but not the IP header

Question 18

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 19

Which of the following is a characteristic of an internal audit?

- ☐ An internal audit is typically shorter in duration than an external audit.
- ☐ The internal audit schedule is published to the organization well in advance.
- ☐ The internal auditor reports to the Information Technology (IT) department
- ☒ Management is responsible for reading and acting upon the internal audit results

Question 20

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 21

What does electronic vaulting accomplish?

- ☒ It protects critical files.
- ☐ It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
- ☐ It stripes all database records
- ☐ It automates the Disaster Recovery Process (DRP)

Question 22

Why is planning in Disaster Recovery (DR) an interactive process?

- ☐ It details off-site storage plans
- ☒ It identifies omissions in the plan
- ☐ It defines the objectives of the plan
- ☐ It forms part of the awareness process

Question 23

Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

- ☐ Mandatory Access Controls (MAC)
- ☐ Enterprise security architecture
- ☐ Enterprise security procedures
- ☒ Role Based Access Controls (RBAC)

Question 24

As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

- ☐ Known-plaintext attack
- ☐ Denial of Service (DoS)
- ☐ Cookie manipulation
- ☒ Structured Query Language (SQL) injection

Question 25

Which of the following mandates the amount and complexity of security controls applied to a security risk?

- ☐ Security vulnerabilities
- ☐ Risk tolerance
- ☒ Risk mitigation
- ☐ Security staff

Question 26

What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

- ☒ Warm site
- ☐ Hot site
- ☐ Mirror site
- ☐ Cold site

Question 27

Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

- ☒ Password requirements are simplified.
- ☐ Risk associated with orphan accounts is reduced.
- ☐ Segregation of duties is automatically enforced.
- ☐ Data confidentiality is increased.

Question 28

A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

- ☐ Transport
- ☐ Data link
- ☐ Network
- ☒ Application

Question 29

A chemical plant wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.

Which of the following is the GREATEST impact on security for the network?

- ☐ The network administrators have no knowledge of ICS
- ☒ The ICS is now accessible from the office network
- ☐ The ICS does not support the office password policy
- ☐ RS422 is more reliable than Ethernet

Question 30

Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

- ☒ System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
- ☐ Data stewardship roles, data handling and storage standards, data lifecycle requirements
- ☐ Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
- ☐ System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

Question 31

What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

- ☐ Information security practitioner
- ☒ Information librarian
- ☐ Computer operator
- ☐ Network administrator

Question 32

Which of the following could cause a Denial of Service (DoS) against an authentication system?

- ☐ Encryption of audit logs
- ☐ No archiving of audit logs
- ☐ Hashing of audit logs
- ☒ Remote access audit logs

Question 33

Which of the following MUST be in place to recognize a system attack?

- ☒ Stateful firewall
- ☐ Distributed antivirus
- ☐ Log analysis
- ☐ Passive honeypot

Question 34

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

- ☐ Walkthrough
- ☒ Simulation
- ☐ Parallel
- ☐ White box

Explanation:

Reference: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61029/Chapter-6-Business-Continuity-Management_amends_04042012.pdf

Question 35

In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

- ☐ systems integration.
- ☐ risk management.
- ☐ quality assurance.
- ☒ change management.

Question 36

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 37

Which of the following is the MAIN reason for using configuration management?

- ☐ To provide centralized administration
- ☐ To reduce the number of changes
- ☐ To reduce errors during upgrades
- ☒ To provide consistency in security controls

Question 38

A continuous information security monitoring program can BEST reduce risk through which of the following?

- ☐ Collecting security events and correlating them to identify anomalies
- ☒ Facilitating system-wide visibility into the activities of critical user accounts
- ☐ Encompassing people, process, and technology
- ☐ Logging both scheduled and unscheduled system changes

Question 39

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 40

Determining outage costs caused by a disaster can BEST be measured by the

- ☐ cost of redundant systems and backups.
- ☐ cost to recover from an outage.
- ☒ overall long-term impact of the outage.
- ☐ revenue lost during the outage.

Question 41

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 42

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 43

Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

- ☐ Delete every file on each drive.
- ☐ Destroy the partition table for each drive using the command line.
- ☐ Degauss each drive individually.
- ☒ Perform multiple passes on each drive using approved formatting methods.

Question 44

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 45

Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

- ☐ Biba
- ☐ Graham-Denning
- ☒ Clark-Wilson
- ☐ Beil-LaPadula

Question 46

During which of the following processes is least privilege implemented for a user account?

- ☒ Provision
- ☐ Approve
- ☐ Request
- ☐ Review

Question 47

What does a Synchronous (SYN) flood attack do?

- ☐ Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
- ☒ Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
- ☐ Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
- ☐ Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Question 48

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

- ☐ Check arguments in function calls
- ☒ Test for the security patch level of the environment
- ☐ Include logging functions
- ☐ Digitally sign each application module

Question 49

Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

- ☒ Change management processes
- ☐ User administration procedures
- ☐ Operating System (OS) baselines
- ☐ System backup documentation

Question 50

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

- ☐ Hardware and software compatibility issues
- ☐ Applications' critically and downtime tolerance
- ☐ Budget constraints and requirements
- ☒ Cost/benefit analysis and business objectives

Explanation:

Reference: <http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3>

Question 51

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 52

A vulnerability in which of the following components would be MOST difficult to detect?

- ☒ Kernel
- ☐ Shared libraries
- ☐ Hardware
- ☐ System application

Question 53

In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

- ☐ The second of two routers can periodically check in to make sure that the first router is operational.
- ☐ The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
- ☒ The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
- ☐ The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

Question 54

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 55

A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device.

Which of the following is MOST effective to mitigate future infections?

- ☐ Develop a written organizational policy prohibiting unauthorized USB devices
- ☐ Train users on the dangers of transferring data in USB devices
- ☒ Implement centralized technical control of USB port connections
- ☐ Encrypt removable USB devices containing data at rest

Question 56

What is the foundation of cryptographic functions?

- ☒ Encryption
- ☐ Cipher
- ☐ Hash
- ☐ Entropy

Question 57

Attack trees are MOST useful for which of the following?

- ☒ Determining system security scopes
- ☐ Generating attack libraries
- ☐ Enumerating threats
- ☐ Evaluating Denial of Service (DoS) attacks

Question 58

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 59

An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

- ☐ Absence of a Business Intelligence (BI) solution
- ☐ Inadequate cost modeling
- ☐ Improper deployment of the Service-Oriented Architecture (SOA)
- ☒ Insufficient Service Level Agreement (SLA)

Question 60

An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

- ☐ Ownership
- ☐ Confidentiality
- ☒ Availability
- ☐ Integrity

Question 61

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- ☒ annually
- ☐ to correspond with staff promotions
- ☐ to correspond with terminations
- ☐ continually

Question 62

Although code using a specific program language may not be susceptible to a buffer overflow attack,

- ☐ most calls to plug-in programs are susceptible.
- ☐ most supporting application code is susceptible.
- ☒ the graphical images used by the application could be susceptible.
- ☐ the supporting virtual machine could be susceptible.

Question 63

DRAG DROP

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

Solution:

<u>Actions</u>		<u>Steps</u>
Define the perimeter.	Identify the vulnerability.	Step 1
Identify the vulnerability.	Define the perimeter.	Step 2
Assess the risk.	Assess the risk.	Step 3
Determine the actions.	Determine the actions.	Step 4

Question 64

The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover.

Which access control mechanism would be preferred?

- ☐ Attribute Based Access Control (ABAC)
- ☐ Discretionary Access Control (DAC)
- ☐ Mandatory Access Control (MAC)
- ☒ Role-Based Access Control (RBAC)

Question 65

The core component of Role Based Access Control (RBAC) must be constructed of defined data elements.

Which elements are required?

- ☐ Users, permissions, operations, and protected objects
- ☐ Roles, accounts, permissions, and protected objects
- ☒ Users, roles, operations, and protected objects
- ☐ Roles, operations, accounts, and protected objects

Question 66

The goal of a Business Impact Analysis (BIA) is to determine which of the following?

- ☐ Cost effectiveness of business recovery
- ☐ Cost effectiveness of installing software security patches
- ☒ Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
- ☐ Which security measures should be implemented

Question 67

A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this happening again?

- ☐ Define additional security controls directly after the merger
- ☐ Include a procurement officer in the merger team
- ☐ Verify all contracts before a merger occurs
- ☒ Assign a compliance officer to review the merger conditions

Question 68

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

- ☒ Configuration
- ☐ Identity
- ☐ Compliance
- ☐ Patch

Question 69

Which of the following is the MOST efficient mechanism to account for all staff during a speedy non-emergency evacuation from a large security facility?

- ☐ Large mantrap where groups of individuals leaving are identified using facial recognition technology
- ☒ Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exit door
- ☐ Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
- ☐ Card-activated turnstile where individuals are validated upon exit

Question 70

In configuration management, what baseline configuration information MUST be maintained for each computer system?

- ☒ Operating system and version, patch level, applications running, and versions.
- ☐ List of system changes, test reports, and change approvals
- ☐ Last vulnerability assessment report and initial risk assessment report
- ☐ Date of last update, test report, and accreditation certificate

Question 71

A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

- ☒ Host VM monitor audit logs
- ☐ Guest OS access controls
- ☐ Host VM access controls
- ☐ Guest OS audit logs

Question 72

Access to which of the following is required to validate web session management?

- ☐ Log timestamp
- ☐ Live session traffic
- ☒ Session state variables
- ☐ Test scripts

Question 73

When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

- ☒ Implementation
- ☐ Initiation
- ☐ Review
- ☐ Development

Question 74

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

- ☐ Connect the device to another network jack
- ☒ Apply remediation's according to security requirements
- ☐ Apply Operating System (OS) patches
- ☐ Change the Message Authentication Code (MAC) address of the network interface

Question 75

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 76

Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

- ☒ Single Sign-On (SSO) authentication support
- ☐ Privileged user authentication support
- ☐ Password reset service support
- ☐ Terminal Access Controller Access Control System (TACACS) authentication support

Question 77

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

- ☒ dig
- ☐ ipconfig
- ☐ ifconfig
- ☐ nbstat

Question 78

Which of the following is the MOST important security goal when performing application interface testing?

- ☐ Confirm that all platforms are supported and function properly
- ☒ Evaluate whether systems or components pass data and control correctly to one another
- ☐ Verify compatibility of software, hardware, and network connections
- ☐ Examine error conditions related to external interfaces to prevent application details leakage

Question 79

Mandatory Access Controls (MAC) are based on:

- ☒ security classification and security clearance
- ☐ data segmentation and data classification
- ☐ data labels and user access permissions
- ☐ user roles and data encryption

Question 80

What is the PRIMARY reason for implementing change management?

- ☐ Certify and approve releases to the environment
- ☐ Provide version rollbacks for system changes
- ☐ Ensure that all applications are approved
- ☒ Ensure accountability for changes to the environment

Question 81

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 82

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 83

Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

- ☒ Application proxy
- ☐ Port filter
- ☐ Network boundary router
- ☐ Access layer switch

Question 84

Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

- ☐ Security governance
- ☒ Risk management
- ☐ Security portfolio management
- ☐ Risk assessment

Question 85

Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

- ☒ Derived credential
- ☐ Temporary security credential
- ☐ Mobile device credentialing service
- ☐ Digest authentication

Question 86

Which of the following is the MOST common method of memory protection?

- ☐ Compartmentalization
- ☒ Segmentation
- ☐ Error correction
- ☐ Virtual Local Area Network (VLAN) tagging

Question 87

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

- ☐ Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
- ☒ Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- ☐ Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
- ☐ Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Question 88

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 89

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 90

During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

- ☒ Calculate the value of assets being accredited.
- ☐ Create a list to include in the Security Assessment and Authorization package.
- ☐ Identify obsolete hardware and software.
- ☐ Define the boundaries of the information system.

Question 91

Which of the following would BEST describe the role directly responsible for data within an organization?

- ☒ Data custodian
- ☐ Information owner
- ☐ Database administrator
- ☐ Quality control

Question 92

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

- ☐ Personal Identity Verification (PIV)
- ☐ Cardholder Unique Identifier (CHUID) authentication
- ☒ Physical Access Control System (PACS) repeated attempt detection
- ☐ Asymmetric Card Authentication Key (CAK) challenge-response

Question 93

Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

- ☐ Low-level formatting
- ☒ Secure-grade overwrite erasure
- ☐ Cryptographic erasure
- ☐ Drive degaussing

Question 94

DRAG DROP

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

<u>Access Control Model</u>		<u>Restrictions</u>
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

Solution:

<u>Access Control Model</u>		<u>Restrictions</u>
Mandatory Access Control	Mandatory Access Control	End user cannot set controls
Discretionary Access Control (DAC)	Discretionary Access Control (DAC)	Subject has total control over objects
Role Based Access Control (RBAC)	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
Rule based access control	Rule based access control	Dynamically assigns roles to subjects based on criteria assigned by a custodian

Question 95

Which of the following are effective countermeasures against passive network-layer attacks?

- ☐ Federated security and authenticated access controls
- ☐ Trusted software development and run time integrity controls
- ☒ Encryption and security enabled applications
- ☐ Enclave boundary protection and computing environment defense

Question 96

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

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

Question 97

What is the term commonly used to refer to a technique of authentication one machine to another by forging packets from a trusted source?

- ☐ Smurfing
- ☐ Man-in-the-Middle (MITM) attack
- ☐ Session redirect
- ☒ Spoofing

Question 98

Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

- ☐ Integration using Lightweight Directory Access Protocol (LDAP)
- ☐ Form-based user registration process
- ☐ Integration with the organizations Human Resources (HR) system
- ☒ A considerably simpler provisioning process

Question 99

Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

- ☐ Inert gas fire suppression system
- ☐ Halon gas fire suppression system
- ☒ Dry-pipe sprinklers
- ☐ Wet-pipe sprinklers

Question 100

Which of the following is a remote access protocol that uses a static authentication?

- ☐ Point-to-Point Tunneling Protocol (PPTP)
- ☐ Routing Information Protocol (RIP)
- ☒ Password Authentication Protocol (PAP)
- ☐ Challenge Handshake Authentication Protocol (CHAP)

Question 101

Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

- ☐ Having emergency contacts established for the general employee population to get information
- ☐ Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
- ☒ Designing business continuity and disaster recovery training programs for different audiences
- ☐ Publishing a corporate business continuity and disaster recovery plan on the corporate website

Question 102

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 103

From a security perspective, which of the following assumptions MUST be made about input to an application?

- ☐ It is tested
- ☐ It is logged
- ☐ It is verified
- ☒ It is untrusted

Question 104

Which of the following is a responsibility of the information owner?

- ☐ Ensure that users and personnel complete the required security training to access the Information System (IS)
- ☐ Defining proper access to the Information System (IS), including privileges or access rights
- ☒ Managing identification, implementation, and assessment of common security controls
- ☐ Ensuring the Information System (IS) is operated according to agreed upon security requirements

Question 105

Which of the following is a responsibility of a data steward?

- ☒ Ensure alignment of the data governance effort to the organization.
- ☐ Conduct data governance interviews with the organization.
- ☐ Document data governance requirements.
- ☐ Ensure that data decisions and impacts are communicated to the organization.

Question 106

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 107

The PRIMARY outcome of a certification process is that it provides documented

- ☐ interconnected systems and their implemented security controls.
- ☐ standards for security assessment, testing, and process evaluation.
- ☐ system weakness for remediation.
- ☒ security analyses needed to make a risk-based decision.

Question 108

Which one of the following data integrity models assumes a lattice of integrity levels?

- ☐ Take-Grant
- ☒ Biba
- ☐ Harrison-Ruzzo
- ☐ Bell-LaPadula

Question 109

Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

- ☐ It must be known to both sender and receiver.
- ☒ It can be transmitted in the clear as a random number.
- ☐ It must be retained until the last block is transmitted.
- ☐ It can be used to encrypt and decrypt information.

Question 110

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

- ☐ Application connection successes resulting in data leakage
- ☐ Administrative costs for restoring systems after connection failure
- ☐ Employee system timeouts from implementing wrong limits
- ☒ Help desk costs required to support password reset requests

Question 111

Which of the following would an attacker BEST be able to accomplish through the use of Remote Access Tools (RAT)?

- ☐ Reduce the probability of identification
- ☐ Detect further compromise of the target
- ☐ Destabilize the operation of the host
- ☒ Maintain and expand control

Question 112

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

- ☐ Mutual authentication
- ☐ Server authentication
- ☒ User authentication
- ☐ Streaming ciphertext data

Question 113

Which of the BEST internationally recognized standard for evaluating security products and systems?

- ☐ Payment Card Industry Data Security Standards (PCI-DSS)
- ☒ Common Criteria (CC)
- ☐ Health Insurance Portability and Accountability Act (HIPAA)
- ☐ Sarbanes-Oxley (SOX)

Question 114

In a data classification scheme, the data is owned by the

- ☐ system security managers
- ☒ business managers
- ☐ Information Technology (IT) managers
- ☐ end users

Question 115

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 116

Proven application security principles include which of the following?

- ☒ Minimizing attack surface area
- ☐ Hardening the network perimeter
- ☐ Accepting infrastructure security controls
- ☐ Developing independent modules

Question 117

An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.

Which contract is BEST in offloading the task from the IT staff?

- ☐ Platform as a Service (PaaS)
- ☒ Identity as a Service (IDaaS)
- ☐ Desktop as a Service (DaaS)
- ☐ Software as a Service (SaaS)

Question 118

What are the steps of a risk assessment?

- ☒ identification, analysis, evaluation
- ☐ analysis, evaluation, mitigation
- ☐ classification, identification, risk management
- ☐ identification, evaluation, mitigation

Question 119

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 120

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

- ☐ Perform a compliance review
- ☒ Perform a penetration test
- ☐ Train the technical staff
- ☐ Survey the technical staff

Question 121

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- ☐ Systems owner
- ☐ Authorizing Official (AO)
- ☒ Information owner
- ☐ Security officer

Question 122

DRAG DROP

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

<u>E-Authentication Token</u>		<u>Description</u>
Memorized Secret Token		A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token		A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
Look-up Secret Token		A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token		A secret shared between the subscriber and credential service provider that is typically character strings

Solution:

<u>E-Authentication Token</u>		<u>Description</u>
Memorized Secret Token	Look-up Secret Token	A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token	Out-of-Band Token	A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
Look-up Secret Token	Pre-registered Knowledge Token	A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token	Memorized Secret Token	A secret shared between the subscriber and credential service provider that is typically character strings

Question 123

Which of the following is a direct monetary cost of a security incident?

- ☐ Morale
- ☐ Reputation
- ☒ Equipment
- ☐ Information

Question 124

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

- ☐ Transport Layer
- ☐ Data-Link Layer
- ☒ Network Layer
- ☐ Application Layer

Question 125

When building a data classification scheme, which of the following is the PRIMARY concern?

- ☐ Purpose
- ☐ Cost effectiveness
- ☐ Availability
- ☒ Authenticity

Question 126

DRAG DROP

Drag the following Security Engineering terms on the left to the BEST definition on the right.

<u>Security Engineering Term</u>		<u>Definition</u>
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

Solution:

<u>Security Engineering Term</u>		<u>Definition</u>
Risk	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	Protection Needs Assessment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	Threat Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	Security Risk Treatment	The method used to identify feasible security risk mitigation options and plans.

Question 127

From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

- ☐ Disable all recursive queries on the name servers
- ☒ Limit zone transfers to authorized devices
- ☐ Configure secondary servers to use the primary server as a zone forwarder
- ☐ Block all Transmission Control Protocol (TCP) connections

Question 128

Which of the following is the FIRST step in the incident response process?

- ☐ Determine the cause of the incident
- ☐ Disconnect the system involved from the network
- ☐ Isolate and contain the system involved
- ☒ Investigate all symptoms to confirm the incident

Question 129

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

- ☒ Packet filtering
- ☐ Port services filtering
- ☐ Content filtering
- ☐ Application access control

Explanation:

Reference: <https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309> (10)

Question 130

Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

- ☐ Use Software as a Service (SaaS)
- ☒ Whitelist input validation
- ☐ Require client certificates
- ☐ Validate data output

Question 131

When implementing a data classification program, why is it important to avoid too much granularity?

- ☒ The process will require too many resources
- ☐ It will be difficult to apply to both hardware and software
- ☐ It will be difficult to assign ownership to the data
- ☐ The process will be perceived as having value

Explanation:

Reference: <http://www.ittoday.info/AIMS/DSM/82-02-55.pdf>

Question 132

Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

- ☒ User awareness
- ☐ Two-factor authentication
- ☐ Anti-phishing software
- ☐ Periodic vulnerability scan

Question 133

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

- ☐ Ensures that a trace for all deliverables is maintained and auditable
- ☐ Enforces backward compatibility between releases
- ☒ Ensures that there is no loss of functionality between releases
- ☐ Allows for future enhancements to existing features

Question 134

A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.

Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

- ☐ Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
- ☐ Gratuitous ARP requires the use of insecure layer 3 protocols.
- ☐ Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
- ☒ Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Question 135

Which security service is served by the process of encryption plaintext with the sender's private key and decrypting cipher text with the sender's public key?

- ☒ Confidentiality
- ☐ Integrity
- ☐ Identification
- ☐ Availability

Question 136

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.

Which of the following is LEAST associated with the attack surface?

- ☐ Input protocols
- ☐ Target processes
- ☒ Error messages
- ☐ Access rights

Question 137

How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

- ☐ Use an impact-based approach.
- ☒ Use a risk-based approach.
- ☐ Use a criticality-based approach.
- ☐ Use a threat-based approach.

Question 138

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.

In which phase of the assessment was this error MOST likely made?

- ☒ Enumeration
- ☐ Reporting
- ☐ Detection
- ☐ Discovery

Question 139

An organization plan on purchasing a custom software product developed by a small vendor to support its business model.

Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

- ☐ A source code escrow clause
- ☒ Right to request an independent review of the software source code
- ☐ Due diligence form requesting statements of compliance with security requirements
- ☐ Access to the technical documentation

Question 140

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

- ☐ Erase
- ☒ Sanitize
- ☐ Encrypt
- ☐ Degauss

Question 141

Which of the following BEST describes Recovery Time Objective (RTO)?

- ☒ Time of application resumption after disaster
- ☐ Time of application verification after disaster.
- ☐ Time of data validation after disaster.
- ☐ Time of data restoration from backup after disaster.

Question 142

In The Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

- ☒ Physical Layer
- ☐ Application Layer
- ☐ Data-Link Layer
- ☐ Network Layer

Question 143

Which one of the following considerations has the LEAST impact when considering transmission security?

- ☐ Network availability
- ☐ Node locations
- ☒ Network bandwidth
- ☐ Data integrity

Question 144

Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

- ☐ Memory review
- ☒ Code review
- ☐ Message division
- ☐ Buffer division

Question 145

Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

- ☒ Standardized configurations for devices
- ☐ Standardized patch testing equipment
- ☐ Automated system patching
- ☐ Management support for patching

Question 146

What protocol is often used between gateway hosts on the Internet?

- ☐ Exterior Gateway Protocol (EGP)
- ☒ Border Gateway Protocol (BGP)
- ☐ Open Shortest Path First (OSPF)
- ☐ Internet Control Message Protocol (ICMP)

Question 147

Which type of test would an organization perform in order to locate and target exploitable defects?

- ☒ Penetration
- ☐ System
- ☐ Performance
- ☐ Vulnerability

Question 148

What is the expected outcome of security awareness in support of a security awareness program?

- ☐ Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
- ☐ Awareness is not an activity or part of the training but rather a state of persistence to support the program
- ☒ Awareness is training. The purpose of awareness presentations is to broaden attention of security.
- ☐ Awareness is not training. The purpose of awareness presentation is simply to focus attention on security.

Question 149

A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

- ☐ Application
- ☐ Storage
- ☒ Power
- ☐ Network

Explanation:

Reference: <https://www.colocationamerica.com/data-center/tier-standards-overview.htm>

Question 150

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 151

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

- ☐ Audit logs
- ☒ Role-Based Access Control (RBAC)
- ☐ Two-factor authentication
- ☐ Application of least privilege

Question 152

An organization regularly conducts its own penetration tests. Which of the following scenarios **MUST** be covered for the test to be effective?

- ☐ Third-party vendor with access to the system
- ☐ System administrator access compromised
- ☒ Internal attacker with access to the system
- ☐ Internal user accidentally accessing data

Question 153

When developing a business case for updating a security program, the security program owner **MUST** do which of the following?

- ☒ Identify relevant metrics
- ☐ Prepare performance test reports
- ☐ Obtain resources for the security program
- ☐ Interview executive management

Question 154

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 155

Which of the following is a common characteristic of privacy?

- ☒ Provision for maintaining an audit trail of access to the private data
- ☐ Notice to the subject of the existence of a database containing relevant credit card data
- ☐ Process for the subject to inspect and correct personal data on-site
- ☐ Database requirements for integration of privacy data

Question 156

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

- ☐ Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point
- ☐ Disable the broadcast of the Service Set Identifier (SSID) name
- ☐ Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization
- ☒ Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

Question 157

Unused space in a disk cluster is important in media analysis because it may contain which of the following?

- ☒ Residual data that has not been overwritten
- ☐ Hidden viruses and Trojan horses
- ☐ Information about the File Allocation table (FAT)
- ☐ Information about patches and upgrades to the system

Question 158

A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

- ☐ Send the log file co-workers for peer review
- ☐ Include the full network traffic logs in the incident report
- ☒ Follow organizational processes to alert the proper teams to address the issue.
- ☐ Ignore data as it is outside the scope of the investigation and the analyst's role.

Question 159

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 160

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

- ☒ Data tokenization
- ☐ Volume encryption
- ☐ Transparent Data Encryption (TDE)
- ☐ Column level database encryption

Question 161

What capability would typically be included in a commercially available software package designed for access control?

- ☒ Password encryption
- ☐ File encryption
- ☐ Source library control
- ☐ File authentication

Question 162

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 163

An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

- ☒ Discretionary Access Control (DAC)
- ☐ Role Based Access Control (RBAC)
- ☐ Media Access Control (MAC)
- ☐ Mandatory Access Control (MAC)

Question 164

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

- ☐ Service Level Agreement (SLA)
- ☒ Business Continuity Plan (BCP)
- ☐ Business Impact Analysis (BIA)
- ☐ Crisis management plan

Question 165

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 166

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

Question 167

During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):

`http://www.companysite.com/products/products.asp?productid=123 or 1=1`

What type of attack does this indicate?

- ☐ Directory traversal
- ☐ Structured Query Language (SQL) injection
- ☒ Cross-Site Scripting (XSS)
- ☐ Shellcode injection

Question 168

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 169

Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

- ☐ Minimize malicious attacks from third parties
- ☐ Manage resource privileges
- ☐ Share digital identities in hybrid cloud
- ☒ Defined a standard protocol

Question 170

Which of the following is MOST appropriate for protecting confidentiality of data stored on a hard drive?

- ☐ Triple Data Encryption Standard (3DES)
- ☒ Advanced Encryption Standard (AES)
- ☐ Message Digest 5 (MD5)
- ☐ Secure Hash Algorithm 2(SHA-2)

Question 171

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.

What step would be taken to ensure that the upgrade did NOT affect the network security posture?

- ☐ Conduct an Assessment and Authorization (A&A)
- ☒ Conduct a security impact analysis
- ☐ Review the results of the most recent vulnerability scan
- ☐ Conduct a gap analysis with the baseline configuration

Question 172

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 173

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.

What code of ethics canon is being observed?

- ☐ Provide diligent and competent service to principals
- ☐ Protect society, the commonwealth, and the infrastructure
- ☒ Advance and protect the profession
- ☐ Act honorable, honesty, justly, responsibly, and legally

Question 174

Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

- ☐ Implement processes for automated removal of access for terminated employees.
- ☒ Delete employee network and system IDs upon termination.
- ☐ Manually remove terminated employee user-access to all systems and applications.
- ☐ Disable terminated employee network ID to remove all access.

Question 175

In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

- ☐ a functional evacuation of personnel
- ☐ a specific test by response teams of individual emergency response functions
- ☐ an activation of the backup site
- ☒ a full-scale simulation of an emergency and the subsequent response functions.

Question 176

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 177

"Stateful" differs from "Static" packet filtering firewalls by being aware of which of the following?

- ☒ Difference between a new and an established connection
- ☐ Originating network location
- ☐ Difference between a malicious and a benign packet payload
- ☐ Originating application session

Question 178

Due to system constraints, a group of system administrators must share a high-level access set of credentials.

Which of the following would be MOST appropriate to implement?

- ☐ Increased console lockout times for failed logon attempts
- ☐ Reduce the group in size
- ☒ A credential check-out process for a per-use basis
- ☐ Full logging on affected systems

Question 179

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 180

Which of the following is the PRIMARY benefit of a formalized information classification program?

- ☐ It minimized system logging requirements.
- ☒ It supports risk assessment.
- ☐ It reduces asset vulnerabilities.
- ☐ It drives audit processes.

Question 181

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 182

A minimal implementation of endpoint security includes which of the following?

- ☒ Trusted platforms
- ☐ Host-based firewalls
- ☐ Token-based authentication
- ☐ Wireless Access Points (AP)

Question 183

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 184

What is the difference between media marking and media labeling?

- ☐ Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
- ☐ Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
- ☐ Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
- ☒ Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Question 185

Who is accountable for the information within an Information System (IS)?

- ☐ Security manager
- ☒ System owner
- ☐ Data owner
- ☐ Data processor

Question 186

Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

- ☐ Logging and audit trail controls to enable forensic analysis
- ☐ Security incident response lessons learned procedures
- ☒ Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
- ☐ Transactional controls focused on fraud prevention

Question 187

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 188

What is the BEST approach to addressing security issues in legacy web applications?

- ☐ Debug the security issues
- ☐ Migrate to newer, supported applications where possible
- ☐ Conduct a security assessment
- ☒ Protect the legacy application with a web application firewall

Question 189

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

- ☐ Application authentication
- ☐ Input validation
- ☒ Digital signing
- ☐ Device encryption

Question 190

Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

- ☐ undergo a security assessment as part of authorization process
- ☐ establish a risk management strategy
- ☐ harden the hosting server, and perform hosting and application vulnerability scans
- ☒ establish policies and procedures on system and services acquisition

Question 191

Which of the following is the BEST reason for the use of security metrics?

- ☐ They ensure that the organization meets its security objectives.
- ☒ They provide an appropriate framework for Information Technology (IT) governance.
- ☐ They speed up the process of quantitative risk assessment.
- ☐ They quantify the effectiveness of security processes.

Question 192

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

- ☐ determine the risk of a business interruption occurring
- ☒ determine the technological dependence of the business processes
- ☐ Identify the operational impacts of a business interruption
- ☐ Identify the financial impacts of a business interruption

Explanation:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKewjbktbTp-LaAhVlr48KHZuhBOUQFggmMAA&url=http%3A%2F%2Fwww.oregon.gov%2Fdas%2FProcurement%2FGuiddoc%2FBusImpAnalysQs.doc&usg=AOvVaw1wBxcnLP8ceI_yhv2rsI9h

Question 193

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 194

What is the BEST way to encrypt web application communications?

- ☐ Secure Hash Algorithm 1 (SHA-1)
- ☐ Secure Sockets Layer (SSL)
- ☐ Cipher Block Chaining Message Authentication Code (CBC-MAC)
- ☒ Transport Layer Security (TLS)

Question 195

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

- ☒ Mandatory Access Control (MAC)
- ☐ Access Control List (ACL)
- ☐ Discretionary Access Control (DAC)
- ☐ Authorized user control

Question 196

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

- ☐ Ensure the fire prevention and detection systems are sufficient to protect personnel
- ☐ Review the architectural plans to determine how many emergency exits are present
- ☒ Conduct a gap analysis of a new facilities against existing security requirements
- ☐ Revise the Disaster Recovery and Business Continuity (DR/BC) plan

Question 197

Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

- ☐ Property book
- ☐ Chain of custody form
- ☐ Search warrant return
- ☒ Evidence tag

Question 198

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 199

Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

- ☐ Lack of software documentation
- ☐ License agreements requiring release of modified code
- ☐ Expiration of the license agreement
- ☒ Costs associated with support of the software

Question 200

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 201

Which of the following is the BEST reason for writing an information security policy?

- ☒ To support information security governance
- ☐ To reduce the number of audit findings
- ☐ To deter attackers
- ☐ To implement effective information security controls

Question 202

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

- ☒ Diffie-Hellman (DH) algorithm
- ☐ Elliptic Curve Cryptography (ECC) algorithm
- ☐ Digital Signature algorithm (DSA)
- ☐ Rivest-Shamir-Adleman (RSA) algorithm

Question 203

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 204

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 205

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

- ☐ Development, testing, and deployment
- ☐ Prevention, detection, and remediation
- ☒ People, technology, and operations
- ☐ Certification, accreditation, and monitoring

Explanation:

Reference: <https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165> (14)

Question 206

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?

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

Question 207

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 208

Which of the following is an initial consideration when developing an information security management system?

- ☐ Identify the contractual security obligations that apply to the organizations
- ☒ Understand the value of the information assets
- ☐ Identify the level of residual risk that is tolerable to management
- ☐ Identify relevant legislative and regulatory compliance requirements

Question 209

Which one of the following affects the classification of data?

- ☐ Assigned security label
- ☐ Multilevel Security (MLS) architecture
- ☐ Minimum query size
- ☒ Passage of time

Question 210

The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

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

Question 211

A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

- ☐ Trusted third-party certification
- ☐ Lightweight Directory Access Protocol (LDAP)
- ☒ Security Assertion Markup language (SAML)
- ☐ Cross-certification

Explanation:

Reference: <https://www.netiq.com/documentation/access-manager-43/applications-configuration-guide/data/b1ka6lkd.html>

Question 212

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- ☐ Revoke access temporarily.
- ☐ Block user access and delete user account after six months.
- ☐ Block access to the offices immediately.
- ☒ Monitor account usage temporarily.

Question 213

What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

- ☒ The IDS can detect failed administrator logon attempts from servers.
- ☐ The IDS can increase the number of packets to analyze.
- ☐ The firewall can increase the number of packets to analyze.
- ☐ The firewall can detect failed administrator login attempts from servers

Question 214

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 215

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 216

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 217

An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

- ☒ Denial of Service (DoS) attack
- ☐ Address Resolution Protocol (ARP) spoof
- ☐ Buffer overflow
- ☐ Ping flood attack

Question 218

Digital certificates used in Transport Layer Security (TLS) support which of the following?

- ☐ Information input validation
- ☐ Non-repudiation controls and data encryption
- ☐ Multi-Factor Authentication (MFA)
- ☒ Server identity and data confidentiality

Question 219

Which of the following is the MOST challenging issue in apprehending cyber criminals?

- ☐ They often use sophisticated method to commit a crime.
- ☐ It is often hard to collect and maintain integrity of digital evidence.
- ☒ The crime is often committed from a different jurisdiction.
- ☐ There is often no physical evidence involved.

Question 220

Who in the organization is accountable for classification of data information assets?

- ☒ Data owner
- ☐ Data architect
- ☐ Chief Information Security Officer (CISO)
- ☐ Chief Information Officer (CIO)

Question 221

Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

- ☒ identity provisioning
- ☐ access recovery
- ☐ multi-factor authentication (MFA)
- ☐ user access review

Question 222

The PRIMARY purpose of accreditation is to:

- ☐ comply with applicable laws and regulations.
- ☒ allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- ☐ protect an organization's sensitive data.
- ☐ verify that all security controls have been implemented properly and are operating in the correct manner.

Question 223

A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

- ☒ Put the device in airplane mode
- ☐ Suspend the account with the telecommunication provider
- ☐ Remove the SIM card
- ☐ Turn the device off

Question 224

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 225

Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

- ☒ Truncating parts of the data
- ☐ Applying Access Control Lists (ACL) to the data
- ☐ Appending non-watermarked data to watermarked data
- ☐ Storing the data in a database

Question 226

The MAIN use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

- ☐ through a firewall at the Session layer
- ☐ through a firewall at the Transport layer
- ☒ in the Point-to-Point Protocol (PPP)
- ☐ in the Payload Compression Protocol (PCP)

Question 227

What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

- ☒ Non-repudiation
- ☐ Efficiency
- ☐ Confidentiality
- ☐ Privacy

Question 228

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 229

What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

- ☒ Risk versus benefit
- ☐ Availability versus auditability
- ☐ Confidentiality versus integrity
- ☐ Performance versus user satisfaction

Question 230

Which of the following BEST describes the responsibilities of a data owner?

- ☐ Ensuring quality and validation through periodic audits for ongoing data integrity
- ☐ Maintaining fundamental data availability, including data storage and archiving
- ☒ Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
- ☐ Determining the impact the information has on the mission of the organization

Explanation:

Reference: <http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/data-and-system-ownership/#gref>

Question 231

What is the MAIN goal of information security awareness and training?

- ☐ To inform users of the latest malware threats
- ☒ To inform users of information assurance responsibilities
- ☐ To comply with the organization information security policy
- ☐ To prepare students for certification

Question 232

What MUST each information owner do when a system contains data from multiple information owners?

- ☐ Provide input to the Information System (IS) owner regarding the security requirements of the data
- ☐ Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.
- ☒ Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
- ☐ Move the data to an Information System (IS) that does not contain data owned by other information owners

Question 233

What is the second step in the identity and access provisioning lifecycle?

- ☐ Provisioning
- ☒ Review
- ☐ Approval
- ☐ Revocation

Question 234

When is a Business Continuity Plan (BCP) considered to be valid?

- ☐ When it has been validated by the Business Continuity (BC) manager
- ☐ When it has been validated by the board of directors
- ☐ When it has been validated by all threat scenarios
- ☒ When it has been validated by realistic exercises

Explanation:

Reference:

http://www.manchester.gov.uk/info/200039/emergencies/6174/business_continuity_planning/5

Question 235

Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

- ☒ Automated dynamic analysis
- ☐ Automated static analysis
- ☐ Manual code review
- ☐ Fuzzing

Question 236

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- ☒ 25%
- ☐ 50%
- ☐ 75%
- ☐ 100%

Question 237

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 238

Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

- ☒ Code quality, security, and origin
- ☐ Architecture, hardware, and firmware
- ☐ Data quality, provenance, and scaling
- ☐ Distributed, agile, and bench testing

Question 239

An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

- ☐ The Data Protection Authority (DPA)
- ☒ The Cloud Service Provider (CSP)
- ☐ The application developers
- ☐ The data owner

Question 240

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 241

What is the PRIMARY goal of fault tolerance?

- ☒ Elimination of single point of failure
- ☐ Isolation using a sandbox
- ☐ Single point of repair
- ☐ Containment to prevent propagation

Question 242

Which of the following is part of a Trusted Platform Module (TPM)?

- ☒ A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
- ☐ A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for “measuring” the state of a computing platform
- ☐ A secure processor targeted at managing digital keys and accelerating digital signing
- ☐ A platform-independent software interface for accessing computer functions

Question 243

What is the MAIN purpose of a change management policy?

- ☐ To assure management that changes to the Information Technology (IT) infrastructure are necessary
- ☐ To identify the changes that may be made to the Information Technology (IT) infrastructure
- ☒ To verify that changes to the Information Technology (IT) infrastructure are approved
- ☐ To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

Question 244

A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

- ☐ Deploying load balancers to distribute inbound traffic across multiple data centers
- ☐ Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
- ☐ Implementing reverse web-proxies to validate each new inbound connection
- ☒ Coordinate with and utilize capabilities within Internet Service Provider (ISP)

Question 245

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

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

Question 246

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).

Which of the following represents a valid measure to help protect the network against unauthorized access?

- ☐ Implement path management
- ☒ Implement port based security through 802.1x
- ☐ Implement DHCP to assign IP address to server systems
- ☐ Implement change management

Question 247

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 248

Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

- ☐ Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
- ☐ Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
- ☐ Management teams will understand the testing objectives and reputational risk to the organization
- ☒ Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

Question 249

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

- ☐ Confidentiality
- ☐ Integrity
- ☒ Availability
- ☐ Accessibility

Question 250

What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

- ☐ To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
- ☒ To validate backup sites' effectiveness
- ☐ To find out what does not work and fix it
- ☐ To create a high level DRP awareness among Information Technology (IT) staff

Question 251

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

- ☒ Least privilege
- ☐ Privilege escalation
- ☐ Defense in depth
- ☐ Privilege bracketing

Question 252

From a cryptographic perspective, the service of non-repudiation includes which of the following features?

- ☐ Validity of digital certificates
- ☐ Validity of the authorization rules
- ☒ Proof of authenticity of the message
- ☐ Proof of integrity of the message

Question 253

When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

- ☐ Accept the risk on behalf of the organization.
- ☐ Report findings to the business to determine security gaps.
- ☒ Quantify the risk to the business for product selection.
- ☐ Approve the application that best meets security requirements.

Question 254

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

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

Question 255

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

- ☒ Mandatory Access Control (MAC) procedures
- ☐ Discretionary Access Control (DAC) procedures
- ☐ Segregation of duties
- ☐ Data link encryption

Question 256

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 257

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 258

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 259

The use of private and public encryption keys is fundamental in the implementation of which of the following?

- ☒ Diffie-Hellman algorithm
- ☐ Secure Sockets Layer (SSL)
- ☐ Advanced Encryption Standard (AES)
- ☐ Message Digest 5 (MD5)

Question 260

Which of the following is MOST important when assigning ownership of an asset to a department?

- ☐ The department should report to the business owner
- ☒ Ownership of the asset should be periodically reviewed
- ☐ Individual accountability should be ensured
- ☐ All members should be trained on their responsibilities

Question 261

It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

- ☒ Negotiate schedule with the Information Technology (IT) operation's team
- ☐ Log vulnerability summary reports to a secured server
- ☐ Enable scanning during off-peak hours
- ☐ Establish access for Information Technology (IT) management

Question 262

Who would be the BEST person to approve an organizations information security policy?

- ☐ Chief Information Officer (CIO)
- ☒ Chief Information Security Officer (CISO)
- ☐ Chief internal auditor
- ☐ Chief Executive Officer (CEO)

Question 263

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

- ☐ Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
- ☒ Maintaining segregation of duties.
- ☐ Standardized configurations for logging, alerting, and security metrics.
- ☐ Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

Question 264

Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

- ☐ parameterized database queries
- ☐ whitelist input values
- ☒ synchronized session tokens
- ☐ use strong ciphers

Question 265

An organization has discovered that users are visiting unauthorized websites using anonymous proxies.

Which of the following is the BEST way to prevent future occurrences?

- ☐ Remove the anonymity from the proxy
- ☐ Analyze Internet Protocol (IP) traffic for proxy requests
- ☒ Disable the proxy server on the firewall
- ☐ Block the Internet Protocol (IP) address of known anonymous proxies

Question 266

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

- ☐ Layer 2 Tunneling Protocol (L2TP)
- ☒ Link Control Protocol (LCP)
- ☐ Challenge Handshake Authentication Protocol (CHAP)
- ☐ Packet Transfer Protocol (PTP)

Question 267

In which of the following programs is it MOST important to include the collection of security process data?

- ☒ Quarterly access reviews
- ☐ Security continuous monitoring
- ☐ Business continuity testing
- ☐ Annual security training

Question 268

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

- ☐ Log all activities associated with sensitive systems
- ☐ Provide links to security policies
- ☐ Confirm that confidentiality agreements are signed
- ☒ Employ strong access controls

Question 269

Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

- ☐ Mandating security policy acceptance
- ☐ Changing individual behavior
- ☒ Evaluating security awareness training
- ☐ Filtering malicious e-mail content

Question 270

Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

- ☐ It is characterized by the stateless behavior of a process implemented in a function
- ☐ Test inputs are obtained from the derived boundaries of the given functional specifications
- ☐ An entire partition can be covered by considering only one representative value from that partition
- ☒ It is useful for testing communications protocols and graphical user interfaces

Question 271

Which of the following is considered a secure coding practice?

- ☐ Use concurrent access for shared variables and resources
- ☒ Use checksums to verify the integrity of libraries
- ☐ Use new code for common tasks
- ☐ Use dynamic execution functions to pass user supplied data

Question 272

Which of the following information MUST be provided for user account provisioning?

- ☐ Full name
- ☒ Unique identifier
- ☐ Security question
- ☐ Date of birth

Question 273

Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

- ☒ WEP uses a small range Initialization Vector (IV)
- ☐ WEP uses Message Digest 5 (MD5)
- ☐ WEP uses Diffie-Hellman
- ☐ WEP does not use any Initialization Vector (IV)

Explanation:

Reference: <http://www.dummies.com/programming/networking/understanding-wep-weaknesses/>

Question 274

Which of the following combinations would MOST negatively affect availability?

- ☒ Denial of Service (DoS) attacks and outdated hardware
- ☐ Unauthorized transactions and outdated hardware
- ☐ Fire and accidental changes to data
- ☐ Unauthorized transactions and denial of service attacks

Question 275

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 276

Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

- ☐ Limit access to predefined queries
- ☐ Segregate the database into a small number of partitions each with a separate security level
- ☒ Implement Role Based Access Control (RBAC)
- ☐ Reduce the number of people who have access to the system for statistical purposes

Question 277

A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results.

What should be implemented to BEST achieve the desired results?

- ☐ Configuration Management Database (CMDB)
- ☐ Source code repository
- ☒ Configuration Management Plan (CMP)
- ☐ System performance monitoring application

Question 278

What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

- ☐ Management support
- ☒ Consideration of organizational need
- ☐ Technology used for delivery
- ☐ Target audience

Question 279

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 280

What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

- ☒ Purging
- ☐ Encryption
- ☐ Destruction
- ☐ Clearing

Question 281

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 282

A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established.

What MUST be considered or evaluated before performing the next step?

- ☐ Notifying law enforcement is crucial before hashing the contents of the server hard drive
- ☐ Identifying who executed the incident is more important than how the incident happened
- ☒ Removing the server from the network may prevent catching the intruder
- ☐ Copying the contents of the hard drive to another storage device may damage the evidence

Question 283

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 284

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

- ☐ Aggregate it into one database in the US
- ☐ Process it in the US, but store the information in France
- ☒ Share it with a third party
- ☐ Anonymize it and process it in the US

Question 285

In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

- ☐ Modifying source code without approval
- ☒ Promoting programs to production without approval
- ☐ Developers checking out source code without approval
- ☐ Developers using Rapid Application Development (RAD) methodologies without approval

Question 286

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

- ☐ Examine the device for physical tampering
- ☐ Implement more stringent baseline configurations
- ☐ Purge or re-image the hard disk drive
- ☒ Change access codes

Question 287

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 288

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 289

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.