



Reference Solution for CISSP.exam.87q

CISSP

CISSP

Certified Information Systems Security Professional

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (87 questions)

Question 1

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 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 11

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 12

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 13

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 14

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 15

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 16

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 17

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 18

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 19

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 20

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 21

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 22

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 23

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 24

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 25

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 26

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

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

Question 27

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 28

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 29

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 30

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 31

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 32

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

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

Question 33

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 34

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 35

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 36

“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 37

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 38

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 39

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 40

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 41

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 42

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 43

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 44

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 45

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 46

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 47

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 48

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 49

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 50

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 51

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 52

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 53

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 54

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 55

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 56

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 57

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 58

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 59

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 60

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 61

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

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

Question 62

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 63

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

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

Question 64

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 65

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 66

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 67

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 68

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 69

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 70

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 71

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 72

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 73

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 74

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 75

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 76

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 77

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 78

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 79

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

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

Question 80

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 81

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 82

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 83

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 84

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 85

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 86

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 87

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