DUMPSGATE

ISC2

CISSP

Certified Information Systems Security Professional

QUESTION & ANSWERS

QUESTION 1

How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

A. It uses clear text and firewall rules.
B. It relies on Virtual Private Networks (VPN).
C. It uses clear text and shared secret keys.
D. It relies on asymmetric encryption keys.

Correct Answer: C

QUESTION 2

What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

A. Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).
B. Define the variable cost for extended downtime scenarios.
C. Identify potential threats to business availability.
D. Establish personnel requirements for various downtime scenarios.

Correct Answer: C

QUESTION 3

Which of the following is an important requirement when designing a secure remote access system?

A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
B. Provide privileged access rights to computer files and systems.
C. Ensure that logging and audit controls are included.
D. Reduce administrative overhead through password self service.

Correct Answer: C

QUESTION 4

An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

A. Recommend an update to the change control process.
B. Verify the approval of the configuration change.

C. Roll back the application to the original configuration.
D. Document the changes to the configuration.

Correct Answer: B

QUESTION 5

For a federated identity solution, a third-party Identity Provider (IdP) is PRIMARILY responsible for which of the following?

A. Access Control
B. Account Management
C. Authentication
D. Authorization

Correct Answer: C

QUESTION 6

What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

A. Isolate and contain the intrusion.
B. Notify system and application owners.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.

Correct Answer: C

QUESTION 7

Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

A. Peer authentication
B. Payload data encryption
C. Session encryption
D. Hashing digest

Correct Answer: C

QUESTION 8

Which of the following can be used to calculate the loss event probability?

A. Total number of possible outcomes divided by frequency of outcomes
B. Number of outcomes divided by total number of possible outcomes
C. Number of outcomes multiplied by total number of possible outcomes
D. Total number of possible outcomes multiplied by frequency of outcomes

Correct Answer: B

QUESTION 9

Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

A. SOC 1 Type1
B. SOC 1Type2
C. SOC 2 Type 1
D. SOC 2 Type 2

Correct Answer: D

QUESTION 10

If virus infection is suspected, which of the following is the FIRST step for the user to take?

A. Unplug the computer from the network.
B. Save the opened files and shutdown the computer.
C. Report the incident to service desk.
D. Update the antivirus to the latest version.

Correct Answer: C

QUESTION 11

Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

A. Load Testing
B. White-box testing
C. Black -boxtesting
D. Performance testing

Correct Answer: B

QUESTION 12

What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

A. In a dedicated Demilitarized Zone (DMZ)
B. In its own separate Virtual Local Area Network (VLAN)
C. At the Internet Service Provider (ISP)
D. Outside the external firewall

Correct Answer: B

QUESTION 13

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

A. Mandatory Access Controls (MAC)
B. Enterprise security architecture
C. Enterprise security procedures
D. Role Based Access Controls (RBAC)

Correct Answer: C

QUESTION 14

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

response
methodologies.
What code of ethics canon is being observed?

A. Provide diligent and competent service to principals
B. Protect society, the commonwealth, and the infrastructure
C. Advance and protect the profession
D. Act honorable, honesty, justly, responsibly, and legally

Correct Answer: C

Explanation/Reference:

Section: Security Operations

QUESTION 15

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

A. Into the options field
B. Between the delivery header and payload
C. Between the source and destination addresses
D. Into the destination address

Correct Answer: B

QUESTION 16

In Identity Management (IdM), when is the verification stage performed?

A. As part of system sign-on
B. Before creation of the identity
C. After revocation of the identity
D. During authorization of the identity

Correct Answer: A

QUESTION 17

Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

A. Large Key encryption
B. Single integrity protection
C. Embedded sequence numbers
D. Randomly generated nonces

Correct Answer: C

QUESTION 18

When conducting a security assessment of access controls, which activity is part of the data analysis phase?

A. Present solutions to address audit exceptions.
B. Conduct statistical sampling of data transactions.
C. Categorize and identify evidence gathered during the audit.
D. Collect logs and reports.

Correct Answer: C

Explanation/Reference:

Topic 14, NEW Questions C

QUESTION 19

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

A. Temporal Key Integrity Protocol (TKIP)
B. Secure Hash Algorithm (SHA)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

Correct Answer: B

QUESTION 20

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?

A. Trusted third-party certification
B. Lightweight Directory Access Protocol (LDAP)
C. Security Assertion Markup language (SAML)
D. Cross-certification

Correct Answer: C

QUESTION 21

Why must all users be positively identified prior to using multi-user computers?

A. To provide access to system privileges
B. To provide access to the operating system
C. To ensure that unauthorized persons cannot access the computers
D. To ensure that management knows what users are currently logged on

Correct Answer: C

QUESTION 22

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

A. Application interface entry and endpoints
B. The likelihood and impact of a vulnerability
C. Countermeasures and mitigations for vulnerabilities
D. A data flow diagram for the application and attack surface analysis

Correct Answer: D

QUESTION 23

What is the MAIN purpose of a change management policy?

A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
B. To identify the changes that may be made to the Information Technology (IT) infrastructure
C. To verify that changes to the Information Technology (IT) infrastructure are approved
D. To determine the necessary for implementing modifications to the Information Technology (IT)infrastructure

Correct Answer: C

Explanation/Reference:

Section: Security Operations

QUESTION 24

An analysis finds unusual activity coming from a computer that was thrown away several months prior, which of the following steps ensure the proper removal of the system?

A. Deactivation
B. Decommission
C. Deploy
D. Procure

Correct Answer: B

QUESTION 25

Which of the following is the MOST important action regarding authentication?

A. Granting access rights
B. Enrolling in the system
C. Establishing audit controls
D. Obtaining executive authorization

Correct Answer: B

QUESTION 26

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

A. Man-in-the-Middle (MITM) attack
B. Smurfing
C. Session redirect
D. Spoofing

Correct Answer: D

QUESTION 27

Discretionary Access Control (DAC) restricts access according to

A. data classification labeling.
B. page views within an application.
C. authorizations granted to the user.
D. management accreditation.

Correct Answer: C

QUESTION 28

What is the MOST important reason to configure unique user IDs?

A. Supporting accountability
B. Reducing authentication errors
C. Preventing password compromise
D. Supporting Single Sign On (SSO)

Correct Answer: A

QUESTION 29

Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If the intrusion causes the system processes to hang, which of the following has been affected?

A. System integrity
B. System availability
C. System confidentiality
D. System auditability

Correct Answer: B

QUESTION 30

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

A. Owner's ability to realize financial gain
B. Owner's ability to maintain copyright
C. Right of the owner to enjoy their creation
D. Right of the owner to control delivery method

Correct Answer: D

Explanation/Reference:

Topic 2, . Asset Security

QUESTION 31

Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Correct Answer: D

QUESTION 32

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?

A. Absence of a Business Intelligence (BI) solution
B. Inadequate cost modeling
C. Improper deployment of the Service-Oriented Architecture (SOA)
D. Insufficient Service Level Agreement (SLA)

Correct Answer: D

QUESTION 33

When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

A. Physical security
B. Data classification
C. Network control
D. Application layer control

Correct Answer: B

QUESTION 34

Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Correct Answer: A

QUESTION 35

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

A. Code quality, security, and origin
B. Architecture, hardware, and firmware
C. Data quality, provenance, and scaling
D. Distributed, agile, and bench testing

Correct Answer: A

QUESTION 36

What type of encryption is used to protect sensitive data in transit over a network?

A. Payload encryption and transport encryption
B. Authentication Headers (AH)
C. Keyed-Hashing for Message Authentication
D. Point-to-Point Encryption (P2PE)

Correct Answer: A

QUESTION 37

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

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

Correct Answer: B

QUESTION 38

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?

A. Configuration Management Database (CMDB)
B. Source code repository
C. Configuration Management Plan (CMP)
D. System performance monitoring application

Correct Answer: A

QUESTION 39

Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.
B. virus infection.
C. packet sniffing.
D. database injection.

Correct Answer: A

QUESTION 40

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

A. Provide input to the Information System (IS) owner regarding the security requirements of the data
B. Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS tooperate.
C. Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
D. Move the data to an Information System (IS) that does not contain data owned by other informationowners

Correct Answer: C

Explanation/Reference:

Section: Security Assessment and Testing

QUESTION 41

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

A. Standards, policies, and procedures
B. Tactical, strategic, and financial
C. Management, operational, and technical
D. Documentation, observation, and manual

Correct Answer: C

QUESTION 42

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

A. Minimize malicious attacks from third parties
B. Manage resource privileges
C. Share digital identities in hybrid cloud
D. Defined a standard protocol

Correct Answer: B

QUESTION 43

Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

A. Use of a unified messaging.
B. Use of separation for the voice network.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.

Correct Answer: B

QUESTION 44

Which of the following factors is PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

A. Testing and Evaluation (TE) personnel changes
B. Changes to core missions or business processes
C. Increased Cross-Site Request Forgery (CSRF) attacks
D. Changes in Service Organization Control (SOC) 2 reporting requirements

Correct Answer: B

QUESTION 45

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will be the PRIMARY security concern as staff is released from the organization?

A. Inadequate IT support
B. Loss of data and separation of duties
C. Undocumented security controls
D. Additional responsibilities for remaining staff

Correct Answer: B

QUESTION 46

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?

A. Application
B. Storage
C. Power
D. Network

Correct Answer: C

QUESTION 47

Why MUST a Kerberos server be well protected from unauthorized access?

A. It contains the keys of all clients.
B. It always operates at root privilege.
C. It contains all the tickets for services.
D. It contains the Internet Protocol (IP) address of all network entities.

Correct Answer: A

QUESTION 48

Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The third party needs to have

A. processes that are identical to that of the organization doing the outsourcing.
B. access to the original personnel that were on staff at the organization.
C. the ability to maintain all of the applications in languages they are familiar with.
D. access to the skill sets consistent with the programming languages used by the organization.

Correct Answer: D

QUESTION 49

A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

A. Network perimeters
B. Demilitarized Zones (DM2)
C. Databases and back-end servers
D. End-user devices

Correct Answer: D

QUESTION 50

Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

A. Business line management and IT staff members
B. Chief Information Officer (CIO) and DR manager
C. DR manager end IT staff members
D. IT staff members and project managers

Correct Answer: B

QUESTION 51

Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

Correct Answer: C

QUESTION 52

Which of the following BEST describes a Protection Profile (PP)?

A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Correct Answer: A

QUESTION 53

Which of the following practices provides the development team with a definition of security and identification of threats in designing software?

A. Penetration testing
B. Stakeholder review
C. Threat modeling
D. Requirements review

Correct Answer: C

QUESTION 54

Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

A. Data access control policies
B. Threat modeling
C. Common Criteria (CC)
D. Business Impact Analysis (BIA)

Correct Answer: A

QUESTION 55

Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

A. Lightweight Directory Access Control (LDAP)
B. Security Assertion Markup Language (SAML)
C. Hypertext Transfer Protocol (HTTP)
D. Kerberos

Correct Answer: A

QUESTION 56

What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

A. Exercise due diligence when deciding to circumvent host government requests.
B. Become familiar with the means in which the code of ethics is applied and considered.
C. Complete the assignment based on the customer's wishes.
D. Execute according to the professional's comfort level with the code of ethics.

Correct Answer: B

QUESTION 57

nternet Protocol (IP) source address spoofing is used to defeat

A. address-based authentication.
B. Address Resolution Protocol (ARP).
C. Reverse Address Resolution Protocol (RARP).
D. Transmission Control Protocol (TCP) hijacking.

Correct Answer: A

QUESTION 58

Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

A. Move cable are away from exterior facing windows
B. Encase exposed cable runs in metal conduit
C. Enable Power over Ethernet (PoE) to increase voltage
D. Bundle exposed cables together to disguise their signals

Correct Answer: B

QUESTION 59

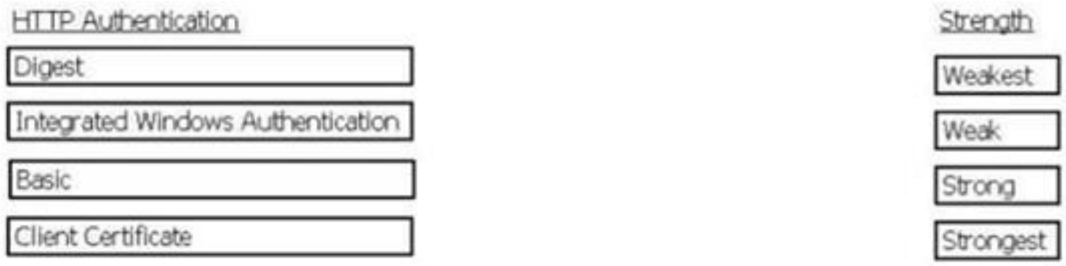
A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this
happening again?

A. Define additional security controls directly after the merger
B. Include a procurement officer in the merger team
C. Verify all contracts before a merger occurs
D. Assign a compliancy officer to review the merger conditions

Correct Answer: D

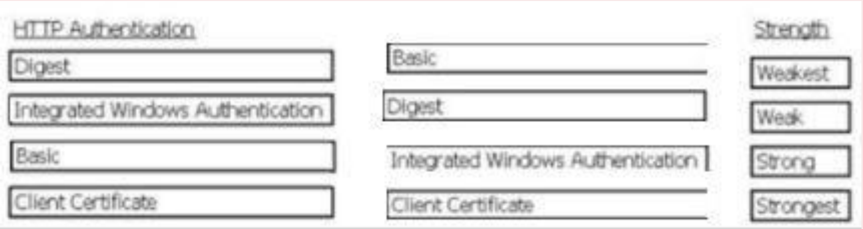
QUESTION 60

Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength.
Drag the authentication type on the correct positions on the right according to strength from weakest to strongest.



HTTP Authentication	Strength
Digest	Weakest
Integrated Windows Authentication	Weak
Basic	Strong
Client Certificate	Strongest

Correct Answer:



HTTP Authentication		Strength
Digest	Basic	Weakest
Integrated Windows Authentication	Digest	Weak
Basic	Integrated Windows Authentication	Strong
Client Certificate	Client Certificate	Strongest

QUESTION 61

Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A. Security credentials
B. Known vulnerabilities
C. Inefficient algorithms
D. Coding mistakes

Correct Answer: A

QUESTION 62

How can an attacker exploit overflow to execute arbitrary code?

A. Modify a function's return address.
B. Alter the address of the stack.
C. Substitute elements in the stack.
D. Move the stack pointer.

Correct Answer: A

QUESTION 63

Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

A. Test
B. Assessment
C. Review
D. Peer review

Correct Answer: C

QUESTION 64

How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

A. Take another backup of the media in question then delete all irrelevant operating system files.
B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
D. Discard harmless files for the operating system, and known installed programs.

Correct Answer: B

QUESTION 65

What is the PRIMARY difference between security policies and security procedures?

A. Policies are used to enforce violations, and procedures create penalties
B. Policies point to guidelines, and procedures are more contractual in nature
C. Policies are included in awareness training, and procedures give guidance
D. Policies are generic in nature, and procedures contain operational details

Correct Answer: D

QUESTION 66

Which of the following is a benefit in implementing an enterprise Identity and Access Management

(IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Correct Answer: A

QUESTION 67

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?

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

Correct Answer: D

QUESTION 68

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?

A. Purging
B. Encryption
C. Destruction
D. Clearing

Correct Answer: A

QUESTION 69

Which inherent password weakness does a One Time Password (OTP) generator overcome?

A. Static passwords must be changed frequently.
B. Static passwords are too predictable.
C. Static passwords are difficult to generate.

D. Static passwords are easily disclosed.

Correct Answer: D

QUESTION 70

Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

A. Implement full-disk encryption
B. Enable multifactor authentication
C. Deploy file integrity checkers
D. Disable use of portable devices

Correct Answer: D

QUESTION 71

Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

A. It uses a Subscriber Identity Module (SIM) for authentication.
B. It uses encrypting techniques for all communications.
C. The radio spectrum is divided with multiple frequency carriers.
D. The signal is difficult to read as it provides end-to-end encryption.

Correct Answer: A

QUESTION 72

Which of the following is the MOST important consideration that must be taken into account when deploying an enterprise patching solution that includes mobile devices?

A. Service provider(s) utilized by the organization
B. Whether it will impact personal use
C. Number of mobile users in the organization
D. Feasibility of downloads due to available bandwidth

Correct Answer: C

QUESTION 73

Which of the following is used to detect steganography?

A. Audio analysis
B. Statistical analysis
C. Reverse engineering
D. Cryptanalysis

Correct Answer: B

QUESTION 74

What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

A. Quantifiable justification
B. Baseline improvement
C. Risk evaluation
D. Formalized acceptance

Correct Answer: A

QUESTION 75

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

A. Integration with organizational directory services for authentication
B. Tokenization of data
C. Accommodation of hybrid deployment models
D. Identification of data location

Correct Answer: D

QUESTION 76

Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?

A. Cloud directory
B. Directory synchronization
C. Assurance framework
D. Lightweight Directory Access Protocol (LDAP)

Correct Answer: B

QUESTION 77

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

A. Smurf
B. Rootkit exploit
C. Denial of Service (DoS)
D. Cross site scripting (XSS)

Correct Answer: D

QUESTION 78

When would an organization review a Business Continuity Management (BCM) system?

A. When major changes occur on systems
B. When personnel changes occur
C. Before and after Disaster Recovery (DR) tests
D. At planned intervals

Correct Answer: D

QUESTION 79

When conducting a forensic criminal investigation on a computer had drive, what should be dene PRIOR to analysis?

A. Create a backup copy of all the important files on the drive.
B. Power off the computer and wait for assistance.
C. Create a forensic image of the hard drive.
D. Install forensic analysis software.

Correct Answer: C

QUESTION 80

In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Correct Answer: D