

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (Exam Topic 15)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

Answer: C

NEW QUESTION 2

- (Exam Topic 15)

A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

- A. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.
- B. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.
- C. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.
- D. Implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

Answer: D

NEW QUESTION 3

- (Exam Topic 15)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EIGRP
- D. RIP

Answer: B

NEW QUESTION 4

- (Exam Topic 15)

Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

- A. A DNS server can be disabled in a denial-of-service (DoS) attack.
- B. A DNS server does not authenticate source of information.
- C. Each DNS server must hold the address of the root servers.
- D. A DNS server database can be injected with falsified checksums.

Answer: A

NEW QUESTION 5

- (Exam Topic 15)

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the BEST design approach to securing this environment?

- A. Place firewalls around critical devices, isolating them from the rest of the environment.
- B. Layer multiple detective and preventative technologies at the environment perimeter.
- C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
- D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer: B

NEW QUESTION 6

- (Exam Topic 15)

Which security evaluation model assesses a product's Security Assurance Level (SAL) in comparison to similar solutions?

- A. Payment Card Industry Data Security Standard (PCI-DSS)
- B. International Organization for Standardization (ISO) 27001
- C. Common criteria (CC)
- D. Control Objectives for Information and Related Technology (COBIT)

Answer: C

NEW QUESTION 7

- (Exam Topic 15)

Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

- A. Creating a prototype to confirm or refine the customer requirements
- B. Drafting requirements for the service level agreement (SLA)
- C. Discussing technology and solution requirements with the customer
- D. Capturing and documenting the requirements of the customer

Answer: D

NEW QUESTION 8

- (Exam Topic 15)

Which of the following provides the MOST secure method for Network Access Control (NAC)?

- A. Media Access Control (MAC) filtering
- B. 802.1X authentication
- C. Application layer filtering
- D. Network Address Translation (NAT)

Answer: B

NEW QUESTION 9

- (Exam Topic 15)

During a penetration test, what are the three PRIMARY objectives of the planning phase?

- A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.
- B. Finalize management approval, determine testing goals, and gather port and service information.
- C. Identify rules of engagement, finalize management approval, and determine testing goals.
- D. Identify rules of engagement, document management approval, and collect system and application information.

Answer: D

NEW QUESTION 10

- (Exam Topic 15)

A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

- A. Risk avoidance
- B. Security engineering
- C. security awareness
- D. Phishing

Answer: C

NEW QUESTION 10

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?

- A. Negative testing
- B. Integration testing
- C. Unit testing
- D. Acceptance testing

Answer: B

NEW QUESTION 12

- (Exam Topic 15)

An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

- A. Fences eight or more feet high with three strands of barbed wire
- B. Fences three to four feet high with a turnstile
- C. Fences accompanied by patrolling security guards
- D. Fences six to seven feet high with a painted gate

Answer: A

NEW QUESTION 17

- (Exam Topic 15)

When reviewing the security logs, the password shown for an administrative login event was ' OR '1'='1' --. This is an example of which of the following kinds of attack?

- A. Brute Force Attack
- B. Structured Query Language (SQL) Injection
- C. Cross-Site Scripting (XSS)
- D. Rainbow Table Attack

Answer: B

NEW QUESTION 18

- (Exam Topic 15)

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

- A. ICS often do not have availability requirements.
- B. ICS are often isolated and difficult to access.
- C. ICS often run on UNIX operating systems.
- D. ICS are often sensitive to unexpected traffic.

Answer: B

NEW QUESTION 19

- (Exam Topic 15)

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

- A. Employee evaluation of the training program
- B. Internal assessment of the training program's effectiveness
- C. Multiple choice tests to participants
- D. Management control of reviews

Answer: B

NEW QUESTION 23

- (Exam Topic 15)

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

- A. Mandatory Access Control (MAC) and Discretionary Access Control (DAC)
- B. Discretionary Access Control (DAC) and Access Control List (ACL)
- C. Role Based Access Control (RBAC) and Mandatory Access Control (MAC)
- D. Role Based Access Control (RBAC) and Access Control List (ACL)

Answer: D

NEW QUESTION 27

- (Exam Topic 15)

What is the PRIMARY benefit of incident reporting and computer crime investigations?

- A. Providing evidence to law enforcement
- B. Repairing the damage and preventing future occurrences
- C. Appointing a computer emergency response team
- D. Complying with security policy

Answer: D

NEW QUESTION 31

- (Exam Topic 15)

Which of the following is the MOST effective preventative method to identify security flaws in software?

- A. Monitor performance in production environments.
- B. Perform a structured code review.
- C. Perform application penetration testing.
- D. Use automated security vulnerability testing tools.

Answer: B

NEW QUESTION 35

- (Exam Topic 15)

What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

- A. Man-in-the-Middle (MITM)
- B. Denial of Service (DoS)
- C. Domain Name Server (DNS) poisoning
- D. Buffer overflow

Answer: B

NEW QUESTION 40

- (Exam Topic 15)

Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

- A. Mandatory Access Control (MAC)
- B. Role Based Access Control (RBAC)
- C. Discretionary Access Control (DAC)
- D. Attribute Based Access Control (ABAC)

Answer:

B

NEW QUESTION 43

- (Exam Topic 15)

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

- A. RAID-0
- B. RAID-1
- C. RAID-5
- D. RAID-6

Answer: A

NEW QUESTION 44

- (Exam Topic 15)

Which audit type is MOST appropriate for evaluating the effectiveness of a security program?

- A. Threat
- B. Assessment
- C. Analysis
- D. Validation

Answer: B

NEW QUESTION 47

- (Exam Topic 15)

A user is allowed to access the file labeled "Financial Forecast," but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

- A. Minimum access control
- B. Rule-based access control
- C. Limited role-based access control (RBAC)
- D. Access control list (ACL)

Answer: B

NEW QUESTION 48

- (Exam Topic 15)

Which of the following is an indicator that a company's new user security awareness training module has been effective?

- A. There are more secure connections to the internal database servers.
- B. More incidents of phishing attempts are being reported.
- C. There are more secure connections to internal e-mail servers.
- D. Fewer incidents of phishing attempts are being reported.

Answer: B

NEW QUESTION 50

- (Exam Topic 15)

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

| SSID | Signal (RSSI) | Channel |
|-----------|---------------|---------|
| Corporate | -50 | 9 |
| Corporate | -69 | 10 |
| Corporate | -67 | 11 |
| Corporate | -63 | 6 |

Which of the following is MOST likely the cause of the issue?

- A. Channel overlap
- B. Poor signal
- C. Incorrect power settings
- D. Wrong antenna type

Answer: A

NEW QUESTION 51

- (Exam Topic 15)

Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

- A. Isolate the network, log an independent report, fix the problem, and redeploy the computer.
- B. Isolate the network, install patches, and report the occurrence.
- C. Prioritize, report, and investigate the occurrence.
- D. Turn the router off, perform forensic analysis, apply the appropriate fin, and log incidents.

Answer: C

NEW QUESTION 56

- (Exam Topic 15)

What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

- A. Reset all passwords.
- B. Shut down the network.
- C. Warn users of a breach.
- D. Segment the network.

Answer: D

NEW QUESTION 59

- (Exam Topic 15)

Which of the following is security control volatility?

- A. A reference to the stability of the security control.
- B. A reference to how unpredictable the security control is.
- C. A reference to the impact of the security control.
- D. A reference to the likelihood of change in the security control.

Answer: D

NEW QUESTION 63

- (Exam Topic 15)

Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

- A. Frequency analysis
- B. Ciphertext-only attack
- C. Probable-plaintext attack
- D. Known-plaintext attack

Answer: D

NEW QUESTION 66

- (Exam Topic 15)

Which of the following addresses requirements of security assessment during software acquisition?

- A. Software assurance policy
- B. Continuous monitoring
- C. Software configuration management (SCM)
- D. Data loss prevention (DLP) policy

Answer: B

NEW QUESTION 70

- (Exam Topic 15)

The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit. After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented. What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

- A. The external penetration testing company used custom zero-day attacks that could not have been predicted.
- B. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.
- C. The scope of the penetration test exercise and the internal audit were significantly different.
- D. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.

Answer: C

NEW QUESTION 71

- (Exam Topic 15)

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

- A. Hybrid frequency band, service set identifier (SSID), and interpolation
- B. Performance, geographic location, and radio signal interference
- C. Facility size, intermodulation, and direct satellite service
- D. Existing client devices, manufacturer reputation, and electrical interference

Answer: D

NEW QUESTION 76

- (Exam Topic 15)

An application is used for funds transfer between an organization and a third-party. During a security audit, an issue with the business continuity/disaster recovery policy and procedures for this application. Which of the following reports should the audit file with the organization?

- A. Service Organization Control (SOC) 1
- B. Statement on Auditing Standards (SAS) 70
- C. Service Organization Control (SOC) 2
- D. Statement on Auditing Standards (SAS) 70-1

Answer: C

NEW QUESTION 77

- (Exam Topic 15)

Which of the following is the MOST effective countermeasure against data remanence?

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

Answer: A

NEW QUESTION 81

- (Exam Topic 15)

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

- A. Traffic plane
- B. Application plane
- C. Data plane
- D. Control plane

Answer: A

NEW QUESTION 85

- (Exam Topic 15)

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

- A. For the establishment, exercise, or defense of legal claims
- B. The personal data has been lawfully processed and collected
- C. The personal data remains necessary to the purpose for which it was collected
- D. For the reasons of private interest

Answer: C

NEW QUESTION 90

- (Exam Topic 15)

- A. Obtain information security management approval.
- B. Maintain the integrity of the application.
- C. Obtain feedback before implementation.
- D. Identify vulnerabilities.

Answer: D

NEW QUESTION 92

- (Exam Topic 15)

Which of the following is the MOST appropriate control for asset data labeling procedures?

- A. Logging data media to provide a physical inventory control
- B. Reviewing audit trails of logging records
- C. Categorizing the types of media being used
- D. Reviewing off-site storage access controls

Answer: C

NEW QUESTION 93

- (Exam Topic 15)

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

- A. RAID level 1
- B. RAID level 3
- C. RAID level 4
- D. RAID level 5

Answer: D

NEW QUESTION 95

- (Exam Topic 15)

Which of the following is the MOST secure password technique?

- A. Passphrase
- B. One-time password
- C. Cognitive password
- D. dphertext

Answer: A

NEW QUESTION 96

- (Exam Topic 15)

In software development, which of the following entities normally signs the code to protect the code integrity?

- A. The organization developing the code
- B. The quality control group
- C. The data owner
- D. The developer

Answer: B

NEW QUESTION 97

- (Exam Topic 15)

Which of the following is the BEST way to determine the success of a patch management process?

- A. Analysis and impact assessment
- B. Auditing and assessment
- C. Configuration management (CM)
- D. Change management

Answer: A

NEW QUESTION 99

- (Exam Topic 15)

Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

- A. Remote Desktop Protocol (RDP)
- B. Federated identity management (FIM)
- C. Single sign-on (SSO)
- D. Multi-factor authentication (MFA)

Answer: B

NEW QUESTION 102

- (Exam Topic 15)

What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

- A. Semi-annually and in alignment with a fiscal half-year business cycle
- B. Annually or less frequently depending upon audit department requirements
- C. Quarterly or more frequently depending upon the advice of the information security manager
- D. As often as necessary depending upon the stability of the environment and business requirements

Answer: D

NEW QUESTION 107

- (Exam Topic 15)

Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

- A. Parallel
- B. Simulation
- C. Table-top
- D. Cut-over

Answer: C

NEW QUESTION 112

- (Exam Topic 15)

Which of the following poses the GREATEST privacy risk to personally identifiable information (PII) when disposing of an office printer or copier?

- A. The device could contain a document with PII on the platen glass
- B. Organizational network configuration information could still be present within the device
- C. A hard disk drive (HDD) in the device could contain PII
- D. The device transfer roller could contain imprints of PII

Answer: B

NEW QUESTION 116

- (Exam Topic 15)

Dumpster diving is a technique used in which stage of penetration testing methodology?

- A. Attack
- B. Discovery
- C. Reporting
- D. Planning

Answer: B

NEW QUESTION 119

- (Exam Topic 15)

What is the benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region?

- A. Identifies which security patches still need to be installed on the system
- B. Stops memory resident viruses from propagating their payload
- C. Reduces the risk of polymorphic viruses from encrypting their payload
- D. Helps prevent certain exploits that store code in buffers

Answer: C

NEW QUESTION 122

- (Exam Topic 15)

When assessing the audit capability of an application, which of the following activities is MOST important?

- A. Determine if audit records contain sufficient information.
- B. Review security plan for actions to be taken in the event of audit failure.
- C. Verify if sufficient storage is allocated for audit records.
- D. Identify procedures to investigate suspicious activity.

Answer: C

NEW QUESTION 126

- (Exam Topic 15)

Which of the following will accomplish Multi-Factor Authentication (MFA)?

- A. Issuing a smart card with a user-selected Personal Identification Number (PIN)
- B. Requiring users to enter a Personal Identification Number (PIN) and a password
- C. Performing a palm and retinal scan
- D. Issuing a smart card and a One Time Password (OTP) token

Answer: A

NEW QUESTION 129

- (Exam Topic 15)

Which of the following is the MOST significant key management problem due to the number of keys created?

- A. Keys are more difficult to provision and
- B. Storage of the keys require increased security
- C. Exponential growth when using asymmetric keys
- D. Exponential growth when using symmetric keys

Answer: B

NEW QUESTION 134

- (Exam Topic 15)

What BEST describes the confidentiality, integrity, availability triad?

- A. A tool used to assist in understanding how to protect the organization's data
- B. The three-step approach to determine the risk level of an organization
- C. The implementation of security systems to protect the organization's data
- D. A vulnerability assessment to see how well the organization's data is protected

Answer: C

NEW QUESTION 135

- (Exam Topic 15)

Commercial off-the-shelf (COTS) software presents which of the following additional security concerns?

- A. Vendors take on the liability for COTS software vulnerabilities.
- B. In-house developed software is inherently less secure.
- C. Exploits for COTS software are well documented and publicly available.
- D. COTS software is inherently less secure.

Answer:

C

NEW QUESTION 136

- (Exam Topic 15)

Security Software Development Life Cycle (SDLC) expects application code to be written in a consistent manner to allow ease of auditing and which of the following?

- A. Protecting
- B. Executing
- C. Copying
- D. Enhancing

Answer: A

NEW QUESTION 139

- (Exam Topic 15)

A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

- A. Read
- B. Execute
- C. Write
- D. Append

Answer: C

NEW QUESTION 141

- (Exam Topic 15)

Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

- A. A pre-action system is installed.
- B. An open system is installed.
- C. A dry system is installed.
- D. A wet system is installed.

Answer: C

NEW QUESTION 146

- (Exam Topic 15)

Which of the following describes the order in which a digital forensic process is usually conducted?

- A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results
- B. Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy
- C. Agree upon examination strategy, ascertain legal authority, conduct examination, and report results
- D. Agree upon examination strategy, ascertain legal authority, report results, and conduct examination

Answer: A

NEW QUESTION 150

- (Exam Topic 15)

At the destination host, which of the following OSI model layers will discard a segment with a bad checksum in the UDP header?

- A. Network
- B. Data link
- C. Transport
- D. Session

Answer: C

NEW QUESTION 151

- (Exam Topic 15)

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

- A. Lower costs throughout the System Development Life Cycle (SDLC)
- B. Facilitate a root cause analysis (RCA)
- C. Enable generation of corrective action reports
- D. Avoid lengthy audit reports

Answer: B

NEW QUESTION 155

- (Exam Topic 15)

An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

- A. Default the user to not share any information.
- B. Inform the user of the sharing feature changes after implemented.
- C. Share only what the organization decides is best.
- D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 158

- (Exam Topic 15)

An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

- A. Health Insurance Portability and Accountability Act (HIPAA)
- B. Service Organization Control (SOC) 2
- C. Payment Card Industry (PCI)
- D. Information Assurance Technical Framework (IATF)

Answer: B

NEW QUESTION 161

- (Exam Topic 15)

What documentation is produced FIRST when performing an effective physical loss control process?

- A. Deterrent controls list
- B. Security standards list
- C. inventory list
- D. Asset valuation list

Answer: C

NEW QUESTION 162

- (Exam Topic 15)

Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

- A. Use Media Gateway Control Protocol (MGCP)
- B. Use Transport Layer Security (TLS) protocol
- C. Use File Transfer Protocol (FTP)
- D. Use Secure Shell (SSH) protocol

Answer: B

NEW QUESTION 164

- (Exam Topic 15)

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

- A. Center for Internet Security (CIS)
- B. Common Vulnerabilities and Exposures (CVE)
- C. Open Web Application Security Project (OWASP)
- D. Common Vulnerability Scoring System (CVSS)

Answer: D

NEW QUESTION 169

- (Exam Topic 15)

Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

- A. Multiprotocol Label Switching (MPLS)
- B. Synchronous Optical Networking (SONET)
- C. Session Initiation Protocol (SIP)
- D. Fiber Channel Over Ethernet (FCoE)

Answer: A

NEW QUESTION 170

- (Exam Topic 15)

Which of the following explains why classifying data is an important step in performing a Risk assessment?

- A. To provide a framework for developing good security metrics
- B. To justify the selection of costly security controls
- C. To classify the security controls sensitivity that helps scope the risk assessment
- D. To help determine the appropriate level of data security controls

Answer: D

NEW QUESTION 172

- (Exam Topic 15)

An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

- A. Cross-Site Scripting (XSS)
- B. Extensible Markup Language (XML) external entities
- C. SQL injection (SQLI)
- D. Cross-Site Request Forgery (CSRF)

Answer: A

NEW QUESTION 174

- (Exam Topic 15)

What is the MOST significant benefit of role-based access control (RBAC)?

- A. Reduction in authorization administration overhead
- B. Reduces inappropriate access
- C. Management of least privilege
- D. Most granular form of access control

Answer: A

NEW QUESTION 179

- (Exam Topic 15)

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

- A. Public safety, duties to individuals, duties to the profession, and duties to principals
- B. Public safety, duties to principals, duties to individuals, and duties to the profession
- C. Public safety, duties to the profession, duties to principals, and duties to individuals
- D. Public safety, duties to principals, duties to the profession, and duties to individuals

Answer: C

NEW QUESTION 181

- (Exam Topic 15)

The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against

invalid input. Which of the following BEST assists this process?

- A. Application fuzzing
- B. Instruction set simulation
- C. Regression testing
- D. Sanity testing

Answer: A

NEW QUESTION 186

- (Exam Topic 15)

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

- A. Wide focus
- B. Strategic
- C. Anticipate
- D. Process

Answer: D

NEW QUESTION 190

- (Exam Topic 15)

Which of the following is TRUE for an organization that is using a third-party federated identity service?

- A. The organization enforces the rules to other organization's user provisioning
- B. The organization establishes a trust relationship with the other organizations
- C. The organization defines internal standard for overall user identification
- D. The organization specifies alone how to authenticate other organization's users

Answer: C

NEW QUESTION 191

- (Exam Topic 15)

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

- A. Planning
- B. Operation
- C. Assessment
- D. Improvement

Answer: B

NEW QUESTION 193

- (Exam Topic 15)

Which of the following are the three MAIN categories of security controls?

- A. Administrative, technical, physical
- B. Corrective, detective, recovery
- C. Confidentiality, integrity, availability
- D. Preventative, corrective, detective

Answer: A

NEW QUESTION 197

- (Exam Topic 15)

A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

- A. Username and personal identification number (PIN)
- B. Fingerprint and retinal scanners
- C. Short Message Services (SMS) and smartphone authenticator
- D. Hardware token and password

Answer: D

NEW QUESTION 201

- (Exam Topic 15)

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

- A. Consolidated data collection
- B. Distributed storage locations
- C. Distributed data collection
- D. Centralized processing location

Answer: C

NEW QUESTION 202

- (Exam Topic 15)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

- A. Layer 3 switch
- B. VPN headend
- C. Next-generation firewall
- D. Proxy server
- E. Intrusion prevention

Answer: C

NEW QUESTION 206

- (Exam Topic 15)

Which of the following documents specifies services from the client's viewpoint?

- A. Service level report
- B. Business impact analysis (BIA)
- C. Service level agreement (SLA)
- D. Service Level Requirement (SLR)

Answer: C

NEW QUESTION 209

- (Exam Topic 15)

What is the FIRST step in developing a patch management plan?

- A. Subscribe to a vulnerability subscription service.
- B. Develop a patch testing procedure.
- C. Inventory the hardware and software used.
- D. Identify unnecessary services installed on systems.

Answer: B

NEW QUESTION 214

- (Exam Topic 15)

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

- A. Detection of sophisticated attackers
- B. Resiliency of the system
- C. Topology of the network used for the system
- D. Risk assessment of the system

Answer: B

NEW QUESTION 219

- (Exam Topic 15)

Which of the following is the MOST effective measure for dealing with rootkit attacks?

- A. Turning off unauthorized services and rebooting the system
- B. Finding and replacing the altered binaries with legitimate ones
- C. Restoring the system from the last backup
- D. Reinstalling the system from trusted sources

Answer: D

NEW QUESTION 224

- (Exam Topic 15)

Which of the following is the MOST important first step in preparing for a security audit?

- A. Identify team members.
- B. Define the scope.
- C. Notify system administrators.
- D. Collect evidence.

Answer: B

NEW QUESTION 228

- (Exam Topic 15)

Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

- A. Memory collection
- B. Forensic disk imaging
- C. Malware analysis
- D. Live response

Answer: A

NEW QUESTION 233

- (Exam Topic 15)

Which technique helps system designers consider potential security concerns of their systems and applications?

- A. Penetration testing
- B. Threat modeling
- C. Manual inspections and reviews
- D. Source code review

Answer: B

NEW QUESTION 235

- (Exam Topic 15)

What are the first two components of logical access control?

- A. Confidentiality and authentication
- B. Authentication and identification
- C. Identification and confidentiality
- D. Authentication and availability

Answer: B

NEW QUESTION 240

- (Exam Topic 15)

Before allowing a web application into the production environment, the security practitioner performs multiple types of tests to confirm that the web application performs as expected. To test the username field, the security practitioner creates a test that enters more characters into the field than is allowed. Which of the following BEST describes the type of test performed?

- A. Misuse case testing
- B. Penetration testing
- C. Web session testing
- D. Interface testing

Answer: A

NEW QUESTION 245

- (Exam Topic 15)

Which software defined networking (SDN) architectural component is responsible for translating network requirements?

- A. SDN Application
- B. SDN Data path
- C. SDN Controller
- D. SDN Northbound Interfaces

Answer: D

NEW QUESTION 246

- (Exam Topic 15)

What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

- A. Implementation Phase
- B. Cancellation Phase
- C. Initialization Phase
- D. Issued Phase

Answer: A

NEW QUESTION 247

- (Exam Topic 15)

Which of the following vulnerabilities can be BEST detected using automated analysis?

- A. Valid cross-site request forgery (CSRF) vulnerabilities
- B. Multi-step process attack vulnerabilities
- C. Business logic flaw vulnerabilities
- D. Typical source code vulnerabilities

Answer: D

NEW QUESTION 250

- (Exam Topic 15)

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

- A. Intrusion prevention system (IPS)
- B. Multi-factor authentication (MFA)
- C. Data loss protection (DLP)
- D. Data at rest encryption

Answer: B

NEW QUESTION 255

- (Exam Topic 15)

A hacker can use a lockout capability to start which of the following attacks?

- A. Denial of service (DoS)
- B. Dictionary
- C. Ping flood
- D. Man-in-the-middle (MITM)

Answer: A

NEW QUESTION 258

- (Exam Topic 15)

An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

- A. Security Assertion Markup Language (SAML)
- B. YAML Ain't Markup Language (YAML)
- C. Hypertext Markup Language (HTML)
- D. Extensible Markup Language (XML)

Answer: A

NEW QUESTION 260

- (Exam Topic 15)

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

- A. Detective and recovery controls
- B. Corrective and recovery controls
- C. Preventative and corrective controls
- D. Recovery and proactive controls

Answer: C

NEW QUESTION 262

- (Exam Topic 15)

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

- A. Data processing
- B. Storage encryption
- C. File hashing
- D. Data retention policy

Answer: C

NEW QUESTION 263

- (Exam Topic 15)

Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

- A. Prevent information about browsing activities from being stored in the cloud.
- B. Store browsing activities in the cloud.
- C. Prevent information about browsing activities from being stored on the personal device.
- D. Store information about browsing activities on the personal device.

Answer: A

NEW QUESTION 266

- (Exam Topic 15)

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

- A. Training
- B. Legal
- C. Business
- D. Storage

Answer: B

NEW QUESTION 270

- (Exam Topic 15)

Which of the following is the BEST method to gather evidence from a computer's hard drive?

- A. Disk duplication
- B. Disk replacement
- C. Forensic signature
- D. Forensic imaging

Answer: D

NEW QUESTION 275

- (Exam Topic 15)

Why are packet filtering routers used in low-risk environments?

- A. They are high-resolution source discrimination and identification tools.
- B. They are fast and flexible, and protect against Internet Protocol (IP) spoofing.
- C. They are fast, flexible, and transparent.
- D. They enforce strong user authentication and audit log generation.

Answer: B

NEW QUESTION 279

- (Exam Topic 15)

A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

- A. Hardware encryption
- B. Certificate revocation list (CRL) policy
- C. Trusted Platform Module (TPM)
- D. Key exchange

Answer: B

NEW QUESTION 283

- (Exam Topic 15)

A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process?

- A. Service-oriented architecture (SOA)
- B. Spiral Methodology
- C. Structured Waterfall Programming Development
- D. Devops Integrated Product Team (IPT)

Answer: C

NEW QUESTION 286

- (Exam Topic 15)

What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

- A. improve the IR process.
- B. Communicate the IR details to the stakeholders.
- C. Validate the integrity of the IR.
- D. Finalize the IR.

Answer: A

NEW QUESTION 291

- (Exam Topic 15)

The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

- A. Grant temporary access to the former application owner's account
- B. Assign a temporary application owner to the system.
- C. Restrict access to the system until a replacement application owner is hired.
- D. Prevent changes to the confidential data until a replacement application owner is hired.

Answer: B

NEW QUESTION 296

- (Exam Topic 15)

What is the BEST design for securing physical perimeter protection?

- A. Crime Prevention through Environmental Design (CPTED)
- B. Barriers, fences, gates, and walls
- C. Business continuity planning (BCP)
- D. Closed-circuit television (CCTV)

Answer: B

NEW QUESTION 297

- (Exam Topic 15)

Which of the following determines how traffic should flow based on the status of the infrastructure true?

- A. Application plane
- B. Data plane
- C. Control plane
- D. Traffic plane

Answer: D

NEW QUESTION 302

- (Exam Topic 15)

A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

- A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system
- B. Add additional ultraviolet light filters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200
- C. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200.
- D. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system

Answer: C

NEW QUESTION 303

- (Exam Topic 15)

Which of the following VPN configurations should be used to separate Internet and corporate traffic?

- A. Split-tunnel
- B. Remote desktop gateway
- C. Site-to-site
- D. Out-of-band management

Answer: A

NEW QUESTION 305

- (Exam Topic 15)

Which of the following techniques evaluates the secure Bet principles of network or software architectures?

- A. Threat modeling
- B. Risk modeling
- C. Waterfall method
- D. Fuzzing

Answer: A

NEW QUESTION 307

- (Exam Topic 15)

Which media sanitization methods should be used for data with a high security categorization?

- A. Clear or destroy
- B. Clear or purge
- C. Destroy or delete
- D. Purge or destroy

Answer: D

NEW QUESTION 311

- (Exam Topic 15)

Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

- A. Payload encryption
- B. Sender confidentiality
- C. Sender non-repudiation
- D. Multi-factor authentication (MFA)

Answer: C

NEW QUESTION 314

- (Exam Topic 15)

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.

Answer: C

NEW QUESTION 315

- (Exam Topic 15)

Which of the following BEST describes centralized identity management?

- A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
- B. Service providers agree to integrate identity system recognition across organizational boundaries.
- C. Service providers identify an entity by behavior analysis versus an identification factor.
- D. Service providers perform as both the credential and identity provider (IdP).

Answer: B

NEW QUESTION 320

- (Exam Topic 15)

Which of the following is an important design feature for the outer door of a mantrap?

- A. Allow it to be opened by an alarmed emergency button.
- B. Do not allow anyone to enter it alone.
- C. Do not allow it to be observed by closed-circuit television (CCTV) cameras.
- D. Allow it be opened when the inner door of the mantrap is also open

Answer: D

NEW QUESTION 324

- (Exam Topic 15)

Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?

- A. System logs
- B. Anti-spyware
- C. Integrity checker
- D. Firewall logs

Answer: C

NEW QUESTION 325

- (Exam Topic 15)

Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

- A. Polyinstantiation
- B. Polymorphism
- C. Encapsulation
- D. Inheritance

Answer: A

NEW QUESTION 330

- (Exam Topic 15)

In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is the BEST way to restrict access to the network?

- A. Use switch port security to limit devices connected to a particular switch port.
- B. Use of virtual local area networks (VLAN) to segregate users.
- C. Use a client-based Network Access Control (NAC) solution.
- D. Use a clientless Network Access Control (NAC) solution

Answer: A

NEW QUESTION 335

- (Exam Topic 15)

Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

- A. Mean time to repair (MTTR)
- B. Quality of Service (QoS) between applications
- C. Availability of network services
- D. Financial penalties in case of disruption

Answer: B

NEW QUESTION 336

- (Exam Topic 15)

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

- A. Network is flooded with communication traffic by the attacker.
- B. Organization loses control of their network devices.
- C. Network management communications is disrupted.
- D. Attacker accesses sensitive information regarding the network topology.

Answer: B

NEW QUESTION 340

- (Exam Topic 15)

In Federated Identity Management (FIM), which of the following represents the concept of federation?

- A. Collection of information logically grouped into a single entity
- B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
- C. Collection of information for common identities in a system
- D. Collection of domains that have established trust among themselves

Answer: D

NEW QUESTION 345

- (Exam Topic 15)

What is the MOST appropriate hierarchy of documents when implementing a security program?

- A. Organization principle, policy, standard, guideline
- B. Policy, organization principle, standard, guideline
- C. Standard, policy, organization principle, guideline
- D. Organization principle, guideline, policy, standard

Answer: C

NEW QUESTION 349

- (Exam Topic 15)

Which of the following techniques evaluates the secure design principles of network OF software architectures?

- A. Risk modeling
- B. Threat modeling
- C. Fuzzing
- D. Waterfall method

Answer: B

NEW QUESTION 353

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

- A. Wireless Access Points (AP)
- B. Token-based authentication
- C. Host-based firewalls
- D. Trusted platforms

Answer: C

NEW QUESTION 356

- (Exam Topic 15)

In an IDEAL encryption system, who has sole access to the decryption key?

- A. System owner
- B. Data owner
- C. Data custodian
- D. System administrator

Answer: B

NEW QUESTION 360

- (Exam Topic 15)

Which of the following statements is MOST accurate regarding information assets?

- A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
- B. S3 Information assets include any information that is valuable to the organization,
- C. Building an information assets register is a resource-intensive job.
- D. Information assets inventory is not required for risk assessment.

Answer: B

NEW QUESTION 364

- (Exam Topic 15)

Which of the following are all elements of a disaster recovery plan (DRP)?

- A. Document the actual location of the ORP, developing an incident notification procedure, evaluating costs of critical components
- B. Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations
- C. Maintain proper documentation of all server logs, developing an incident notification procedure, establishing recovery locations
- D. Document the actual location of the ORP, recording minutes at all ORP planning sessions, establishing recovery locations

Answer: C

NEW QUESTION 368

- (Exam Topic 15)

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

- A. Scheduled team review of coding style and techniques for vulnerability patterns
- B. Using automated programs to test for the latest known vulnerability patterns
- C. The regular use of production code routines from similar applications already in use
- D. Ensure code editing tools are updated against known vulnerability patterns

Answer: B

NEW QUESTION 373

- (Exam Topic 15)

Building blocks for software-defined networks (SDN) require which of the following?

- A. The SDN is mostly composed of virtual machines (VM).
- B. The SDN is composed entirely of client-server pairs.
- C. Virtual memory is used in preference to random-access memory (RAM).
- D. Random-access memory (RAM) is used in preference to virtual memory.

Answer: C

NEW QUESTION 377

- (Exam Topic 14)

What form of attack could this represent?

- A. A Denial of Service (DoS) attack against the gateway router because the router can no longer accept packets from
- B. A transport layer attack that prevents the resolution of 10.102.10.6 address
- C. A Denial of Service (DoS) attack against 10.102.10.2 because it cannot respond correctly to ARP requests
- D. A masquerading attack that sends packets intended for 10.102.10.6 to 10.102.10.2

Answer:

D

NEW QUESTION 378

- (Exam Topic 14)

Which one of the following documentation should be included in a Disaster Recovery (DR) package?

- A. Source code, compiled code, firmware updates, operational log book and manuals.
- B. Data encrypted in original format, auditable transaction data, and recovery instructions for future extraction on demand.
- C. Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions,.....
- D. System configuration including hardware, software, hardware, interfaces, software Application Programming Interface (API) configuration, data structure,

Answer: C

NEW QUESTION 382

- (Exam Topic 14)

What should an auditor do when conducting a periodic audit on media retention?

- A. Check electronic storage media to ensure records are not retained past their destruction date.
- B. Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information....
- C. Check that hard disks containing backup data that are still within a retention cycle are being destroyed....
- D. Ensure that data shared with outside organizations is no longer on a retention schedule.

Answer: A

NEW QUESTION 386

- (Exam Topic 14)

An organization wants to enable users to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (FIM). Which of the following is used behind the scenes in a FIM deployment?

- A. Standard Generalized Markup Language (SGML)
- B. Extensible Markup Language (XML)
- C. Security Assertion Markup Language (SAML)
- D. Transaction Authority Markup Language (XAML)

Answer: C

NEW QUESTION 389

- (Exam Topic 14)

An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

- A. The CSP determines data criticality.
- B. The CSP provides end-to-end encryption services.
- C. The CSP's privacy policy may be developed by the organization.
- D. The CSP may not be subject to the organization's country legislation.

Answer: D

NEW QUESTION 393

- (Exam Topic 14)

Which of the following value comparisons MOST accurately reflects the agile development approach?

- A. Processes and tools over individuals and interactions
- B. Contract negotiation over customer collaboration
- C. Following a plan over responding to change
- D. Working software over comprehensive documentation

Answer: D

NEW QUESTION 397

- (Exam Topic 14)

Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

- A. Symmetric
- B. Asymmetric
- C. Ephemeral
- D. Permanent

Answer: A

Explanation:

Reference: <https://www.brainscape.com/flashcards/cryptography-message-integrity-6886698/packs/10957693>

NEW QUESTION 398

- (Exam Topic 14)

What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

- A. Resumption procedures describing the actions to be taken to return to normal business operations
- B. Emergency procedures describing the necessary actions to be taken following an incident jeopardizes business operations
- C. Fallback procedures describing what action are to be taken to more essential business activities to alternative temporary locations
- D. Maintain schedule how and the plan will be tested and the process for maintaining the plan

Answer: B

NEW QUESTION 400

- (Exam Topic 14)

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.

Answer: A

NEW QUESTION 405

- (Exam Topic 14)

Which of the following types of data would be MOST difficult to detect by a forensic examiner?

- A. Slack space data
- B. Steganographic data
- C. File system deleted data
- D. Data stored with a different file type extension

Answer: C

NEW QUESTION 408

- (Exam Topic 14)

Which of the following four iterative steps are conducted on third-party vendors in an on-going basis?

- A. Investigate, Evaluate, Respond, Monitor
- B. Frame, Assess, Respond, Monitor
- C. Frame, Assess, Remediate, Monitor
- D. Investigate, Assess, Remediate, Monitor

Answer: C

NEW QUESTION 411

- (Exam Topic 14)

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)

Answer: A

NEW QUESTION 413

- (Exam Topic 14)

Which of the following is used to detect steganography?

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

Answer: C

NEW QUESTION 418

- (Exam Topic 14)

During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should an assessor do?

- A. Increase the number and type of relevant staff to interview.
- B. Conduct a comprehensive examination of the Disaster Recovery Plan (DRP).
- C. Increase the level of detail of the interview questions.
- D. Conduct a detailed review of the organization's DR policy.

Answer: A

NEW QUESTION 421

- (Exam Topic 14)

Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

- A. Data Loss Protection (DIP), firewalls, data classification
- B. Least privilege access, Data Loss Protection (DLP), physical access controls
- C. Staff vetting, least privilege access, Data Loss Protection (DLP)
- D. Background checks, data encryption, web proxies

Answer: B

NEW QUESTION 424

- (Exam Topic 14)

From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

- A. Return the media to the system owner.
- B. Delete the sensitive data from the media.
- C. Physically destroy the retired media.
- D. Encrypt data before it is stored on the media.

Answer: C

NEW QUESTION 429

- (Exam Topic 14)

If a content management system (CSM) is implemented, which one of the following would occur?

- A. The test and production systems would be running the same software
- B. The applications placed into production would be secure
- C. Developers would no longer have access to production systems
- D. Patching the systems would be completed more quickly

Answer: A

NEW QUESTION 433

- (Exam Topic 14)

Which of the following job functions MUST be separated to maintain data and application integrity?

- A. Applications development and systems analysis
- B. Production control and data control functions
- C. Scheduling and computer operations
- D. Systems development and systems maintenance

Answer: D

NEW QUESTION 436

- (Exam Topic 14)

The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

- A. Users, permissions, operators, and protected objects
- B. Users, roles, operations, and protected objects
- C. Roles, accounts, permissions, and protected objects
- D. Roles, operations, accounts, and protected objects

Answer: B

NEW QUESTION 441

- (Exam Topic 14)

A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

- A. No, because the encryption solution is internal to the cloud provider.
- B. Yes, because the cloud provider meets all regulations requirements.
- C. Yes, because the cloud provider is GDPR compliant.
- D. No, because the cloud provider is not certified to host government data.

Answer: B

NEW QUESTION 444

- (Exam Topic 14)

An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.

Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

- A. The audit assessment has been conducted by an independent assessor.
- B. The audit reports have been signed by the third-party senior management.

- C. The audit reports have been issued in the last six months.
- D. The audit assessment has been conducted by an international audit firm.

Answer: A

NEW QUESTION 447

- (Exam Topic 14)

What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

- A. Sectors which are not assigned to a perform may contain data that was purposely hidden.
- B. Volume address information for he hard disk may have been modified.
- C. partition tables which are not completely utilized may contain data that was purposely hidden
- D. Physical address information for the hard disk may have been modified.

Answer: A

NEW QUESTION 451

- (Exam Topic 14)

Which of the following BEST describes how access to a system is granted to federated user accounts?

- A. With the federation assurance level
- B. Based on defined criteria by the Relying Party (RP)
- C. Based on defined criteria by the Identity Provider (IdP)
- D. With the identity assurance level

Answer: C

Explanation:

Reference: <https://resources.infosecinstitute.com/cissp-domain-5-refresh-identity-and-access-management/>

NEW QUESTION 452

- (Exam Topic 14)

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.

Answer: C

Explanation:

Reference:
<https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently/>

NEW QUESTION 454

- (Exam Topic 14)

A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

- A. Log of backup administrative actions
- B. Log of the transported media and its classification marking
- C. Log of the transported media and Its detailed contents
- D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 458

- (Exam Topic 14)

According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

- A. Level 0: Incomplete
- B. Level 1: Performed
- C. Level 2: Managed
- D. Level 3: Defined

Answer: D

NEW QUESTION 463

- (Exam Topic 14)

An organization implements a Remote Access Server (RAS). Once users connect to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use during this authentication?

- A. Transport layer security (TLS)

- B. Message Digest 5 (MD5)
- C. Lightweight Extensible Authentication Protocol (EAP)
- D. Subscriber Identity Module (SIM)

Answer: A

NEW QUESTION 466

- (Exam Topic 14)

Which of the following initiates the systems recovery phase of a disaster recovery plan?

- A. Issuing a formal disaster declaration
- B. Activating the organization's hot site
- C. Evacuating the disaster site
- D. Assessing the extent of damage following the disaster

Answer: A

NEW QUESTION 469

- (Exam Topic 14)

Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

- A. Issued Phase
- B. Cancellation Phase
- C. Implementation phase
- D. Initialization Phase

Answer: C

NEW QUESTION 472

- (Exam Topic 14)

Which of the following phases involves researching a target's configuration from public sources when performing a penetration test?

- A. Information gathering
- B. Social engineering
- C. Target selection
- D. Traffic enumeration

Answer: A

NEW QUESTION 476

- (Exam Topic 14)

During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BFST protect One confidentiality of information traveling One wireless transmission media?

- A. Configure a firewall to logically separate the data at the boundary.
- B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
- C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
- D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

Answer: B

NEW QUESTION 477

- (Exam Topic 14)

Match the level of evaluation to the correct common criteria (CC) assurance level.

Drag each level of evaluation on the left to is corresponding CC assurance level on the right

| Level of Evaluation | Assurance Level |
|---|-----------------|
| Structurally tested | 1 |
| Methodically tested and checked | 2 |
| Methodically designed, tested, and reviewed | 3 |
| Functionally tested | 4 |
| Semiformally verified design and tested | 5 |
| Formally verified design and tested | 6 |
| Semiformally designed and tested | 7 |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

| Level of Evaluation | Assurance Level |
|---|-----------------|
| Structurally tested | 1 |
| Methodically tested and checked | 2 |
| Methodically designed, tested, and reviewed | 3 |
| Functionally tested | 4 |
| Semiformally verified design and tested | 5 |
| Formally verified design and tested | 6 |
| Semiformally designed and tested | 7 |

NEW QUESTION 481

- (Exam Topic 14)

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 and IT staff members
- D. IT staff members and project managers

Answer: B

NEW QUESTION 485

- (Exam Topic 14)

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.

Answer: B

NEW QUESTION 489

- (Exam Topic 14)

An employee receives a promotion that entitles them to access higher-level functions on the company's accounting system, as well as keeping their access to the previous system that is no longer needed or applicable. What is the name of the process that tries to remove this excess privilege?

- A. Access provisioning
- B. Segregation of Duties (SoD)
- C. Access certification
- D. Access aggregation

Answer: B

NEW QUESTION 492

- (Exam Topic 14)

A security professional recommends that a company integrate threat modeling into its Agile development processes. Which of the following BEST describes the benefits of this approach?

- A. Reduce application development costs.
- B. Potential threats are addressed later in the Software Development Life Cycle (SDLC).
- C. Improve user acceptance of implemented security controls.
- D. Potential threats are addressed earlier in the Software Development Life Cycle (SDLC).

Answer: D

NEW QUESTION 494

- (Exam Topic 14)

What high Availability (HA) option of database allows multiple clients to access multiple database servers simultaneously?

- A. Non-Structured Query Language (NoSQL) database
- B. Relational database
- C. Shadow database
- D. Replicated database

Answer: C

NEW QUESTION 497

- (Exam Topic 14)

Which of the following trust services principles refers to the accessibility of information used by the systems, products, or services offered to a third-party provider's customers?

- A. Security
- B. Privacy
- C. Access
- D. Availability

Answer: C

Explanation:

Reference: <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/tr>

NEW QUESTION 499

- (Exam Topic 14)

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)

Answer: B

NEW QUESTION 504

- (Exam Topic 14)

Which of the following will help prevent improper session handling?

- A. Ensure that all UIWebView calls do not execute without proper input validation.
- B. Ensure that tokens are sufficiently long, complex, and pseudo-random.
- C. Ensure JavaScript and plugin support is disabled.
- D. Ensure that certificates are valid and fail closed.

Answer: B

NEW QUESTION 509

- (Exam Topic 14)

What is the threat modeling order using process for Attack simulation and threat analysis (PASTA)?

- A. Application decomposition, threat analysis, vulnerability detection, attack enumeration, risk/impact analysis
- B. Threat analysis, vulnerability detection, application decomposition, attack enumeration, risk/Impact analysis

- C. Risk/impact analysis, application decomposition, threat analysis, vulnerability detection, attack enumeration
- D. Application decomposition, threat analysis, risk/impact analysis, vulnerability detection, attack enumeration

Answer: A

NEW QUESTION 513

- (Exam Topic 14)

- A. The signer verifies that the software being loaded is the software originated by the signer.
- B. The vendor certifies the software being loaded is free of malicious code and that it was originated by the signer.
- C. The signer verifies that the software being loaded is free of malicious code.
- D. Both vendor and the signer certify the software being loaded is free of malicious code and it was originated by the signer.

Answer: A

NEW QUESTION 517

- (Exam Topic 14)

Company A is evaluating new software to replace an in-house developed application. During the acquisition process. Company A specified the security retirement, as well as the functional requirements. Company B responded to the acquisition request with their flagship product that runs on an Operating System (OS) that Company A has never used nor evaluated. The flagship product meets all security -and functional requirements as defined by Company A. Based upon Company B's response, what step should Company A take?

- A. Move ahead with the acquisition process, and purchase the flagship software
- B. Conduct a security review of the OS
- C. Perform functionality testing
- D. Enter into contract negotiations ensuring Service Level Agreements (SLA) are established to include security patching

Answer: B

NEW QUESTION 518

- (Exam Topic 14)

Why are mobile devices something difficult to investigate in a forensic examination?

- A. There are no forensics tools available for examination.
- B. They may have proprietary software installed to protect them.
- C. They may contain cryptographic protection.
- D. They have password-based security at logon.

Answer: B

NEW QUESTION 519

- (Exam Topic 14)

Which of the following presents the PRIMARY concern to an organization when setting up a federated single sign-on (SSO) solution with another

- A. Sending assertions to an identity provider
- B. Requesting Identity assertions from the partners domain
- C. defining the identity mapping scheme
- D. Having the resource provider query the Identity provider

Answer: C

NEW QUESTION 523

- (Exam Topic 14)

Which area of embedded devices are most commonly attacked?

- A. Application
- B. Firmware
- C. Protocol
- D. Physical Interface

Answer: A

NEW QUESTION 526

- (Exam Topic 14)

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 |
|--|--|
| <input type="text" value="Digest"/> | <input type="text" value="Weakest"/> |
| <input type="text" value="Integrated Windows Authentication"/> | <input type="text" value="Weak"/> |
| <input type="text" value="Basic"/> | <input type="text" value="Strong"/> |
| <input type="text" value="Client Certificate"/> | <input type="text" value="Strongest"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

HTTP Authentication

Strength

| | |
|-----------------------------------|-----------|
| Basic | Weakest |
| Digest | Weak |
| Integrated Windows Authentication | Strong |
| Client Certificate | Strongest |

NEW QUESTION 529

- (Exam Topic 14)

What Is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?

- A. Consult the lead investigate to team the details of the case and required evidence.
- B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.
- C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.
- D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.

Answer: D

NEW QUESTION 530

- (Exam Topic 14)

What is the PRIMARY objective for conducting an internal security audit?

- A. Verify that all systems and Standard Operating Procedures (SOP) are properly documented.
- B. Verify that all personnel supporting a system are knowledgeable of their responsibilities.
- C. Verify that security controls are established following best practices.
- D. Verify that applicable security controls are implemented and effective.

Answer: D

NEW QUESTION 532

- (Exam Topic 14)

Which of the following is critical if an employee is dismissed due to violation of an organization's acceptable use policy (Aup) ?

- A. Appropriate documentation
- B. privilege suspension
- C. proxy records
- D. Internet access logs

Answer: A

NEW QUESTION 537

- (Exam Topic 14)

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

- A. Ensuing Quality and validation trough periodic audits for ongoing data integrity
- B. Determining the impact the information has on the mission of the organization
- C. Maintaining fundamental data availability, including data storage and archiving
- D. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security

Answer: B

NEW QUESTION 538

- (Exam Topic 14)

Individuals have been identified and determined as having a need-to-know for the information. Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

- A. Attribute Based Access Control (ABAC)
- B. Role-Based Access Control (RBAC)
- C. Discretionary Access Control (DAC)
- D. Mandatory Access Control (MAC)

Answer: D

NEW QUESTION 542

- (Exam Topic 13)

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

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 546

- (Exam Topic 13)

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

| <u>Role</u> | | <u>Responsibility</u> |
|----------------------|--|---|
| 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. |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

| <u>Role</u> | | <u>Responsibility</u> |
|----------------------|----------------------|---|
| 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. |

NEW QUESTION 549

- (Exam Topic 13)

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

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 553

- (Exam Topic 13)

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

- A. To choose the primary development language
- B. To choose the integrated development environment
- C. To match the software requirements to the delivery plan
- D. To project manage the software delivery

Answer: D

NEW QUESTION 557

- (Exam Topic 13)

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

- A. Erase
- B. Sanitize
- C. Encrypt
- D. Degauss

Answer: B

NEW QUESTION 558

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 561

- (Exam Topic 13)

What is the PRIMARY goal of fault tolerance?

- A. Elimination of single point of failure
- B. Isolation using a sandbox
- C. Single point of repair
- D. Containment to prevent propagation

Answer: A

NEW QUESTION 566

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 570

- (Exam Topic 13)

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

- A. Security governance
- B. Risk management
- C. Security portfolio management
- D. Risk assessment

Answer: B

NEW QUESTION 575

- (Exam Topic 13)

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

Answer: D

NEW QUESTION 579

- (Exam Topic 13)

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

- A. Stateful firewall
- B. Distributed antivirus
- C. Log analysis

D. Passive honeypot

Answer: C

NEW QUESTION 582

- (Exam Topic 13)

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

- A. Reduce the probability of identification
- B. Detect further compromise of the target
- C. Destabilize the operation of the host
- D. Maintain and expand control

Answer: D

NEW QUESTION 584

- (Exam Topic 13)

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?

- A. Directory traversal
- B. Structured Query Language (SQL) injection
- C. Cross-Site Scripting (XSS)
- D. Shellcode injection

Answer: C

NEW QUESTION 588

- (Exam Topic 13)

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

- A. Morale
- B. Reputation
- C. Equipment
- D. Information

Answer: C

NEW QUESTION 592

- (Exam Topic 13)

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

- A. Log all activities associated with sensitive systems
- B. Provide links to security policies
- C. Confirm that confidentiality agreements are signed
- D. Employ strong access controls

Answer: D

NEW QUESTION 597

- (Exam Topic 13)

Which of the following is the BEST Identity-as-a-Service (IDaaS) solution for validating users?

- A. Single Sign-On (SSO)
- B. Security Assertion Markup Language (SAML)
- C. Lightweight Directory Access Protocol (LDAP)
- D. Open Authentication (OAuth)

Answer: B

NEW QUESTION 599

- (Exam Topic 13)

What are the steps of a risk assessment?

- A. identification, analysis, evaluation
- B. analysis, evaluation, mitigation
- C. classification, identification, risk management
- D. identification, evaluation, mitigation

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 602

- (Exam Topic 13)

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

- A. To support information security governance
- B. To reduce the number of audit findings
- C. To deter attackers
- D. To implement effective information security controls

Answer: A

NEW QUESTION 603

- (Exam Topic 13)

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?

- A. The network administrators have no knowledge of ICS
- B. The ICS is now accessible from the office network
- C. The ICS does not support the office password policy
- D. RS422 is more reliable than Ethernet

Answer: B

NEW QUESTION 604

- (Exam Topic 13)

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

- A. Truncating parts of the data
- B. Applying Access Control Lists (ACL) to the data
- C. Appending non-watermarked data to watermarked data
- D. Storing the data in a database

Answer: A

NEW QUESTION 606

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 608

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 611

- (Exam Topic 13)

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

- A. Countermeasure effectiveness
- B. Type of potential loss
- C. Incident likelihood
- D. Information ownership

Answer: C

NEW QUESTION 615

- (Exam Topic 13)

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

- A. Modifying source code without approval
- B. Promoting programs to production without approval
- C. Developers checking out source code without approval
- D. Developers using Rapid Application Development (RAD) methodologies without approval

Answer: A

NEW QUESTION 620

- (Exam Topic 13)

Which of the following is MOST effective in detecting information hiding in Transmission Control Protocol/Internet Protocol (TCP/IP) traffic?

- A. Stateful inspection firewall
- B. Application-level firewall
- C. Content-filtering proxy
- D. Packet-filter firewall

Answer: A

NEW QUESTION 622

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 626

- (Exam Topic 13)

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?

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

Answer: D

NEW QUESTION 629

- (Exam Topic 13)

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. Define a standard protocol

Answer: B

NEW QUESTION 632

- (Exam Topic 13)

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?

- A. Attribute Based Access Control (ABAC)
- B. Discretionary Access Control (DAC)
- C. Mandatory Access Control (MAC)
- D. Role-Based Access Control (RBAC)

Answer: D

NEW QUESTION 635

- (Exam Topic 13)

An organization plans 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. A source code escrow clause
- B. Right to request an independent review of the software source code
- C. Due diligence form requesting statements of compliance with security requirements
- D. Access to the technical documentation

Answer: B

NEW QUESTION 639

- (Exam Topic 13)

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

- A. Triple Data Encryption Standard (3DES)
- B. Advanced Encryption Standard (AES)
- C. Message Digest 5 (MD5)
- D. Secure Hash Algorithm 2(SHA-2)

Answer: B

NEW QUESTION 644

- (Exam Topic 13)

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?

- A. Discretionary Access Control (DAC)
- B. Role Based Access Control (RBAC)
- C. Media Access Control (MAC)
- D. Mandatory Access Control (MAC)

Answer: A

NEW QUESTION 645

- (Exam Topic 13)

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

- A. The IDS can detect failed administrator logon attempts from servers.
- B. The IDS can increase the number of packets to analyze.
- C. The firewall can increase the number of packets to analyze.
- D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 649

- (Exam Topic 13)

Which of the following is considered a secure coding practice?

- A. Use concurrent access for shared variables and resources
- B. Use checksums to verify the integrity of libraries
- C. Use new code for common tasks
- D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 653

- (Exam Topic 13)

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?

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

Answer: D

Explanation:

Section: Security Operations

NEW QUESTION 655

- (Exam Topic 13)

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

- A. Penetration
- B. System
- C. Performance
- D. Vulnerability

Answer: A

NEW QUESTION 656

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

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

Answer:

C

NEW QUESTION 659

- (Exam Topic 12)

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

- A. Data classification policy
- B. Software and hardware inventory
- C. Remediation recommendations
- D. Names of participants

Answer: B

NEW QUESTION 661

- (Exam Topic 12)

Reciprocal backup site agreements are considered to be

- A. a better alternative than the use of warm sites.
- B. difficult to test for complex systems.
- C. easy to implement for similar types of organizations.
- D. easy to test and implement for complex systems.

Answer: B

NEW QUESTION 662

- (Exam Topic 12)

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.

Answer: B

NEW QUESTION 664

- (Exam Topic 12)

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

- A. Full name
- B. Unique identifier
- C. Security question
- D. Date of birth

Answer: B

NEW QUESTION 667

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 672

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 675

- (Exam Topic 12)

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

- A. Mandating security policy acceptance
- B. Changing individual behavior
- C. Evaluating security awareness training
- D. Filtering malicious e-mail content

Answer: C

NEW QUESTION 679

- (Exam Topic 12)

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?

- A. Administrator should request data owner approval to the user access
- B. Administrator should request manager approval for the user access
- C. Administrator should directly grant the access to the non-sensitive files
- D. Administrator should assess the user access need and either grant or deny the access

Answer: A

NEW QUESTION 682

- (Exam Topic 12)

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

- A. Length of Initialization Vector (IV)
- B. Protection against message replay
- C. Detection of message tampering
- D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 683

- (Exam Topic 12)

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

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system
- D. Internal user accidentally accessing data

Answer: B

NEW QUESTION 686

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 691

- (Exam Topic 12)

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

- A. cost of redundant systems and backups.
- B. cost to recover from an outage.
- C. overall long-term impact of the outage.
- D. revenue lost during the outage.

Answer: C

NEW QUESTION 693

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 695

- (Exam Topic 12)

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

- A. organization policy.

- B. industry best practices.
- C. industry laws and regulations.
- D. management feedback.

Answer: A

NEW QUESTION 697

- (Exam Topic 12)

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

- A. The dynamic reconfiguration of systems
- B. The cost of downtime
- C. A recovery strategy for all business processes
- D. A containment strategy

Answer: C

NEW QUESTION 702

- (Exam Topic 12)

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

- A. Cost effectiveness of business recovery
- B. Cost effectiveness of installing software security patches
- C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
- D. Which security measures should be implemented

Answer: C

NEW QUESTION 706

- (Exam Topic 12)

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

- A. Transport and Session
- B. Data-Link and Transport
- C. Network and Session
- D. Physical and Data-Link

Answer: B

NEW QUESTION 709

- (Exam Topic 12)

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

- A. most calls to plug-in programs are susceptible.
- B. most supporting application code is susceptible.
- C. the graphical images used by the application could be susceptible.
- D. the supporting virtual machine could be susceptible.

Answer: C

NEW QUESTION 710

- (Exam Topic 12)

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 |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 roles permissions to particular duties based on job function
 Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

NEW QUESTION 714

- (Exam Topic 12)

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

- A. Reduced risk to internal systems.
- B. Prepare the server for potential attacks.
- C. Mitigate the risk associated with the exposed server.
- D. Bypass the need for a firewall.

Answer: A

NEW QUESTION 717

- (Exam Topic 12)

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

- A. Notification tool
- B. Message queuing tool
- C. Security token tool
- D. Synchronization tool

Answer: C

NEW QUESTION 719

- (Exam Topic 11)

Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

- A. Confidentiality and Integrity
- B. Availability and Accountability
- C. Integrity and Availability
- D. Accountability and Assurance

Answer: D

NEW QUESTION 723

- (Exam Topic 12)

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 | <input type="text"/> | Labeling of sensitive data |
| Technical | <input type="text"/> | Biometrics for authentication |
| Logical | <input type="text"/> | Constrained user interface |
| Physical | <input type="text"/> | Radio Frequency Identification (RFID) badge |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Administrative – labeling of sensitive data
 Technical – Constrained user interface
 Logical – Biometrics for authentication
 Physical – Radio Frequency Identification (RFID) badge

NEW QUESTION 727

- (Exam Topic 11)

What security risk does the role-based access approach mitigate MOST effectively?

- A. Excessive access rights to systems and data
- B. Segregation of duties conflicts within business applications
- C. Lack of system administrator activity monitoring
- D. Inappropriate access requests

Answer: A

NEW QUESTION 728

- (Exam Topic 11)

What is the MOST efficient way to secure a production program and its data?

- A. Disable default accounts and implement access control lists (ACL)
- B. Harden the application and encrypt the data
- C. Disable unused services and implement tunneling
- D. Harden the servers and backup the data

Answer: B

NEW QUESTION 730

- (Exam Topic 11)

The application of which of the following standards would BEST reduce the potential for data breaches?

- A. ISO 9000
- B. ISO 20121
- C. ISO 26000
- D. ISO 27001

Answer: D

NEW QUESTION 732

- (Exam Topic 11)

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

Answer: D

NEW QUESTION 733

- (Exam Topic 11)

What is the GREATEST challenge to identifying data leaks?

- A. Available technical tools that enable user activity monitoring.
- B. Documented asset classification policy and clear labeling of assets.
- C. Senior management cooperation in investigating suspicious behavior.
- D. Law enforcement participation to apprehend and interrogate suspects.

Answer: B

NEW QUESTION 738

- (Exam Topic 11)

Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

- A. Policy documentation review
- B. Authentication validation
- C. Periodic log reviews
- D. Interface testing

Answer: C

NEW QUESTION 740

- (Exam Topic 11)

Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Secure Architecture

Do you advertise shared security services with guidance for project teams?

Education & Guidance

Are most people tested to ensure a baseline skill- set for secure development practices?

Strategy & Metrics

Does most of the organization know about what's required based on risk ratings?

Vulnerability Management

Are most project teams aware of their security point(s) of contact and response team(s)?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

| | | |
|--------------------------|--------------------------|--|
| Secure Architecture | Secure Architecture | Do you advertise shared security services with guidance for project teams? |
| Education & Guidance | Education & Guidance | Are most people tested to ensure a baseline skill- set for secure development practices? |
| Strategy & Metrics | Strategy & Metrics | Does most of the organization know about what's required based on risk ratings? |
| Vulnerability Management | Vulnerability Management | Are most project teams aware of their security point(s) of contact and response team(s)? |

NEW QUESTION 743

- (Exam Topic 11)

After acquiring the latest security updates, what must be done before deploying to production systems?

- A. Use tools to detect missing system patches
- B. Install the patches on a test system
- C. Subscribe to notifications for vulnerabilities
- D. Assess the severity of the situation

Answer: B

NEW QUESTION 748

- (Exam Topic 11)

By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

- A. Lock pinging
- B. Lock picking
- C. Lock bumping
- D. Lock bricking

Answer: B

NEW QUESTION 750

- (Exam Topic 11)

Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

- A. security impact analysis.
- B. structured code review.
- C. routine self assessment.
- D. cost benefit analysis.

Answer: A

NEW QUESTION 753

- (Exam Topic 11)

Which of the following is a recommended alternative to an integrated email encryption system?

- A. Sign emails containing sensitive data
- B. Send sensitive data in separate emails
- C. Encrypt sensitive data separately in attachments
- D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 756

- (Exam Topic 11)

Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

- A. poor governance over security processes and procedures
- B. immature security controls and procedures
- C. variances against regulatory requirements
- D. unanticipated increases in security incidents and threats

Answer: A

NEW QUESTION 759

- (Exam Topic 11)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via

an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

- A. Document the system as high risk
- B. Perform a vulnerability assessment
- C. Perform a quantitative threat assessment
- D. Notate the information and move on

Answer: B

NEW QUESTION 761

- (Exam Topic 11)

What is the GREATEST challenge of an agent-based patch management solution?

- A. Time to gather vulnerability information about the computers in the program
- B. Requires that software be installed, running, and managed on all participating computers
- C. The significant amount of network bandwidth while scanning computers
- D. The consistency of distributing patches to each participating computer

Answer: B

NEW QUESTION 766

- (Exam Topic 11)

Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

- A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
- B. Selection to meet the security objectives stated in test documents
- C. Security behavior expected of a TOE
- D. Definition of the roles and responsibilities

Answer: C

NEW QUESTION 771

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 776

- (Exam Topic 11)

Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

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

Answer: C

NEW QUESTION 781

- (Exam Topic 11)

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.

Answer: D

NEW QUESTION 783

- (Exam Topic 11)

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

- A. Concept, Development, Production, Utilization, Support, Retirement
- B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
- C. Acquisition, Measurement, Configuration Management, Production, Operation, Support

D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 787

- (Exam Topic 11)

Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

- A. Ineffective data classification
- B. Lack of data access controls
- C. Ineffective identity management controls
- D. Lack of Data Loss Prevention (DLP) tools

Answer: A

NEW QUESTION 792

- (Exam Topic 11)

While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

- A. They should be recycled to save energy.
- B. They should be recycled according to NIST SP 800-88.
- C. They should be inspected and sanitized following the organizational policy.
- D. They should be inspected and categorized properly to sell them for reuse.

Answer: C

NEW QUESTION 793

- (Exam Topic 11)

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?

- A. Insecure implementation of Application Programming Interfaces (API)
- B. Improper use and storage of management keys
- C. Misconfiguration of infrastructure allowing for unauthorized access
- D. Vulnerabilities within protocols that can expose confidential data

Answer: D

NEW QUESTION 797

- (Exam Topic 11)

Retaining system logs for six months or longer can be valuable for what activities?

- A. Disaster recovery and business continuity
- B. Forensics and incident response
- C. Identity and authorization management
- D. Physical and logical access control

Answer: B

NEW QUESTION 800

- (Exam Topic 11)

After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

- A. Implement strong passwords authentication for VPN
- B. Integrate the VPN with centralized credential stores
- C. Implement an Internet Protocol Security (IPSec) client
- D. Use two-factor authentication mechanisms

Answer: D

NEW QUESTION 801

- (Exam Topic 11)

Which of the following is most helpful in applying the principle of LEAST privilege?

- A. Establishing a sandboxing environment
- B. Setting up a Virtual Private Network (VPN) tunnel
- C. Monitoring and reviewing privileged sessions
- D. Introducing a job rotation program

Answer: A

NEW QUESTION 804

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

- A. The cost required to install patches will be reduced.
- B. The time during which systems will remain vulnerable to an exploit will be decreased.
- C. The likelihood of system or application incompatibilities will be decreased.
- D. The ability to cover large geographic areas is increased.

Answer: C

NEW QUESTION 807

- (Exam Topic 11)

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.

Answer: C

NEW QUESTION 810

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 811

- (Exam Topic 11)

For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

- A. Information Systems Security Officer
- B. Data Owner
- C. System Security Architect
- D. Security Requirements Analyst

Answer: B

NEW QUESTION 813

- (Exam Topic 11)

How does an organization verify that an information system's current hardware and software match the standard system configuration?

- A. By reviewing the configuration after the system goes into production
- B. By running vulnerability scanning tools on all devices in the environment
- C. By comparing the actual configuration of the system against the baseline
- D. By verifying all the approved security patches are implemented

Answer: C

NEW QUESTION 814

- (Exam Topic 10)

Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

- A. Timing
- B. Cold boot
- C. Side channel
- D. Acoustic cryptanalysis

Answer: B

NEW QUESTION 816

- (Exam Topic 10)

According to best practice, which of the following is required when implementing third party software in a production environment?

- A. Scan the application for vulnerabilities
- B. Contract the vendor for patching
- C. Negotiate end user application training
- D. Escrow a copy of the software

Answer: A

NEW QUESTION 818

- (Exam Topic 10)

With data labeling, which of the following MUST be the key decision maker?

- A. Information security
- B. Departmental management
- C. Data custodian
- D. Data owner

Answer: D

NEW QUESTION 820

- (Exam Topic 10)

Which of the following is the BEST solution to provide redundancy for telecommunications links?

- A. Provide multiple links from the same telecommunications vendor.
- B. Ensure that the telecommunications links connect to the network in one location.
- C. Ensure that the telecommunications links connect to the network in multiple locations.
- D. Provide multiple links from multiple telecommunications vendors.

Answer: D

NEW QUESTION 821

- (Exam Topic 10)

Which of the following is a critical factor for implementing a successful data classification program?

- A. Executive sponsorship
- B. Information security sponsorship
- C. End-user acceptance
- D. Internal audit acceptance

Answer: A

NEW QUESTION 823

- (Exam Topic 10)

Which of the following violates identity and access management best practices?

- A. User accounts
- B. System accounts
- C. Generic accounts
- D. Privileged accounts

Answer: C

NEW QUESTION 824

- (Exam Topic 10)

Which of the following assures that rules are followed in an identity management architecture?

- A. Policy database
- B. Digital signature
- C. Policy decision point
- D. Policy enforcement point

Answer: D

NEW QUESTION 826

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

- A. Severity of risk
- B. Complexity of strategy
- C. Frequency of incidents
- D. Ongoing awareness

Answer: A

NEW QUESTION 830

- (Exam Topic 10)

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

- A. Time of data validation after disaster
- B. Time of data restoration from backup after disaster
- C. Time of application resumption after disaster
- D. Time of application verification after disaster

Answer: C

NEW QUESTION 834

- (Exam Topic 10)

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 indicate where the IT budget is BEST allocated during this time?

- A. Policies
- B. Frameworks
- C. Metrics
- D. Guidelines

Answer: C

NEW QUESTION 836

- (Exam Topic 10)

An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

- A. Pending legal hold
- B. Long term data mining needs
- C. Customer makes request to retain
- D. Useful for future business initiatives

Answer: A

NEW QUESTION 841

- (Exam Topic 10)

What is the MAIN feature that onion routing networks offer?

- A. Non-repudiation
- B. Traceability
- C. Anonymity
- D. Resilience

Answer: C

NEW QUESTION 844

- (Exam Topic 10)

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

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Ownership

Answer: A

NEW QUESTION 849

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Following best practice, where should the permitted access for each department and job classification combination be specified?

- A. Security procedures
- B. Security standards
- C. Human resource policy
- D. Human resource standards

Answer: B

NEW QUESTION 850

- (Exam Topic 10)

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 organization should ensure that the third party's physical security controls are in place so that they

- A. are more rigorous than the original controls.
- B. are able to limit access to sensitive information.
- C. allow access by the organization staff at any time.
- D. cannot be accessed by subcontractors of the third party.

Answer: B

NEW QUESTION 853

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CISSP Practice Exam Features:

- * CISSP Questions and Answers Updated Frequently
- * CISSP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP Practice Test Here](#)