QUESTION 460
An organization would like to implement an authorization mechanism that would simplify the assignment of various system access permissions for many users with similar job responsibilities. Which type of authorization mechanism would be the BEST choice for the organization to implement?

A. Role-based access control (RBAC)
B. Discretionary access control (DAC)
C. Content-dependent Access Control
D. Rule-based Access Control

Answer: A

QUESTION 461
Which service management process BEST helps information technology (IT) organizations with reducing cost, mitigating risk, and improving customer service?

A. Kanban
B. Lean Six Sigma
C. Information Technology Service Management (ITSM)
D. Information Technology Infrastructure Library (ITIL)

Answer: D

QUESTION 462
Under the General Data Protection Regulation (GDPR), what is the maximum amount of time allowed for reporting a personal data breach?

A. 24 hours
B. 48 hours
C. 72 hours
D. 96 hours

Answer: C
Explanation:
Under the General Data Protection Regulation (GDPR), the maximum amount of time allowed for reporting a personal data breach is 72 hours.

This means that organizations must notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

QUESTION 463
What is the MOST effective method to enhance security of a single sign-on (SSO) solution that interfaces with critical systems?

A. Two-factor authentication
B. Reusable tokens for application level authentication
C. High performance encryption algorithms
D. Secure Sockets Layer (SSL) for all communications

Answer: A
Explanation:
Two-factor authentication (2FA) adds an additional layer of security to the authentication process by requiring users to provide two forms of identification: something they know (e.g., a password) and something they have (e.g., a physical token or a mobile device). This approach significantly reduces the risk of unauthorized access even if the user's password is compromised.

QUESTION 464
A security practitioner detects an Endpoint attack on the organization's network. What is the MOST reasonable approach to mitigate future Endpoint attacks?

A. Remove all non-essential client-side web services from the network.
B. Harden the client image before deployment.
C. Screen for harmful exploits of client-side services before implementation.
D. Block all client-side web exploits at the perimeter.

Answer: B
Explanation:
Harden the client image before deployment is the most reasonable approach to mitigating future Endpoint attacks. Hardening the client image involves removing or disabling any unnecessary software or services, configuring the system to meet security best practices, and implementing appropriate security controls. By removing or disabling unnecessary software or services, the attack surface of the system is reduced, making it more difficult for attackers to exploit vulnerabilities in the system.

QUESTION 465
The Chief Information Security Officer (CISO) is to establish a single, centralized, and relational repository to hold all information regarding the software and hardware assets. Which of the following s ions would be the BEST option?

A. Information Security Management System (ISMS)
B. Configuration Management Database (CMDB)
C. Security Information and Event Management (SIEM)
D. Information Technology Asset Management (ITAM)

Answer: B
Explanation:
The CMDB tracks IT assets from a service and operational perspective, while ITAM focuses on IT assets from a financial and cost perspective.

QUESTION 466
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

A. Magnetism
B. Generation
C. Consumption

D. Static discharge

Answer: C
Explanation:
Simple power analysis is a method of side-channel attack that examines a chip's current consumption over a period of time.

QUESTION 467
Which of the following is a benefit of implementing data-in-use controls?

A. If the data is lost, it must be decrypted to be opened.
B. When the data is being viewed, it can only be printed by authorized users.
C. When the data is being viewed, it can be accessed using secure protocols.
D. If the data is lost, it may not be accessible to unauthorized users.

Answer: B

QUESTION 468
Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication
B. Self-registration
C. Basic authentication
D. Digest authentication

Answer: D
Explanation:
Digest Authentication is the best option here as it does not require the password to be transmitted. Rather, the client takes the username and password and uses the MD5 hashing algorithm to create a hash, which is then sent to the SQL Server.
The given answer, Form-based authentication is not particularly secure as the content of the user dialog box is sent as plain text, and the target server is not authenticated. This form of authentication can expose your user names and passwords unless all connections are over SSL.

QUESTION 469
Which of the following secure transport protocols is often used to secure Voice over Internet Protocol (VoIP) communications on a network from end to end?

A. Secure File Transfer Protocol (SFTP)
B. Secure Real-time Transport Protocol (SRTP)
C. Generic Routing Encapsulation (GRE)
D. Internet Protocol Security (IPSec)

Answer: B
Explanation:
Secure Real Time Transport Protocol (SRTP), aka Secure RTP or RTP Protocol, is used in VoIP, video and multimedia applications.

QUESTION 470
What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reflected by the retina
B. The pattern of blood vessels at the back of the eye
C. The size, curvature, and shape of the retina
D. The pattern of light receptors It the back of the eye

Answer: B
Explanation:
The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.

QUESTION 471
Which of the following is a MUST for creating a new custom-built, cloud-native application designed to be horizontally scalable?

A. Network as a Service (NaaS)
B. Platform as a Service (PaaS)
C. Infrastructure as a Service (IaaS)
D. Software as a Service (SaaS)

Answer: B
Explanation:
When creating a new custom-built, cloud-native application designed to be horizontally scalable, a Platform as a Service (PaaS) is a must. PaaS provides a platform that includes development tools, runtime environments, and infrastructure management, allowing developers to focus on building and scaling their applications without worrying about the underlying infrastructure. It provides the necessary framework for developing and deploying cloud-native applications with ease and scalability. Horizontal scalability, in particular, is often achieved through features provided by PaaS platforms, such as load balancing and auto-scaling.

QUESTION 472
Which of the following access control mechanisms characterized subjects and objects using a set of encoded security-relevant properties?

A. Mandatory access control (MAC)
B. Role-based access control (RBAC)
C. Attribute-based access control (ABAC)
D. Discretionary access control (DAC)

Answer: C
Explanation:
Attribute-based access control (ABAC) is an access control mechanism that characterizes subjects (users, processes) and objects (resources) using a set of encoded security-relevant attributes or properties. ABAC allows for fine-grained access control decisions based on various attributes such as user roles, resource classifications, time of access, and other contextual information. This flexibility in defining access policies makes ABAC suitable for complex and dynamic access control scenarios.

QUESTION 473
Which kind of dependencies should be avoided when implementing secure design principles in software-defined networking (SDN)?

A. Hybrid
B. Circular
C. Dynamic
D. Static

Answer: B
Explanation:
Circular dependencies occur when two or more components or entities depend on each other in a way that creates a circular chain of dependencies. This can lead to issues such as deadlock, where components wait for each other indefinitely, and it can make the system more difficult to manage and secure. To ensure the reliability and security of an SDN environment, it's important to minimize or eliminate circular dependencies among components.

QUESTION 474
Which mechanism provides the BEST protection against buffer overflow attacks in memory?

A. Address Space Layout Randomization (ASLR)
B. Memory management unit
C. Stack and heap allocation
D. Dynamic random access memory (DRAM)

Answer: A
Explanation:
ASLR randomizes the memory addresses of program components, making it difficult for attackers to predict the location of vulnerable functions or data structures in memory. This helps mitigate buffer overflow attacks by adding an additional layer of security.

QUESTION 475
Which of the following terms is used for online service providers operating within a federation?

A. Active Directory Federation Services (ADFS)
B. Relying party (RP)
C. Single sign-on (SSO)
D. Identity and access management (IAM)

Answer: A
Explanation:
In a federated identity system, the relying party (RP) is a service provider that relies on an identity provider (IdP) to authenticate and provide identity information for users. This allows users to access multiple services using a single sign-on (SSO) across different providers while maintaining their identity and access management (IAM) across these services.

QUESTION 476
The Chief Information Security Officer (CISO) of a large financial institution is responsible for implementing the security controls to protect the confidentiality and integrity of the organization's Information Systems. Which of the controls below is prioritized FIRST?

A. Firewall and reverse proxy
B. Web application firewall (WAF) and HyperText Transfer Protocol Secure (HTTPS)
C. Encryption of data in transit and data at rest
D. Firewall and intrusion prevention system (IPS)

Answer: C

QUESTION 477
Who is the BEST person to review developed application code to ensure it has been tested and verified?

A. A developer who knows what is expected of the application, but not the same one who developed it.
B. A member of quality assurance (QA) should review the developer's code.
C. A developer who understands the application requirements document, and who also developed the code.
D. The manager should review the developer's application code.

Answer: B

QUESTION 478
A bank failed to meet service-level agreements (SLA) with customers after suffering from a database failure of the

transaction processing system (TPS) that resulted in delayed financial deposits. A regulatory agency overseeing the bank would like to determine if the cause of the delay was a material weakness. Which of the following documents is MOST relevant for the regulatory agency to review?

A. Business continuity plan (BCP)
B. Business impact analysis (BIA)
C. Continuity of Operations Plan (COOP)
D. Enterprise resource planning (ERP)

Answer: B

QUESTION 479
What is the MOST effective way to ensure that a cloud service provider does not access a customer's data stored within its infrastructure?

A. Use the organization's encryption tools and data management controls.
B. Ensure that the cloud service provider will contractually not access data unless given explicit authority.
C. Request audit logs on a regular basis.
D. Utilize the cloud provider's key management and elastic hardware security module (HSM) support.

Answer: A
Explanation:
Most secure is to avoid the use and reliance of CSP's key infrastructure and only use internal one.

QUESTION 480
Prohibiting which of the following techniques is MOST helpful in preventing users from obtaining confidential data by using statistical queries?

A. Sequences of queries that refer repeatedly to the same population
B. Repeated queries that access multiple databases
C. Selecting all records from a table and displaying all columns
D. Running queries that access sensitive data

Answer: A
Explanation:
Statistical queries are queries that use statistical properties of a data set, rather than individual examples. They can support rich analysis of the data, such as histograms, marginals, distributions, and machine learning models. However, they can also pose a risk of revealing confidential data if not properly controlled.

QUESTION 481
Which of the following is a major component of the federated identity management (FIM) implementation model and used to establish a network between dozens of organizations?

A. Identity as a Service (IDaaS)
B. Attribute-based access control (ABAC)
C. Cross-certification
D. Trusted third party (TTP)

Answer: C
Explanation:
Cross-certification is a major component of the federated identity management (FIM) implementation model and is used to establish a network between dozens of organizations.
Cross-certification allows two different organizations to establish mutual trust by exchanging and validating each other's digital certificates. This mutual trust enables users in one organization to access resources in another organization

without the need for separate user accounts or authentication processes.

QUESTION 482
A Chief Information Security Officer (CISO) is considering various proposals for evaluating security weaknesses and vulnerabilities at the source code level. Which of the following items BEST equips the CISO to make smart decisions for the organization?

A. The Common Weakness Risk Analysis Framework (CWRAF)
B. The Common Vulnerabilities and Exposures (CVE)
C. The Common Weakness Enumeration (CWE)
D. The Open Web Application Security Project (OWASP) Top Ten

Answer: A
Explanation:
The Common Weakness Risk Analysis Framework (CWRAF). CWRAF is a framework that helps prioritize the security weaknesses and vulnerabilities in source code based on the operational context and potential impact of the software. CWRAF can also correlate scan findings to Common Weakness Enumeration (CWE) and Security Technical Implementation Guides (STIGs) to provide a comprehensive report of the security risks. The other items, such as CVE, CWE, and OWASP Top Ten, are useful sources of information about common vulnerabilities and exposures, but they do not provide a tailored analysis of the source code based on the specific operational environment and requirements.

QUESTION 483
Which of the following methods is MOST effective in mitigating Cross-Site Scripting (XSS) vulnerabilities within HyperText Markup Language (HTML) websites?

A. Use antivirus and endpoint protection on the server to secure the web-based application
B. Place the web-based system in a defined Demilitarized Zone (DMZ)
C. Use .NET framework with .aspx extension to provide a higher level of security to the web application so that the web server display can be locked down
D. Not returning any HTML tags to the browser client

Answer: D

QUESTION 484
Which of the following MOST accurately describes the Security Target (ST) in the Common Criteria framework?

A. The set of rules that define how resources or assets are managed and protected
B. A product independent set of security criteria for a class of products
C. The product and documentation to be evaluated
D. A document that includes a product specific set of security criteria

Answer: D

QUESTION 485
An organization has approved deployment of a virtual environment for the development servers and has established controls for restricting access to resources. In order to implement best security practices for the virtual environment, the security team MUST also implement which of the following steps?

A. Implement a dedicated management network for the hypervisor.
B. Deploy Terminal Access Controller Access Control System Plus (TACACS+) for authentication.
C. Implement complex passwords using Privileged Access Management (PAM).
D. Capture network traffic for the network interface.

Answer: A
Explanation:
Implementing a dedicated management network for the hypervisor is a critical security measure in virtual environments.

This network separation ensures that the management interface and communication with the hypervisor are isolated from the production network. It reduces the attack surface and the risk of unauthorized access to the hypervisor, making it more difficult for attackers to compromise the virtualization infrastructure.

QUESTION 486
Which of the following is a weakness of the Data Encryption Standard (DES)?

A. Block encryption scheme
B. Use of same key for encryption and decryption
C. Publicly disclosed algorithm
D. Inadequate key length

Answer: D
Explanation:
One of the weaknesses of the Data Encryption Standard (DES) is its key size. DES uses a 56-bit key, which is considered too short by modern cryptographic standards. This key size can be easily brute-forced by attackers with sufficient computing power, allowing them to decrypt DES-encrypted data relatively easily.

QUESTION 487
What are facets of trustworthy software in supply chain operations?

A. Functionality, safety, reliability, integrity, and accuracy
B. Confidentiality, integrity, availability, authenticity, and possession
C. Safety, reliability, availability, resilience, and security
D. Reparability, security, upgradability, functionality, and accuracy

Answer: C
Explanation:
Trustworthy software in supply chain operations requires that the software possess key characteristics such as safety, reliability, availability, resilience, and security. Safety ensures that the software does not harm people or the environment. Reliability ensures that the software works as intended and does not fail prematurely. Availability ensures that the software is available when needed. Resilience ensures that the software can withstand and recover from disruptions. Security ensures that the software is protected from unauthorized access, modification, or destruction.

QUESTION 488
In order to meet the project delivery deadline, a web application developer used readily available software components. Which is the BEST method for reducing the risk associated with this practice?

A. Ensure developers are using approved software development frameworks.
B. Obtain components from official sources over secured link.
C. Ensure encryption of all sensitive data in a manner that protects and defends against threats.
D. Implement a process to verify the effectiveness of the software components and settings.

Answer: B

QUESTION 489
To ensure proper governance of information throughout the lifecycle, which of the following should be assigned FIRST?

A. Owner
B. Classification
C. Custodian
D. Retention

Answer: B
Explanation:
The data owner sometimes refer to as the organizational owner or senior manager is the person who has the ultimate

organizational responsibility for data, the owner is typically the chief executive officer (CEO), president or a department head (DH). Data owners identify the classification of data and ensure that it is labeled properly.. in that case the first thing to assign is classification. my point is you dont assign the organizational owner.

QUESTION 490
An effective information security strategy is PRIMARILY based upon which of the following?

A. Risk management practices
B. Security budget constraints
C. Security control implementation
D. Industry and regulatory standards

Answer: A
Explanation:
A strategy that is focused solely on implementing security controls without a clear understanding of the organization's specific risks may result in over-engineering or under-engineering security controls. This can lead to unnecessary expense, operational disruption, or a false sense of security.

QUESTION 491
One of Canada's leading pharmaceutical firms recently hired a Chief Data Officer (CDO) to oversee its data privacy program. The CDO has discovered the firm's marketing department has been collecting information from individuals without their knowledge and consent via the company website. Which of the following privacy regulations should concern the CDO regarding this practice?

A. The Health Insurance Portability and Accountability Act (HIPAA)
B. The Privacy Act of 1974
C. The Fair Information Practice Principles (FIPPs)
D. The Personal Information Protection and Electronic Documents Act (PIPEDA)

Answer: D
Explanation:
PIPEDA is Canada's federal privacy law governing the collection, use, and disclosure of personal information by private sector organizations. It sets out rules for how organizations must handle individuals' personal information, including obtaining consent for the collection and use of personal data. Violating PIPEDA by collecting information without consent can result in significant penalties and fines. Therefore, the CDO should be concerned about ensuring compliance with PIPEDA and rectifying the unauthorized data collection practice.

QUESTION 492
An organization is attempting to strengthen the configuration of its enterprise resource planning (ERP) software in order to enforce sufficient segregation of duties (SoD). Which of the following approaches would BEST improve SoD effectiveness?

A. Implementation of frequent audits of access and activity in the ERP by a separate team with no operational duties
B. Implementation of strengthened authentication measures including mandatory second-factor authentication
C. Review of ERP access profiles to enforce the least-privilege principle based on existing employee responsibilities
D. Review of employee responsibilities and ERP access profiles to differentiate mission activities from system support activities

Answer: D
Explanation:
Reviewing ERP access profiles to enforce the least-privilege principle based on existing employee responsibilities is a good practice to ensure that employees have access only to the data and functionality they need to perform their job duties. However, it does not directly address SoD and may not be effective in preventing SoD violations.

QUESTION 493
Which type of log collection is focused on detecting and responding to attacks, malware infection, and data theft?

A. Intrusion detection
B. Operational
C. Security
D. Compliance

Answer: C

QUESTION 494
If a medical analyst independently provides protected health information (PHI) to an external marketing organization, which ethical principal is this a violation of?

A. Higher ethic in the worst case
B. Informed consent
C. Change of scale test
D. Privacy regulations

Answer: B
Explanation:
The ethical principle that is violated by a medical analyst who independently provides protected health information (PHI) to an external marketing organization is informed consent. Informed consent is the principle that every medical professional should allow the patient to retain control over their body and their data, and that the patient should be informed of and agree to any use or disclosure of their PHI. By providing PHI to an external organization without the patient's knowledge and consent, the medical analyst is violating the patient's right to privacy and autonomy.

QUESTION 495
Which of the following measures is the MOST critical in order to safeguard from a malware attack on a smartphone?

A. Enable strong password.
B. Install anti-virus for mobile.
C. Enable biometric authentication.
D. Prevent jailbreaking or rooting.

Answer: D
Explanation:
The most critical measure in order to safeguard from a malware attack on a smartphone is to prevent jailbreaking or rooting. Jailbreaking or rooting is the process of removing the manufacturer's or carrier's restrictions on a smartphone, which allows the user to install unauthorized apps or modify the system settings. However, this also removes a lot of the built-in security features of the smartphone, such as encryption, sandboxing, and app verification, and exposes the device to malware infections and attacks. Therefore, it is advisable to avoid jailbreaking or rooting your smartphone and to download apps only from reputable sources.

QUESTION 496
Which of the following Secure Shell (SSH) remote access practices is MOST suited for scripted functions?

A. Restricting authentication by Internet Protocol (IP) address
B. Requiring multi-factor authentication (MFA)
C. Implementing access credentials management tools
D. Using public key-based authentication method

Answer: D
Explanation:
Public key-based authentication is particularly well-suited for scripted functions because it allows for automated,

passwordless access to remote systems. With this method, a public key is generated and stored on the server, and a corresponding private key is used on the client-side for authentication. Since there are no passwords involved, scripted processes can use the private key to authenticate securely without manual password entry.

QUESTION 497
Which stage in the identity management (IdM) lifecycle constitutes the GREATEST risk for an enterprise if performed incorrectly?

A. Propagating
B. Deprovisioning
C. Provisioning
D. Maintaining

Answer: B
Explanation:
Deprovisioning, also known as offboarding or deactivation, involves the process of revoking access and privileges for users who are leaving the organization or no longer need access to certain resources. If deprovisioning is not performed correctly or in a timely manner, it can pose significant security risks to an organization.

QUESTION 498
Which of the following reports provides the BEST attestation of detailed controls when evaluating an Identity as a Service (IDaaS) solution?

A. Service Organization Control (SOC) 1
B. Service Organization Control (SOC) 2
C. Service Organization Control (SOC) 3
D. Statement on Auditing Standards (SAS) 70

Answer: B

QUESTION 499
Single sign-on (SSO) for federated identity management (FIM) must be implemented and managed so that authorization mechanisms protect access to privileged information using OpenID Connect (OIDC) token or Security Assertion Markup Language (SAML) assertion. What is the BEST method to use to protect them?

A. Pass data in a bearer assertion, only signed by the identity provider.
B. Tokens and assertion should use base64 encoding to assure confidentiality.
C. Use a challenge and response mechanism such as Challenge Handshake Authentication Protocol (CHAP).
D. The access token or assertion should be encrypted to ensure privacy.

Answer: D

QUESTION 500
The client of a security firm reviewed a vulnerability assessment report and claims the report is inaccurate. The client states that the vulnerabilities listed are not valid because the host's operating system (OS) was not properly detected. Where in the vulnerability assessment process did the error MOST likely occur?

A. Report writing
B. Detection
C. Enumeration
D. Scanning

Answer: D

QUESTION 501

For a victim of a security breach to prevail in a negligence claim, what MUST the victim establish?

A. Concern
B. Breach of contract
C. Proximate cause
D. Hardship

Answer: C

QUESTION 502
A large international organization that collects information from its consumers has contracted with a Software as a Service (SaaS) cloud provider to process this data. The SaaS cloud provider uses additional data processing to demonstrate other capabilities it wishes to offer to the data owner. This vendor believes additional data processing activity is allowed since they are not disclosing to other organizations. Which of the following BEST supports this rationale?

A. The data was encrypted at all times and only a few cloud provider employees had access.
B. As the data owner, the cloud provider has the authority to direct how the data will be processed.
C. As the data processor, the cloud provider has the authority to direct how the data will be processed.
D. The agreement between the two parties is vague and does not detail how the data can be used.

Answer: D
Explanation:
The large org is the data controller and CSP is its data processor. But data processors do not decide how to process data. Data Controller, the large org controls how data is to be processed.

QUESTION 503
A security engineer is conducting an audit of an organization's Voice over Internet Protocol (VoIP) phone network due to a large increase in charges from their phone provider. The engineer discovers unauthorized endpoints have connected to the phone server from the public internet and placed hundreds of unauthorized calls to parties around the globe. Which type of attack occurred?

A. Control eavesdropping
B. Toll fraud
C. Call hijacking
D. Address spoofing

Answer: B

QUESTION 504
An organization is looking to improve threat detection on their wireless network. The company goal is to automate alerts to improve response efforts. Which of the following best practices should be implemented FIRST?

A. Deploy a standalone guest Wi-Fi network.
B. Implement multi-factor authentication (MFA) on all domain accounts.
C. Deploy a wireless intrusion detection system (IDS).
D. Implement 802.1x authentication.

Answer: C
Explanation:
The best practice that should be implemented first to improve threat detection on the wireless network is C. Deploy a wireless intrusion detection system (IDS). A wireless IDS can monitor the network traffic and alert the administrator of any suspicious or malicious activity, such as unauthorized access, denial-of-service attacks, or rogue access points. A wireless IDS can also help automate the response efforts by blocking or isolating the attackers. The other options are also important for wireless network security, but they are not directly related to threat detection.

QUESTION 505
Security personnel should be trained by emergency management personnel in what to do before and during a disaster, as well as their role in recovery efforts. Personnel should take required training for emergency response procedures and protocols. Which part of physical security design does this fall under?

A. Legal concerns
B. Loss prevention
C. Emergency preparedness
D. Liability for employee conduct

Answer: C
Explanation:
The training of security personnel on what to do before, during, and after a disaster, as well as their role in recovery efforts, aligns with the concept of emergency preparedness. This involves preparing individuals and organizations for potential emergencies, disasters, or other unexpected events. It includes training, planning, and implementing procedures to ensure a coordinated and effective response to various scenarios that may impact the security and safety of personnel and assets.

QUESTION 506
How is protection for hypervisor host and software administration functions BEST achieved?

A. Enforce network controls using a host-based firewall.
B. Deploy the management interface in a dedicated virtual network segment.
C. The management traffic pathway should have separate physical network interface cards (NIC) and network.
D. Deny permissions to specific virtual machines (VM) groups and objects.

Answer: C

QUESTION 507
To ensure compliance with the General Data Protection Regulation (GDPR), who in the organization should the help desk manager confer with before selecting a Software as a Service (SaaS) solution?

A. Data owner
B. Database administrator (DBA)
C. Data center manager
D. Data Protection Officer (DPO)

Answer: D

QUESTION 508
An Information System Security Officer (ISSO) employed by a large corporation, while also freelancing in a similar role for a competitor, violates what canon of the (ISC)2 Code of Professional Ethics?

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

Answer: B
Explanation:
We must ensure that we are in a position to provide unbiased, competent service to our organization.

QUESTION 509
Which is the FIRST action the Incident Response team should take when an incident is suspected?

A. Choose a containment strategy.
B. Record all facts regarding the incident.
C. Attempt to identify the attacker.
D. Notify management of the incident.

Answer: B
Explanation:
When the incident is suspected, you want to record all facts to help confirm if it becomes and actual incident. Once it becomes confirmed as an actual incident then containment is the next course of action.

QUESTION 510
A hospital has three data classification levels: shareable without restrictions, shareable with restrictions, and internal use only. Which of the following BEST demonstrates adhering to principles of good enterprise data classification?

A. A printout of the employee code of conduct marked "shareable with restrictions" is posted in the hallway where patients have access.
B. A printout of the employee code of conduct marked "internal use only" is posted in the waiting room.
C. A memo regarding a newly discovered data breach marked as "internal use only" is posted on the wall in the employee lunchroom.
D. An electronic health record (EHR) with personally identifiable information (PII) marked as "sharable with restrictions" is found in the employee lunchroom.

Answer: C

QUESTION 511
A web application requires users to register before they can use its services. Users must choose a unique username and a password that contains a minimum of eight characters. Which method MUST be used to store these passwords to ensure offline attacks are difficult?

A. Use an encryption algorithm that is fast with a random per-user encryption key.
B. Use a hash function that is fast with a per-user random salt.
C. Use a hash function with a cost factor and a per-user random salt.
D. Use an encryption algorithm with a random master key.

Answer: C
Explanation:
Active discovery is identifying and cataloging assets within an organization's environment. This can be done manually or through the use of automated tools. The goal of active discovery is to create an accurate inventory of all devices and software within the network.

QUESTION 512
Which of the following is the PRIMARY objective of performing scans with an active discovery tool?

A. Discovering virus and malware activity
B. Discovering changes for security configuration management (CM)
C. Asset identification (ID) and inventory management
D. Vulnerability management and remediation

Answer: C

QUESTION 513
A large law firm would like to enable employees to participate in a bring your own device (BYOD) program. Only devices with up-to-date antivirus and operating system (OS) patches will be allowed on the network. Which solution will BEST enforce the security requirements?

A. Endpoint Detection and Response
B. Next-Generation Firewall
C. Intrusion detection and prevention system (IDPS)
D. Network Access Control (NAC)

Answer: D

QUESTION 514
A security operations center (SOC) discovers a recently deployed router beaconing to a malicious website. Replacing the router fixes the issue. What is the MOST likely cause of the router's behavior?

A. The network administrator failed to reconfigure the router's access control list (ACL).
B. The router was damaged during shipping or installed incorrectly.
C. The router was counterfeit and acquired through unauthorized channels.
D. The network administrator failed to update the router's firmware.

Answer: C
Explanation:
The router was beaconing to a malicious site. This is a sign of root kit like malware messing up the newly installed router. This is a tell-tale sign of a counterfeit product.

QUESTION 515
The principle that personally identifiable information (PII) should be kept up-to-date and relevant to the purposes for which they are to be used is attributed to which fair information practice per the United States (US) Organization for Economic Cooperation and Development (OECD)?

A. Purpose Specification
B. Security Safeguards
C. Collection Limitation
D. Data Quality

Answer: D

QUESTION 516
Which of the following are common components of a Security Assertion Markup Language (SAML) based federation system?

A. Client, Service Provider, identity provider (IdP), Token
B. Client, Service Provider, Resource Server, Grant
C. Client, Authorization Server, identity provider (IdP), Claim
D. Client, Authorization Server, Resource Server, Assertion

Answer: A

QUESTION 517
Which of the following is the MOST effective way to ensure hardware and software remain updated throughout an organization?

A. Performance of frequent security configuration audits
B. Performance of regular vulnerability scans
C. Use an inventory management tool
D. Use an automated configuration monitoring system

Answer: D

QUESTION 518
When developing an electronic health record (EHR) in the United States (US), which of the following would be the BEST source of information for any compliance requirements?

A. World Health Organization (WHO)
B. International Organization for Standardization (ISO)
C. Health and Human Services (HHS)
D. American Public Health Association (APHA)

Answer: C

QUESTION 519
An organization suspects it is receiving spoofed e-mails from a foreign-hosted web e-mail service. Where can the MOST relevant be found to begin the process of identifying the perpetrator?

A. E-mail logs from foreign-hosted web server
B. Message header of received e-mails
C. Traffic logs from the corporate firewall
D. Log files of the corporate Simple Mail Transfer Protocol (SMTP) server

Answer: B

QUESTION 520
A new internal auditor is tasked with auditing the supply chain. The system owner stated that the last internal auditor was terminated because the auditor discovered too many deficient controls. The auditor reports this conversation to their manager. Which of the following audit integrity principles BEST applies to this situation?

A. Demonstrate competence while performing professional duties.
B. Perform professional duties with honesty, diligence, and responsibility.
C. Perform professional duties in accordance with company policy.
D. Be aware of any influences that may be exerted on professional judgement.

Answer: B

QUESTION 521
An organization implements supply chain risk management (SCRM) into all phases of the Systems Development Life Cycle (SDLC). What methodology is MOST important to ensure that SCRM requirements are met?

A. Supplier self-assessment
B. Procurement assessment
C. Vulnerability assessment
D. Third-party assessment

Answer: D

QUESTION 522
An organization needs to evaluate the effectiveness of security controls implemented on a new system. Which of the following roles should the organization entrust to conduct the evaluation?

A. Authorizing Official (AO)
B. System owner
C. Control assessor
D. Information System Security Officer (ISSO)

Answer: C

QUESTION 523
During a disruptive event, which security continuity objectives will maintain an organization's information security to a predetermined level?

A. Disaster recovery plan (DRP)
B. Impact assessment report
C. Information security continuity plan
D. Business continuity plan (BCP)

Answer: C

QUESTION 524
An organization is implementing a bring your own device (BYOD) policy. What would be BEST for mitigating the risk of users managing their own devices and potentially bringing in malware?

A. Setting up access control lists (ACL) for these devices.
B. Installing a firewall on the organization's primary network.
C. Setting up a separate network within the organization's demilitarized zone (DMZ).
D. Setting up a separate, external wired or wireless network dedicated to these devices.

Answer: D

QUESTION 525
An organization acquired used technological equipment. This equipment will be integrated with new and existing business processes. What is the MOST appropriate consideration to identify the equipment that requires protection?

A. Total monetary value of the acquisition
B. The age of the computing hardware
C. Stakeholder concerns of how the assets are used
D. Length and extent of support by the vendor

Answer: D

QUESTION 526
Which of the following is one of the key objectives regarding data management roles and responsibilities?

A. Determine data quality metrics.
B. Define important data ownership regardless of functions.
C. Establish data ownership during the final phase of a project.
D. Install data accountability.

Answer: D

QUESTION 527
What BEST describes data ownership?

A. Geographic sovereignty
B. Confidentiality and integrity
C. Accuracy and precision
D. Legal responsibilities

Answer: D
Explanation:

Data ownership is the act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policy implemented by the data owner.

QUESTION 528
A senior security engineer has been tasked with ensuring the confidentiality and integrity of the organization's most valuable personally identifiable information (PII). This data is stored on local file and database servers within the organization's data center. The following security measures have been implemented to ensure that unauthorized access is detected and logged.

```
- Network segmentation and enhanced access logging of the database and file servers
- Implemented encryption of data at rest
- Implemented full packet capture of the network traffic in and out of the sensitive network segment
- Ensured all transaction log data and packet captures are backed up to corporate backup appliance within the corporate backup network segment
```

Which of the following is the MOST likely way to exfiltrate PII while avoiding detection?

A. Unauthorized access to the file server via Secure Shell (SSH)
B. Unauthorized access to the database server via a compromised web application
C. Unauthorized access to the database server via a compromised user account
D. Unauthorized access to the backup server via a compromised service account

Answer: B
Explanation:
According to web results, the most likely way to exfiltrate PII while avoiding detection is to use techniques that anonymize connections to servers, tunnel data over DNS, HTTP, or HTTPS, or use fileless attacks and remote code execution. These methods can help bypass network segmentation, encryption, packet capture, and logging measures. Therefore, the best answer among the given options is B. Unauthorized access to the database server via a compromised web application. This could allow the attacker to execute malicious code on the server and send the data over an encrypted or obfuscated channel to a remote server.

QUESTION 529
During the change management process, which of the following is used to identify and record new risks?

A. Risk assessment
B. Lessons learned register
C. Risk register
D. Risk report

Answer: C

QUESTION 530
The defense strategy 摧ever trust any input?is MOST effective against which of the following web-based system vulnerabilities?

A. Injection vulnerabilities
B. Sensitive data exposure
C. Man-in-the-browser attack
D. Broken authentication

Answer: A

QUESTION 531
What is the MOST effective way to mitigate distributed denial of service (DDoS) attacks?

A. Deploy a web application firewall (WAF).

B. Block access to Transmission Control Protocol (TCP) ports under attack.
C. Detect and block bad Internet Protocol (IP) subnets on the corporate firewall.
D. Engage an upstream Internet service provider (ISP).

Answer: D

QUESTION 532
Which function does 802.1X provide?

A. Network intrusion detection system (NIDS)
B. Wireless access point (WAP)
C. Wi-Fi Protected Access (WPA)
D. Network Access Control (NAC)

Answer: D

QUESTION 533
Which of the following is the PRIMARY benefit of implementing an Information Security Management System (ISMS)?

A. Correlates system events to monitor and demonstrate system health
B. Improves customer confidence by demonstrating adherence to best practices
C. Increases employee education and awareness of security policies
D. Ensures user compliance with computing standards

Answer: B

QUESTION 534
Concerning appropriate data retention policies, which of the following is the MAIN risk factor for the availability of archived information?

A. Data stored in third-party environments.
B. Data maintained offline requires a higher time to access.
C. Data recorded in obsolete media cannot be read.
D. Retention of data involves a cost.

Answer: C

QUESTION 535
Wi-Fi Protected Access 2 (WPA2) is a security protocol designed with which of the following security feature?

A. Encryption control
B. Malware attack protection
C. Data availability
D. Replay attack protection

Answer: A
Explanation:
TKIP is a protection against replay attacks, it is included in WPA and WPA2, the main feature in WPA2 compared to WPA is encryption with AES.

QUESTION 536
What security technique in the Software Development Life Cycle (SDLC) should be leveraged to BEST ensure secure development throughout a project?

A. Dynamic application security testing (DAST)

B. Waterfall
C. Simple Object Access Protocol
D. Static application security testing (SAST)

Answer: D

QUESTION 537
In designing the architecture of an access control system, it was determined that confidentiality and controlled access to information were the primary focus. Which of the following security models is the BEST choice for the organization?

A. Biba integrity model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Brewer-Nash model

Answer: C

QUESTION 538
An organization is developing employee training content to increase awareness of Payment Card Industry (PCI) standards. What are the three types of awareness roles applicable to the organization?

A. All personnel, specialized, management
B. Standard, privileged, administrator
C. Basic, intermediate, advanced
D. Technical, operational, administrative

Answer: A
Explanation:
When developing employee training content to increase awareness of Payment Card Industry (PCI) standards, the three types of awareness roles applicable to the organization are:
All personnel: All employees who handle cardholder data should receive training on PCI compliance requirements, their roles and responsibilities, and how to report security incidents or concerns.
Specialized: Employees with specialized roles, such as IT or security personnel, who are responsible for implementing and maintaining PCI compliance measures, should receive more in-depth training on technical and operational aspects of compliance.
Management: Management-level employees who oversee PCI compliance programs and initiatives should receive training on the overall scope and objectives of compliance, as well as their responsibilities for ensuring compliance across the organization.

QUESTION 539
Which of the following is the BEST method to perform an end-to-end testing on production for both operational and security requirements?

A. Synthetic transaction analysis.
B. Dynamic code analysis
C. Static code analysis
D. Vulnerability analysis

Answer: B

QUESTION 540
A security architect is reviewing an implemented security framework. After the review, the security architect wants to enhance the security by implementing segregation of duties (SoD) to address protection against fraud. Which security model BEST protects the integrity of data?

A. The Brewer-Nash model

B. The Biba Integrity model
C. The Bell-LaPadula model
D. The Clark-Wilson model

Answer: D

QUESTION 541
An organization is building an enterprise system using attribute-based access control (ABAC). To avoid inadvertent exposure, what should organizations do to ensure the proper handling of personally identifiable information (PII) and enforcement of PII regulations across the enterprise?

A. Employ trust agent.
B. Employ trust agreements.
C. Employ training program.
D. Employ regulations from leadership.

Answer: C

QUESTION 542
Which of the following is a strong security protection provided by Trusted Platform Module (TPM)?

A. Providing data integrity through digital signatures
B. Creation of a secure kernel
C. Separation of encryption keys from storage devices
D. Reporting of system integrity

Answer: C

QUESTION 543
An application developer is developing a web application that will store and process personal information of European Union (EU) residents. Which of the following security principles explicitly specified in General Data Protection Regulation (GDPR), should the developer apply to safeguard the personal information in the application?

A. Authorization
B. Tokenization
C. Pseudonymization
D. Authentication

Answer: C

QUESTION 544
A security architect is implementing an authentication system for a distributed network of servers. This network will be accessed by users on workstations that cannot trust the identity of the user. Which solution should the security architect use to have the users trust one another?

A. One-way authentication
B. Kerberos
C. Mutual authentication
D. Single session software tokens

Answer: C

QUESTION 545
Which process compares its results against a standard to determine whether the results meet the standard?

A. Penetration test
B. Security audit
C. Security assessment
D. Functional review

Answer: B

QUESTION 546
A security consultant has been hired by a company to establish its vulnerability management program. The consultant is now in the deployment phase. Which of the following tasks is part of this process?

A. Educate and train key stakeholders.
B. Measure effectiveness of the program's stated goals.
C. Determine a budget and cost analysis for the program.
D. Select and procure supporting technologies.

Answer: D

QUESTION 547
An organization is formulating a strategy to provide access to third-party partners. The information technology (IT) department has been tasked with providing access by utilizing cloud services. Which of the following technologies is MOST commonly employed for completing the task?

A. Identity as a Service (IDaaS)
B. Firewall as a service
C. Infrastructure as a Service (IaaS)
D. Software as a Service (SaaS)

Answer: A

QUESTION 548
Which of the following are key activities when conducting a security assessment?

A. Schedule, collect, examine
B. Interview, examine, simulate
C. Collect, interview, test
D. Examine, interview, test

Answer: D
Explanation:
Assessors may examine, interview and perform direct tests to determine effectiveness of the controls.

QUESTION 549
An organization wants to ensure that employees that move to a different department within the organization do not retain access privileges from their former department. To this end, the organization has implemented role-based access control (RBAC). Which additional measure is MOST important to successfully limit excess access privileges?

A. Business role review
B. Line manager review of assigned roles
C. Segregation of duties (SoD) review
D. Access control matrix

Answer: A
Explanation:
Business role review is the most important additional measure to successfully limit excess access privileges when

implementing RBAC.