Vendor: ISC

Exam Code: CISSP

Exam Name: Certified Information Systems Security Professional

Version: DEMO

QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**