BCS

CISMP-V9

Foundation Certificate in Information Security Management Principles V9.0

Question: 784

In the context of file transfers, which of the following protocols is most commonly recommended for secure file transmission over the internet?

A. FTP
B. SFTP
C. TFTP
D. HTTP

Answer: B

Explanation: SFTP (Secure File Transfer Protocol) provides a secure channel for transferring files over a network, incorporating encryption for data protection during transmission.

Question: 785

In the context of national and international information security standards, which of the following sources is most authoritative for current best practices and compliance requirements, especially for organizations looking to align with global benchmarks?

A. National Institute of Standards and Technology (NIST)
B. Internet Engineering Task Force (IETF)
C. International Organization for Standardization (ISO)
D. International Electrotechnical Commission (IEC)

Answer: C

Explanation: The International Organization for Standardization (ISO) is the most authoritative source for global standards, including those related to information security. ISO standards are widely recognized and adopted internationally, providing a framework for organizations to manage their information security.

Question: 786

When considering vulnerabilities in procedures, which of the following practices is most likely to lead to a critical security incident?

A. Regular staff training on security best practices
B. Frequent software updates
C. Lack of incident response procedures
D. Strong password policies

Answer: C

Explanation: A lack of incident response procedures can lead to inadequate handling of security incidents, exacerbating their impact.

Question: 787

Which of the following statements best captures the importance of maintaining an accurate and current inventory of physical access controls?

A. It helps in tracking employee performance
B. It is only necessary during audits
C. It ensures accountability and enhances security posture
D. It complicates the access process for employees

Answer: C

Explanation: Maintaining an accurate inventory of physical access controls ensures accountability and enhances security posture by allowing for effective monitoring and management of access rights.

Question: 788

Which of the following statements best describes the vulnerabilities associated with the Internet of Things (IoT) in terms of accidental threats?

A. Poor software design in IoT devices can lead to unforeseen vulnerabilities.
B. IoT devices are inherently secure and pose minimal risk.
C. IoT devices are primarily targeted by external malicious actors.
D. All IoT devices have robust security protocols in place.

Answer: A

Explanation: Poor software design in IoT devices can lead to significant vulnerabilities, making them susceptible to accidental threats and potential exploitation by attackers.

Question: 789

What is a significant risk when relying on third-party forensic services for investigations?

A. Potential for miscommunication leading to incomplete investigations
B. Enhanced expertise and resources available from external vendors
C. Increased speed in data recovery and analysis
D. Assurance of confidentiality in all communications

Answer: A

Explanation: Potential for miscommunication leading to incomplete investigations is a significant risk, as differences in understanding or expectations can hinder the effectiveness of the forensic process.

Question: 790

In relation to COTS systems, which of the following security issues is most likely to arise during the integration phase?

A. Lack of user training
B. Vendor lock-in
C. Insufficient vendor support
D. Incompatibility with existing security policies

Answer: D

Explanation: During integration, COTS systems may not align with existing security policies, leading to potential vulnerabilities and compliance issues.

Question: 791

Which of the following best illustrates the concept of "social engineering" as a deliberate threat?

A. A hacker exploiting a software vulnerability
B. An employee unknowingly disclosing information to a scammer posing as IT support
C. A business partner accidentally sharing confidential data
D. A natural disaster disrupting business operations

Answer: B

Explanation: Social engineering involves manipulating individuals into divulging confidential information, often by posing as someone trustworthy, exemplifying a deliberate threat.

Question: 792

Regarding common public key infrastructures (PKI), which of the following trust models is characterized by a hierarchical structure where a root CA (Certificate Authority) issues certificates to subordinate CAs?

A. Hierarchical Trust Model
B. Two-way Trust
C. Web of Trust
D. Peer-to-Peer Trust

Answer: A

Explanation: The Hierarchical Trust Model is defined by a root CA that issues certificates to subordinate CAs, creating a structured approach to managing trust in digital communications.

Question: 793

When developing a service continuity plan, which factor is critical to ensuring that the plan remains effective in the face of evolving threats?

A. Comprehensive training for all employees
B. Regular testing and updates of the plan
C. Detailed documentation of procedures
D. Engagement of external consultants

Answer: B

Explanation: Regular testing and updates of the service continuity plan are critical for ensuring its effectiveness against evolving threats, as this allows organizations to adapt and improve their strategies accordingly.

Question: 794

In what manner does the alignment of information security with business strategy contribute to organizational success?

A. It creates silos within the organization
B. It ensures that security initiatives support and enable business objectives
C. It complicates decision-making processes
D. It focuses solely on compliance with regulations

Answer: B

Explanation: Aligning information security with business strategy ensures that security initiatives effectively support and enable business objectives, contributing to overall organizational success.

Question: 795

In terms of policy enforcement, which of the following practices is most effective for ensuring compliance across the organization?

A. Establishing a culture of fear around policy violations
B. Relying on self-reporting without verification
C. Implementing regular audits and assessments with clear consequences for non-compliance
D. Only penalizing high-profile employees to deter violations

Answer: C

Explanation: Implementing regular audits and assessments with clear consequences for non-compliance helps ensure accountability and promotes a culture of adherence to security policies.

Question: 796

During a security risk assessment, which of the following factors is LEAST likely to influence the evaluation of a potential risk?

A. The historical data of similar incidents affecting the organization.
B. The opinions of IT staff regarding the effectiveness of current controls.
C. The organization's overall business strategy and objectives.
D. The potential impact on the organization’s brand and reputation.

Answer: B

Explanation: While IT staff opinions are valuable, they are less influential than objective historical data, business strategy, and brand impact when evaluating risks.

Question: 797

Which of the following is a key advantage of having a well-defined information security policy in place?

A. It eliminates the need for any other security measures
B. It provides a framework for consistent decision-making and accountability in security practices
C. It simplifies the security landscape by focusing only on technical controls
D. It allows for the complete delegation of security responsibilities to external parties

Answer: B

Explanation: A well-defined information security policy provides a framework for consistent decision-making and accountability, guiding the organization's security practices effectively.

Question: 798

When configuring intrusion prevention systems (IPS), which of the following strategies would most effectively enhance detection capabilities against sophisticated attacks?

A. Implementing signature-based detection only
B. Combining both signature and anomaly-based detection methods
C. Relying solely on anomaly-based detection
D. Disabling logging to improve performance

Answer: B

Explanation: Combining both signature and anomaly-based detection methods allows the IPS to effectively identify known attacks while also detecting unusual patterns that may indicate sophisticated, previously unknown threats.

Question: 799

Which factor is critical in determining the appropriate level of security clearance required for employees handling sensitive information?

A. The employee's tenure with the organization

B. The sensitivity level of the information and the employee's role
C. The employee’s personal interests and qualifications
D. The employee's previous job performance evaluations

Answer: B

Explanation: The appropriate level of security clearance is determined by the sensitivity of the information and the employee's role, ensuring that access is granted appropriately.

Question: 800

When assessing the risks associated with social media, which of the following sources is most likely to lead to an accidental data breach within an organization?

A. Trusted partner sharing sensitive information
B. Internal employee posting confidential data
C. Weak procedures and processes in data handling
D. Managed services failing to secure third-party access

Answer: B

Explanation: Internal employees posting confidential data on social media can inadvertently lead to data breaches, demonstrating the risks associated with personal disclosures online.

Question: 801

What is the most critical factor in ensuring the ongoing relevance of documentation related to security and incident response plans?

A. Limiting access to the documentation to upper management only.
B. Regularly reviewing and updating the documentation based on lessons learned from incidents.
C. Creating documentation solely for compliance purposes.
D. Avoiding changes to the documentation to maintain consistency.

Answer: B

Explanation: Regularly reviewing and updating documentation based on lessons learned from incidents ensures that it remains relevant and effective in guiding responses to future incidents.

Question: 802

When considering the implementation of ISA/IEC 62443 standards, which of the following key aspects should organizations prioritize to enhance their industrial control system security?

A. Employee training and awareness programs
B. Secure software development lifecycle
C. Risk assessment and management processes

D. Network segmentation and access control

Answer: D

Explanation: ISA/IEC 62443 emphasizes the importance of network segmentation and access control to protect industrial control systems from cybersecurity threats. Proper segmentation helps limit access and reduces the attack surface.

Question: 803

Which of the following statements best describes the purpose of a risk register in the risk management process?

A. To serve as a historical document for audits
B. To provide a comprehensive overview of identified risks and their management
C. To eliminate all identified risks
D. To communicate risks solely to senior management

Answer: B

Explanation: A risk register is a vital tool that provides an overview of identified risks, their assessment, and management strategies, facilitating informed decision-making.

Question: 804

As part of a secure network management strategy, an organization conducts periodic mapping of its network infrastructure. Which of the following is the primary purpose of this practice?

A. To ensure all devices are updated with the latest software
B. To maintain compliance with regulatory requirements
C. To identify and eliminate unused devices
D. To visualize network performance metrics

Answer: C

Explanation: Periodic mapping of the network infrastructure helps identify and eliminate unused devices, reducing the attack surface and enhancing overall security.

Question: 805

In the context of modern business models such as cloud computing and outsourcing, how does information security contribute to the protection of business assets while facilitating new opportunities and innovation?

A. By creating barriers that limit business expansion
B. By ensuring compliance with outdated regulations

C. By focusing solely on physical asset protection
D. By integrating security measures that enhance trust and reduce risk

Answer: D

Explanation: Information security enhances trust and reduces risk by integrating security measures that align with new business models, enabling organizations to innovate while protecting valuable assets.

Question: 806

When considering the need for secure off-site storage of sensitive data, which of the following is the most critical factor to ensure data integrity and availability?

A. The reputation of the storage provider.
B. The cost of the storage solution.
C. The physical security of the storage facility.
D. The distance of the storage site from the primary location.

Answer: C

Explanation: The physical security of the storage facility is the most critical factor in ensuring data integrity and availability, as it protects sensitive data from theft or damage.

Question: 807

In the context of security testing, which of the following practices is essential for ensuring the validity and reliability of test results?

A. Conducting tests without informing stakeholders
B. Using a consistent testing methodology
C. Relying solely on external consultants for testing
D. Performing tests only on new systems

Answer: B

Explanation: Using a consistent testing methodology ensures that test results are valid and reliable, allowing for meaningful comparisons and assessments of security posture over time.

Question: 808

Which vulnerability type, when associated with email systems, poses a significant risk of confidentiality breaches through phishing attacks?

A. Hardware vulnerabilities
B. Weaknesses in software
C. Procedures

D. People vulnerabilities

Answer: D

Explanation: People vulnerabilities, such as employees falling victim to phishing attacks, can lead to significant confidentiality breaches.

Question: 809

In the context of security incident management, what is the primary function of a post-incident review?

A. To assign blame for the incident
B. To evaluate the effectiveness of the response and identify areas for improvement
C. To create a public relations strategy
D. To ensure that all employees are aware of the incident

Answer: B

Explanation: A post-incident review evaluates the effectiveness of the response and identifies lessons learned, which are crucial for enhancing future incident management processes.