ISC2 CISSP Mock Exam

Shared by Long on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the BEST reason to include supply chain risks in a corporate risk register?

Options:

A- Risk registers help fund corporate supply chain risk management (SCRM) systems.
B- Risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite.
C- Risk registers can be used to illustrate residual risk across the company.
D- Risk registers allow for the transfer of risk to third parties.

Answer:

B

Explanation:

The best reason to include supply chain risks in a corporate risk register is that risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite. A risk register is a tool for documenting and managing risks across an organization. A risk register typically includes information such as risk identification, risk analysis, risk evaluation, risk treatment, risk monitoring and review. By including supply chain risks in a risk register, an organization can identify the sources and impacts of the risks, assess their likelihood and severity, evaluate their acceptability, implement appropriate controls, and monitor their effectiveness. A risk register can also help an organization to align its supply chain risk management with its overall risk management strategy and objectives. A risk register does not help fund corporate SCRM systems, as it is not a budgeting tool. A risk register does not illustrate residual risk across the company, as it does not show the risk level after applying controls. A risk register does not allow for the transfer of risk to third parties, as it does not assign risk ownership or responsibility.Reference:Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 1: Security and Risk Management, page 72.

Question 2

Question Type: MultipleChoice

What is the HIGHEST priority in agile development?

Options:

A- Selecting appropriate coding language
B- Managing costs of product delivery
C- Early and continuous delivery of software
D- Maximizing the amount of code delivered

Answer:

C

Explanation:

The highest priority in agile development is early and continuous delivery of software. Agile development is a type of software development methodology that is based on the principles of the Agile Manifesto, which values individuals and interactions, working software, customer collaboration, and responding to change. Agile development aims to deliver software products or services that meet the changing needs and expectations of the customers and stakeholders, by using an iterative, incremental, and collaborative approach. Agile development involves various methods or frameworks, such as Scrum, Kanban, or Extreme Programming. The highest priority in agile development is early and continuous delivery of software, as stated in the first principle of the Agile Manifesto: 'Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.' Early and continuous delivery of software means that the software products or services are delivered to the customers or stakeholders in short and frequent cycles, rather than in long and infrequent cycles. Early and continuous delivery of software can help to improve the quality and value of the software products or services, by enabling faster feedback, validation, and verification of the software products or services, as well as by allowing more flexibility and adaptability to the changing requirements and preferences of the customers or stakeholders. Selecting appropriate coding language, managing costs of product delivery, or maximizing the amount of code delivered are not the highest priorities in agile development, as they are either more related to the technical, financial, or quantitative aspects of software development, rather than the customer-oriented or value-driven aspects of software development.Reference:CISSP All-in-One Exam Guide, Eighth Edition, Chapter 21: Software Development Security, page 1155;CISSP Official (ISC)2 Practice Tests, Third Edition, Domain 8: Software Development Security, Question 8.11, page 305.

Question 3

Question Type: MultipleChoice

At what stage of the Software Development Life Cycle (SDLC) does software vulnerability remediation MOST likely cost the least to implement?

Options:

A- Development
B- Testing
C- Deployme
D- Design

Answer:

D

Explanation:

Software vulnerability remediation is the process of identifying and fixing the weaknesses or flaws in a software application or system that could be exploited by attackers. Software vulnerability remediation is most likely to cost the least to implement at the design stage of the Software Development Life Cycle (SDLC), which is the phase where the requirements and specifications of the software are defined and the architecture and components of the software are designed. At this stage, the software developers can apply security principles and best practices, such as secure by design, secure by default, and secure coding, to prevent or minimize the introduction of vulnerabilities in the software. Remediation at the design stage is also easier and cheaper than at later stages, such as development, testing, or deployment, because it does not require modifying or rewriting the existing code, which could introduce new errors or affect the functionality or performance of the software.Reference:CISSP All-in-One Exam Guide, Eighth Edition, Chapter 21: Software Development Security, pp. 2021-2022; [Official (ISC)2 CISSP CBK Reference, Fifth Edition], Domain 8: Software Development Security, pp. 1395-1396.

Question 4

Question Type: MultipleChoice

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

Options:

A- The actual origin and tools used for the test can be hidden.
B- Information may be found on related breaches and hacking.
C- Vulnerabilities can be tested without impact on the tested environment.
D- Information may be found on hidden vendor patches.

Answer:

B

Explanation:

The way that navigating the dark web can add value to a penetration test when assessing web vulnerabilities is that information may be found on related breaches and hacking. The dark web is a part of the internet that is not indexed or accessible by conventional search engines or browsers, and that requires special software or tools, such as Tor or I2P, to access. The dark web is often used for illegal or malicious activities, such as selling or buying drugs, weapons, or stolen data, or sharing or exchanging hacking tools, techniques, or information. Navigating the dark web can add value to a penetration test when assessing web vulnerabilities, as it can help to find information on related breaches and hacking, such as the vulnerabilities, exploits, or attacks that have been used or disclosed by hackers or cybercriminals against the target system or organization, or the data or credentials that have been stolen or compromised from the target system or organization. This information can help to identify or verify the existing or potential web vulnerabilities, to evaluate or prioritize the web vulnerabilities, or to simulate or replicate the web vulnerabilities or attacks. The actual origin and tools used for the test can be hidden, vulnerabilities can be tested without impact on the tested environment, or information may be found on hidden vendor patches are not the ways that navigating the dark web can add value to a penetration test when assessing web vulnerabilities, as they are not true or relevant. The actual origin and tools used for the test cannot be hidden by navigating the dark web, as this is not a function or a feature of the dark web. The actual origin and tools used for the test can be hidden by using other techniques or methods, such as proxy servers, virtual private networks, or encryption. Vulnerabilities cannot be tested without impact on the tested environment by navigating the dark web, as this is not a purpose or a benefit of the dark web. Vulnerabilities can be tested without impact on the tested environment by using other techniques or methods, such as sandboxing, virtualization, or simulation. Information on hidden vendor patches cannot be found by navigating the dark web, as this is not a type or a source of information that is available or accessible on the dark web. Information on hidden vendor patches can be found by using other techniques or methods, such as reverse engineering, vulnerability scanning, or vendor disclosure.Reference:Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 21: Software Development Security, page 2034.

Question 5

Question Type: MultipleChoice

If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

Options:

A- Classless Inter-Domain Routing (CIDR)
B- Deterministic routing
C- Internet Protocol (IP) routing lookups
D- Boundary routing

Answer:

B

Explanation:

If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), deterministic routing becomes even more essential to the assurance of network. WAN is a network that spans a large geographic area, such as a country or a continent, and connects multiple local area networks (LANs) or other networks. WAN is used to transmit data, voice, or video over long distances, using various technologies, such as leased lines, packet switching, or circuit switching. VoIP is a technology that enables the delivery of voice communications over IP networks, such as the internet or WANs. VoIP converts the analog voice signals into digital packets, and transmits them over the IP networks, using various protocols, such as Session Initiation Protocol (SIP) or Real-time Transport Protocol (RTP). Deterministic routing is a routing technique that ensures that the packets are always sent along the same path or route between the source and destination devices. Deterministic routing can provide the following benefits for the WAN that supports VoIP:

It can improve the quality and reliability of the voice communications, as the packets are always delivered in the same order and with the same delay, avoiding issues such as packet loss, jitter, or latency.

It can enhance the security and privacy of the voice communications, as the packets are always routed through the same trusted and secure devices, avoiding the exposure or interception by unauthorized or malicious devices.

It can simplify the management and troubleshooting of the network, as the network administrators can easily monitor and control the network traffic and performance, and identify

and resolve any problems or errors.Reference:CISSP All-in-One Exam Guide, Chapter 4: Communication and Network Security, Section: Wide Area Networks, pp. 191-192.

Question 6

Question Type: MultipleChoice

Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

Options:

A- Mobile Device Management (MDM) with device wipe
B- Whole device encryption with key escrow
C- Virtual private network (VPN) with traffic encryption
D- Mobile device tracking with geolocation

Answer:

A

Explanation:

The feature that is most effective in mitigating against theft of data on a corporate mobile device which has been stolen is Mobile Device Management (MDM) with device wipe. MDM is a security technique that involves managing and securing the mobile devices that are used by the users or employees of an organization, and enforcing the security policies and standards of the organization on the mobile devices. MDM can provide the feature of device wipe, which is the ability to remotely erase or delete the data and information stored on the mobile device, in case the mobile device is lost or stolen.MDM with device wipe can mitigate against theft of data on a corporate mobile device which has been stolen, as it can prevent or reduce the unauthorized access, disclosure, or compromise of the data and information on the mobile device34.Reference:CISSP CBK, Fifth Edition, Chapter 4, page 378;2024 Pass4itsure CISSP Dumps, Question 18.

Question 7

Question Type: MultipleChoice

Which of the following is a risk matrix?

Options:

A- A database of risks associated with a specific information system.
B- A table of risk management factors for management to consider.
C- A two-dimensional picture of risk for organizations, products, projects, or other items of interest.
D- A tool for determining risk management decisions for an activity or system.

Answer:

C

Explanation:

A risk matrix is a graphical tool that helps visualize and prioritize the risks associated with a specific context, such as an organization, a product, a project, or an activity. A risk matrix typically plots the likelihood of a risk occurring on one axis and the impact of the risk on the other axis. The resulting matrix is divided into cells that indicate the level of risk for each combination of likelihood and impact. The level of risk can be color-coded or labeled as low, medium, high, or extreme. A risk matrix can help identify the most significant risks that need to be addressed or mitigated.Reference:Official (ISC)2 CISSP CBK Reference, Chapter 1: Security and Risk Management, Section: Risk Management Concepts, pp. 43-44.

Question 8

Question Type: MultipleChoice

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

Options:

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

Explanation:

The primary difference between security policies and security procedures is that policies are generic in nature, and procedures contain operational details. Security policies are the high-level statements or rules that define the goals, objectives, and requirements of security for an organization. Security procedures are the low-level steps or actions that specify how to implement, enforce, and comply with the security policies.

A . Policies are used to enforce violations, and procedures create penalties is not a correct answer, as it confuses the roles and functions of policies and procedures. Policies are used to create penalties, and procedures are used to enforce violations. Penalties are the consequences or sanctions that are imposed for violating the security policies, and they are defined by the policies. Enforcement is the process or mechanism of ensuring compliance with the security policies, and it is carried out by the procedures.

B . Policies point to guidelines, and procedures are more contractual in nature is not a correct answer, as it misrepresents the nature and purpose of policies and procedures. Policies are not merely guidelines, but rather mandatory rules that bind the organization and its stakeholders to follow the security principles and standards. Procedures are not contractual in nature, but rather operational in nature, as they describe the specific tasks and activities that are necessary to achieve the security goals and objectives.

C . Policies are included in awareness training, and procedures give guidance is not a correct answer, as it implies that policies and procedures have different audiences and functions. Policies and procedures are both included in awareness training, and they both give guidance. Awareness training is the process of educating and informing the organization and its stakeholders about the security policies and procedures, and their roles and responsibilities in security. Guidance is the process of providing direction and advice on how to comply with the security policies and procedures, and how to handle security issues and incidents.

Question 9

Question Type: MultipleChoice

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?

Options:

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

Explanation:

WPA2 is a security protocol that encrypts the data sent over wireless networks. It provides stronger protection than WEP or WPA, which are older and weaker protocols. WPA2 prevents unauthorized access to the wireless network and ensures the confidentiality of the information transmitted. Configuring the APs to use WPA2 is a logical control that can reduce the risk of wireless eavesdropping or interception outside the campus area. Reference: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 5: Communication and Network Security, page 237. CISSP Practice Exam Questions and Answers in 2023, Question 14.

Question 10

Question Type: MultipleChoice

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

Options:

A- Application authentication
B- Input validation
C- Digital signing
D- Device encryption

Answer:

C

Explanation:

The technique that an organization should use to assure application integrity is digital signing. Digital signing is a technique that uses cryptography to generate a digital signature for a message or a document, such as an application. The digital signature is a value that is derived from the message and the sender's private key, and it can be verified by the receiver using the sender's public key. Digital signing can help to assure application integrity, which means that the application has not been altered or tampered with during the transmission or storage. Digital signing can also help to assure application authenticity, which means that the application originates from the legitimate source. Application authentication, input validation, and device encryption are not techniques that can assure application integrity, but they can help to assure application security, usability, or confidentiality, respectively.Reference:CISSP All-in-One Exam Guide, Eighth Edition, Chapter 5: Security Engineering, page 607;Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 3: Security Architecture and Engineering, page 388.