MSiS Test 1 Practice (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Questions

1. **What security strategy at the organizational level identifies threats the organization might face?**

   A. Risk assessment

   B. Incident response

   C. Vulnerability analysis

   D. Compliance auditing

2. **Which of the following is an approach used to mitigate risks in information systems?**

   A. Avoidance strategies

   B. Compliance with regulations

   C. Leakage detection

   D. Inter-department collaboration

3. **How many types of end user agreements are typically recognized?**

   A. Two

   B. Three

   C. Four

   D. Five

4. **A significant difference in which aspect allows data to zip through a 5G network much faster than a 4G network?**

   A. Gbps

   B. Device support

   C. Bandwidth

   D. Latency

5. **What role do stakeholders play in project management?**

   A. They are responsible for the technical execution of the project

   B. They are individuals or groups influencing the project's success

   C. They manage the project team's performance directly

   D. They determine the project's budget and timeline

6. **What type of network allows for the central management of configurations and policies?**

    A. Peer-to-peer network

    B. Software-defined network

    C. Client-server network

    D. Wireless network

7. **Which type of network connects users and resources across wider geographical areas?**

    A. Extranet

    B. Intranet

    C. Local area network

    D. Wide area network

8. **Which statement regarding mainframe computers is NOT accurate?**

    A. Provides capacity for massive data processing

    B. Features backward compatibility

    C. Supports dozens or hundreds of users

    D. Typical of being a single user computer

9. **Which statement is FALSE regarding website creation?**

    A. Hannah can purchase and use specialized software to create her site.

    B. Hannah must set up a server computer before publishing her Web site.

    C. If Hannah knows how, she can code her site using a plain text editor.

    D. Hannah can hire someone to design and build her Web site for her.

10. **What is the main goal of network security?**

    A. To increase internet speed

    B. To ensure compliance with regulations

    C. To protect networks from unauthorized access

    D. To provide customer support

Answers

1. A
2. A
3. B
4. D
5. B
6. B
7. D
8. D
9. B
10. C

Explanations

1. What security strategy at the organizational level identifies threats the organization might face?

A. Risk assessment

B. Incident response

C. Vulnerability analysis

D. Compliance auditing

The security strategy that identifies threats the organization might face is risk assessment. This process involves systematically analyzing potential risks, including threats and vulnerabilities that could adversely impact the organization. By conducting a risk assessment, an organization gains insights into various potential hazards, enabling it to prioritize risks based on their likelihood and potential impact. This understanding allows for the implementation of appropriate mitigation strategies to protect the organization's assets and ensure business continuity. Risk assessments also involve evaluating existing controls and how effective they are in mitigating the identified risks. This makes it possible for organizations to make informed decisions about resource allocation, ensuring that they address the most critical threats effectively. Ultimately, risk assessment serves as a foundational step in developing a comprehensive security strategy.

2. Which of the following is an approach used to mitigate risks in information systems?

A. Avoidance strategies

B. Compliance with regulations

C. Leakage detection

D. Inter-department collaboration

Avoidance strategies are a fundamental approach in risk management for information systems, where the goal is to eliminate the risk entirely before it can cause harm. This can involve changing processes or practices to sidestep potential threats. For example, an organization may decide to discontinue using a particular system or technology that poses significant vulnerabilities, thus removing the associated risks. While compliance with regulations is crucial for ensuring that organizations meet legal and industry standards, it doesn't actively eliminate risks but rather helps manage them within the boundaries of those regulations. Leakage detection is focused on identifying potential data breaches or losses after they have happened, which is more reactive than proactive. Inter-department collaboration is beneficial for enhancing communication and sharing information about risks, but it does not directly address risk mitigation on its own. Avoidance strategies distinctly address and mitigate risks by opting for safer alternatives, making it a proactive method.

3. How many types of end user agreements are typically recognized?

A. Two

B. Three

C. Four

D. Five

The correct answer is that there are typically three types of end user agreements recognized. These agreements are critical in defining the relationship between software providers and users. The three primary types usually identified are: 1. **End User License Agreement (EULA)**: This is a legal contract between the software developer or publisher and the user, which outlines how the software can be used. It typically covers rights related to installation, usage limitations, and liabilities. 2. **Terms of Service (ToS)**: This agreement governs the use of a service, particularly online services. It includes terms related to acceptable behavior, user rights, and service guarantees, which are essential for platforms that provide accessible services over the internet. 3. **Privacy Policy**: While not always classified strictly as an end user agreement in the same context as the first two, it is nonetheless essential. It informs users about how their personal data will be collected, used, and protected, which is increasingly important in the context of data privacy laws. Recognizing these three types is important because they help users understand their rights and obligations when using software or online services. Each serves a distinct purpose and together, they provide a comprehensive framework for user agreements in the digital landscape.

4. A significant difference in which aspect allows data to zip through a 5G network much faster than a 4G network?

A. Gbps

B. Device support

C. Bandwidth

D. Latency

The significant difference that allows data to zip through a 5G network much faster than a 4G network is latency. Latency refers to the time it takes for data to travel from the source to the destination and back again. In 5G networks, this latency is dramatically reduced compared to 4G networks, enabling faster response times and more instantaneous communication. Lower latency enhances the performance of applications that require real-time data exchange, such as online gaming, autonomous vehicles, and remote surgery. While factors like bandwidth, which refers to the amount of data transmitted over a network in a given time, and Gbps, which is a measure of speed, are important, they do not directly explain the speed advantage of 5G in terms of real-time interaction. Device support also plays a role in the overall experience of a network but does not fundamentally change the speed characteristics associated with latency.

5. What role do stakeholders play in project management?

A. They are responsible for the technical execution of the project

B. They are individuals or groups influencing the project's success

C. They manage the project team's performance directly

D. They determine the project's budget and timeline

Stakeholders are vital to the success of any project as they are individuals or groups who have an interest in or may be affected by the project's outcomes. They can include a wide range of people, from project sponsors and team members to customers and regulatory bodies. Their influence can shape various aspects of the project, including its scope, budget, and overall direction. Understanding the needs and expectations of stakeholders is essential for effective communication and engagement throughout the project lifecycle. Their feedback and involvement can guide project decisions and help identify potential challenges early on, thereby ensuring that the project aligns with their interests and ultimately achieves greater success. The other options focus on specific roles or responsibilities that do not encompass the broader influence stakeholders have on a project. For example, while stakeholders can impact decisions regarding budget and timeline, they are not solely responsible for managing the project, executing technical tasks, or directly managing team performance. Instead, project managers typically handle those responsibilities while remaining attuned to stakeholder input and expectations.

6. What type of network allows for the central management of configurations and policies?

A. Peer-to-peer network

B. Software-defined network

C. Client-server network

D. Wireless network

A software-defined network (SDN) is specifically designed to centralize the management of configurations and policies through a controller that can dynamically adjust the flow of data across the network. This central control enables network administrators to manage traffic and apply policies without needing to make manual adjustments on individual devices. In an SDN, the control plane is separated from the data plane, allowing for greater flexibility and automation in network management. Administrators can implement changes across the entire network quickly, responding to differing traffic demands or security needs in real-time. This contrasts with other network types where management can be more distributed or reliant on individual components, making SDN particularly advantageous for environments that require rapid adaptation and streamlined management procedures. Peer-to-peer networks do not have a centralized management system, while client-server networks depend heavily on a central server existing in a more traditional architecture, lacking the dynamic capabilities of an SDN. Wireless networks can be managed centrally, but that doesn't inherently imply the software-defined nature or centralized configuration management that characterizes SDNs.

7. Which type of network connects users and resources across wider geographical areas?

A. Extranet

B. Intranet

C. Local area network

D. Wide area network

The correct answer highlights the function of a wide area network (WAN), which is designed to connect users and resources over large geographical areas, often spanning cities, countries, or even continents. WANs utilize a variety of transmission technologies to facilitate this connectivity, such as leased telecommunication lines, satellite links, and other means of data transmission. This enables organizations to maintain communication and resource sharing among multiple locations, making it a crucial system for businesses and individuals who require access to data and applications across vast distances. In contrast, options like the intranet and local area network (LAN) serve more localized purposes. An intranet is a private network that allows access within an organization, while a LAN connects devices within a limited area, such as a single building or campus. An extranet grants controlled access to external users but typically remains within the confines of the organization's existing network. Each of these alternatives focuses on connectivity in smaller, more localized networks, making them unsuitable for connections across broader geographical spans that a WAN specifically addresses.

8. Which statement regarding mainframe computers is NOT accurate?

A. Provides capacity for massive data processing

B. Features backward compatibility

C. Supports dozens or hundreds of users

D. Typical of being a single user computer

Mainframe computers are designed to handle large volumes of data and process it efficiently. They provide significant capacity for massive data processing, making them well-suited for tasks such as transaction processing and analytics. Backward compatibility is a critical feature of mainframe systems. This means that older software applications can still run on newer mainframe models, which helps organizations upgrade their systems without losing access to their existing applications. Mainframes are engineered to support dozens, hundreds, or even thousands of users simultaneously. This multi-user capability is essential for large organizations that rely on mainframes for business-critical operations. In contrast, describing a mainframe as a typical single user computer is inaccurate. Mainframes are not designed for a single user; they serve as centralized systems that provide services to multiple users at once, emphasizing their ability to manage concurrent processing and extensive workloads. Thus, the statement that mainframes are typical of being a single-user computer is the one that does not accurately reflect the characteristics of these powerful computing systems.

9. Which statement is FALSE regarding website creation?

A. Hannah can purchase and use specialized software to create her site.

B. Hannah must set up a server computer before publishing her Web site.

C. If Hannah knows how, she can code her site using a plain text editor.

D. Hannah can hire someone to design and build her Web site for her.

The statement that Hannah must set up a server computer before publishing her website is inaccurate. In reality, setting up a server computer is not a requirement for individuals looking to publish a website. Instead, many individuals use web hosting services that provide the necessary infrastructure to host a website without needing to maintain their own physical server. These hosting services manage the server-side operations, allowing users to focus on creating and managing their website content. The other statements are true: specialized software can indeed simplify the website creation process; coding can be done directly in a text editor for those with the necessary skills; and hiring a professional web designer or developer is a common practice to ensure a polished and functional website.

10. What is the main goal of network security?

A. To increase internet speed

B. To ensure compliance with regulations

C. To protect networks from unauthorized access

D. To provide customer support

The primary goal of network security is to protect networks from unauthorized access, ensuring that sensitive data and resources are safeguarded against potential threats. This encompasses a variety of measures, including the implementation of firewalls, intrusion detection systems, and encryption technologies, all aimed at preventing unauthorized users from gaining access to networked systems. By focusing on safeguarding the integrity, confidentiality, and availability of data, network security plays a crucial role in maintaining the trustworthiness of an organization's information systems. While increasing internet speed, ensuring compliance with regulations, and providing customer support are important aspects of managing IT networks, they do not directly address the core purpose of network security. The essence of network security lies in creating a robust defense against cyber threats, thereby protecting organizational assets from malicious activities.