CC - Certified in Cybersecurity Exam (200 Questions) - Results

Question 1: **Correct**

What is the primary difference between signature-based detection and behavioral-based detection in an Intrusion Detection System (IDS)?

- **Signature-based detection relies on pre-configured rules, while behavioral-based detection uses machine learning to detect abnormal behavior.**
- **Signature-based detection looks for known patterns of malicious behavior, while behavioral-based detection looks for abnormal behavior patterns.**
- **(Correct)**
- **Behavioral-based detection can only be used for network-based IDS.**
- **Signature-based detection is more accurate than behavioral-based detection.**

Explanation

Signature-based detection relies on pre-configured rules that look for known patterns of malicious behavior, while behavioral-based detection looks for abnormal behavior patterns that deviate from what is considered normal

activity. While signature-based detection can be more accurate in identifying known threats, behavioral-based detection can help detect unknown threats that may not have a pre-configured signature.

Question 2: **Skipped**

Which of the following is NOT a benefit of network segmentation?

- **Better compliance with regulatory requirements**
- **Improved network security**
- **Easier network management**
- **(Correct)**
- **Increased network performance**

Explanation

Network segmentation can make network management more complex, as there are more subnetworks to manage. However, the benefits of improved security, compliance, and performance usually outweigh this added complexity.

Question 3: **Skipped**

Which layer of the OSI model is responsible for routing and forwarding data packets between different networks?

- **Network layer**
- **(Correct)**

- **Data Link layer**
- **Transport layer**
- **Application layer**

Explanation

The Network layer of the OSI model is responsible for routing and forwarding data packets between different networks.

Question 4: **Skipped**

What is the main objective of the General Data Protection Regulation (GDPR)?

- **To regulate the use of personal data**
- **To enforce the right to be forgotten**
- **To prevent the unauthorized sharing of personal information**
- **To protect the privacy of European citizens**
- **(Correct)**

Explanation

The General Data Protection Regulation (GDPR) was created to protect the privacy of European citizens. Its main objective is to ensure that the personal data of European citizens is protected and handled responsibly. It regulates the use of personal data, prevents unauthorized

sharing of personal information, and enforces the right to be forgotten.

Question 5: **Skipped**

In an organization that uses Mandatory Access Control (MAC), a user wants to access a file that has been classified as "Top Secret". What level of clearance does the user need to access the file?

- **The user needs to have a clearance level equal to or higher than "Top Secret".**
- **(Correct)**
- **The user cannot access the file.**
- **The user needs to have a "Top Secret" clearance.**
- **The user needs to have a clearance level lower than "Top Secret".**

Explanation

In a Mandatory Access Control (MAC) system, access control is determined by a central authority based on predefined policies. The policies typically specify the clearance level required to access a resource. In this case, the user needs to have a clearance level equal to or higher than "Top Secret" to access the file.

Question 6: **Skipped**

What are the types of alarms used in physical security?

- **All of the above**
- **(Correct)**
- **Panic alarms**
- **Burglar alarms**
- **Fire alarms**

Explanation

Physical security systems use a variety of alarms to alert authorities of different types of potential threats. Fire alarms are used to alert authorities of a potential fire, burglar alarms are used to alert authorities of a potential intrusion, and panic alarms are used to alert authorities of an emergency situation where immediate assistance is required. All of these types of alarms play a critical role in maintaining the security of a secure area.

Question 7: **Skipped**

Which cloud service model provides the most flexibility and control over the underlying infrastructure?

- **All options**
- **Infrastructure as a Service (IaaS)**
- **(Correct)**
- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**

Explanation

Infrastructure as a Service (IaaS) provides the most flexibility and control over the underlying infrastructure, as users have direct access to virtualized computing resources such as servers, storage, and networking. SaaS and PaaS provide higher-level abstractions that can make it easier to develop and deploy applications, but they do not offer the same level of control over the underlying infrastructure.

Question 8: **Skipped**

What is a containment plan in the context of incident response?

- **A plan for containing the spread of an incident.**
- **(Correct)**
- **A plan for containing the spread of a fire.**
- **A plan for containing the spread of a virus.**
- **A plan for containing the spread of an environmental hazard.**

Explanation

A containment plan in the context of incident response is a documented process that outlines the steps that an organization will take to contain the spread of an incident,

such as a cyber-attack or a data breach. This plan should be well-rehearsed and practiced, in order to ensure that the incident does not escalate and cause further harm to the organization and its stakeholders.

Question 9: **Skipped**

What are some common methods used for risk identification?

- **Brainstorming**
- **Root cause analysis**
- **All of the above**
- **(Correct)**
- **SWOT analysis**

Explanation

There are several common methods used for risk identification, including brainstorming, root cause analysis, and SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis. These methods can be used to identify and understand the risks facing an organization and to determine the likelihood and potential impact of those risks.

Question 10: **Skipped**

What does the term "Wi-Fi" stand for?

- **Wireless Framework**
- **Wireless Fiber**
- **Wireless Fire**
- **Wireless Fidelity**
- **(Correct)**

Explanation

The term "Wi-Fi" was originally created as a play on the term "Hi-Fi" (High Fidelity) used in the music industry, and stands for "Wireless Fidelity."

Question 11: **Skipped**

Which of the following is a potential use case for hash functions?

- **Digital signature verification**
- **Data encryption**
- **Data compression**
- **Password storage**
- **(Correct)**

Explanation

Hash functions can be used to store passwords securely by creating a one-way hash of the password and storing it instead of the actual password. This way, if an attacker gains access to the password database, they cannot easily retrieve the original passwords. Hash functions can

also be used for data integrity checking, digital signature verification, and other security applications.

Question 12: **Skipped**

What are some advantages of using a qualitative risk assessment tool?

- **Improved flexibility in assessing risks**
- **Improved understanding of subjective factors affecting risks**
- **All of the above**
- **(Correct)**
- **Improved ability to prioritize risks based on expert judgment**

Explanation

One advantage of using a qualitative risk assessment tool is that it can provide improved flexibility in assessing risks. By using subjective data, such as expert judgment and scenario analysis, organizations can better understand the subjective factors affecting risks and prioritize risks based on this understanding. This type of tool can also provide improved ability to prioritize risks based on expert judgment.

Question 13: **Skipped**

What is the primary purpose of a Bring Your Own Device (BYOD) policy?

- **To require employees to purchase company-approved devices.**
- **To allow employees to use their personal devices for work-related tasks.**
- **(Correct)**
- **To ensure that employees use company-provided devices only.**
- **To prohibit the use of personal devices for work-related tasks.**

Explanation

A Bring Your Own Device (BYOD) policy is designed to allow employees to use their personal devices, such as smartphones or tablets, for work-related tasks. This can increase productivity and convenience for employees, as they can work from anywhere, at any time, using the devices they are most comfortable with. However, a BYOD policy should also establish guidelines and requirements for device security, data protection, and acceptable use, to ensure that company data is protected and employees are using their devices appropriately.

Question 14: **Skipped**

How is dual control typically implemented in a cybersecurity context?

- **By requiring two individuals to enter separate parts of a password**
- **By requiring two individuals to physically access a secured facility at the same time**
- **By requiring two individuals to independently verify the accuracy of data**
- **By requiring two individuals to complete separate parts of a transaction**
- **(Correct)**

Explanation

Dual control in a cybersecurity context is typically implemented by requiring two individuals to complete separate parts of a transaction. For example, when a sensitive file is being transferred, one individual might initiate the transfer, while another individual approves the transfer. This helps to ensure that sensitive information is not transferred to an unauthorized individual.

Question 15: **Skipped**

What is authentication in the context of cybersecurity?

- **The process of verifying the identity of a user or device**

- (Correct)
- **The process of detecting and preventing security threats**
- **The process of encrypting data**
- **The process of backing up data**

Explanation

Authentication is the process of verifying the identity of a user or device before granting access to resources or information. It is an important aspect of cybersecurity as it helps to ensure that only authorized users or devices can access sensitive information.

Question 16: **Skipped**

Which of the following best describes the three-way-handshake?

- **A method for establishing a connection between two devices on a network**
- (Correct)
- **A security protocol used to protect sensitive data during transmission**
- **A process for resolving network conflicts between multiple devices**
- **A method for blocking a connection between two devices on a network**

Explanation

The three-way-handshake is a method used to establish a connection between two devices on a network. It involves a series of three messages between the devices to ensure that both sides are ready and willing to communicate.

Question 17: **Skipped**

Which of the following protocols is considered to be more secure for remote access?

- **FTP**
- **Telnet**
- **SSH**
- **(Correct)**
- **HTTP**

Explanation

SSH (Secure Shell) is considered to be more secure for remote access because it encrypts data transmitted between the client and server, while Telnet does not. This means that sensitive information, such as login credentials, is protected from interception and unauthorized access.

Question 18: **Skipped**

Which of the following is an example of Discretionary Access Control (DAC)?

- **A company's CEO has access to all resources in the organization.**
- **A user can modify the permissions of files and folders that they own.**
- **(Correct)**
- **A user's access to resources is determined by an administrator.**
- **A user is only given access to resources based on their job function.**

Explanation

Discretionary Access Control (DAC) is an access control mechanism that allows users to determine who can access resources that they own. In this example, the user can modify the permissions of files and folders that they own.

Question 19: **Skipped**

Which of the following best describes the main benefit of implementing a DAC system?

- **It is resistant to attacks and exploits.**
- **It provides a high level of security and control over access to resources.**

- (Correct)
- **It allows for flexible and dynamic access permissions.**
- **It is easy to implement and manage.**

Explanation

Discretionary Access Control (DAC) is a security mechanism that provides owners of resources with control over who can access those resources and what level of access they are granted. In a DAC system, owners determine the access permissions of their resources based on their own discretion. The main benefit of implementing DAC is that it provides a high level of security and control over access to resources. However, one of the limitations of DAC is that it can result in users having too much access to resources if owners grant access to users who may not need it. It is important to implement other security mechanisms, such as the Principle of Least Privilege and Role-Based Access Control, to ensure that access is granted at the appropriate level.

Question 20: **Skipped**

What is the purpose of using a mantrap in an access control system?

- **To provide a means of escape in case of emergency**
- **To provide additional security to a high secure area**
- **(Correct)**
- **To increase the speed of entry into a building**
- **To reduce the number of doors in a building**

Explanation

A mantrap is used in an access control system to provide additional security to a high secure area by controlling access through two secure doors and verifying the identity of individuals before they are granted access to the secure area.

Question 21: **Skipped**

How does the use of surveillance cameras improve physical security?

- **By recording events for future use**
- **All of the above**
- **(Correct)**
- **By deterring potential attackers**
- **By providing real-time monitoring**

Explanation

Surveillance cameras provide real-time monitoring, deter potential attackers and also record events for future use, thereby improving the physical security of the premises.

Question 22: **Skipped**

In an organization that uses Discretionary Access Control (DAC), a user wants to grant access to a file to a colleague. What is the user's next step?

- **The user must obtain approval from the resource owner before granting access to the colleague.**
- **The user must obtain approval from the system administrator before granting access to the colleague.**
- **The user must modify the file permissions and add the colleague to the access control list.**
- **The user can grant the access to the colleague without any additional approval.**
- **(Correct)**

Explanation

In a Discretionary Access Control (DAC) system, the owner of the resource has the authority to grant or deny access to other users. Therefore, the user can grant the access to the colleague without any additional approval.

Question 23: **Skipped**

Which of the following fire suppression systems uses a gas as the extinguishing agent?

- **Clean agent**
- **(Correct)**
- **Foam**
- **Dry chemical**
- **Wet chemical**

Explanation

Clean agent systems use a gas as the extinguishing agent to suppress fires. These systems are commonly used to protect sensitive equipment and electronics.

Question 24: **Skipped**

An organization has classified their data into different categories based on their sensitivity, but they are not consistently applying access controls. What is the risk of not consistently applying access controls?

- **Data may be deleted accidentally**
- **Data may be modified without authorization**
- **The organization may run out of storage space**
- **Sensitive data may be exposed to unauthorized users**
- **(Correct)**

Explanation

The risk of not consistently applying access controls is that sensitive data may be exposed to unauthorized users, which can lead to data breaches, loss of intellectual property, or regulatory noncompliance. By not consistently applying access controls, organizations may inadvertently allow sensitive data to be accessed by users who should not have access, which can put the organization and its stakeholders at risk.

Question 25: **Skipped**

Which of the following best describes the main benefit of implementing a MAC system?

- **It allows for flexible and dynamic access permissions.**
- **It is resistant to attacks and exploits.**
- **It is easy to implement and manage.**
- **It provides a high level of security and control over access to resources.**
- **(Correct)**

Explanation

The main benefit of implementing a MAC system is that it provides a high level of security and control over access to resources. Since access control is determined by a central

authority based on policies, access is granted only to authorized users, and is limited to the minimum necessary level.

Question 26: **Skipped**

Which of the following is a principle of the General Data Protection Regulation (GDPR)?

- **Right to be Forgotten**
- **All of the above**
- **(Correct)**
- **Data Minimization**
- **Transparency**

Explanation

All options are correct. The principle of data minimization requires data controllers to limit the collection and processing of personal data to only what is necessary for the specific purpose for which it is being processed. The principle of transparency requires data controllers to be transparent about how personal data is collected, processed, and used, and to provide individuals with clear and easily accessible information about their privacy rights. The Right to be Forgotten is a principle under the GDPR, which gives individuals the right to request the

deletion of their personal data under certain circumstances, such as when the data is no longer necessary for the purpose for which it was collected or processed.

Question 27: **Skipped**

What is sandboxing and how does it protect against malware?

- **A technique for backing up data**
- **A method for detecting malware**
- **A method for encrypting sensitive information**
- **An isolated environment for executing untrusted code**
- **(Correct)**

Explanation

Sandboxing is a technique in which untrusted code, such as downloaded software or emails, is executed in an isolated environment, separate from the main system. This helps prevent malware from infecting the main system, as any malicious code is contained within the sandbox and cannot access sensitive information or cause harm to the system.

Question 28: **Skipped**

Which component of the on-premises infrastructure is responsible for providing redundancy in case of a hardware failure?

- **Power Generator**
- **Data center/closets**
- **HVAC**
- **Redundancy**
- **(Correct)**

Explanation

The redundancy component of the on-premises infrastructure is responsible for providing backup hardware in case of a hardware failure. This is important because hardware failures can cause downtime and data loss if not properly addressed.

Question 29: **Skipped**

What is the Segregation of Duties?

- **A security control that requires employees to work in separate physical locations.**
- **A security control that ensures employees have access to all resources they need to perform their job functions.**
- **A security control that allows employees to perform multiple roles within an organization.**

- **A security control that divides responsibilities among multiple employees to reduce the risk of fraud or errors.**
- **(Correct)**

Explanation

The Segregation of Duties is a security control that divides responsibilities among multiple employees to reduce the risk of fraud or errors. This means that no single employee has complete control over a particular process or resource, which helps prevent errors or malicious activities.

Question 30: **Skipped**

A financial institution is trying to determine the potential losses it could incur from a cyber attack. What type of risk assessment tool would be the most appropriate to use in this scenario?

- **Digital risk assessment**
- **Both quantitative and qualitative risk assessment**
- **Quantitative risk assessment**
- **(Correct)**
- **Qualitative risk assessment**

Explanation

Quantitative risk assessments are used to determine the potential financial impact of risks. In this scenario, the financial institution would use this type of assessment to determine the potential losses it could incur from a cyber attack, helping it to develop a more effective risk management plan. This would include measures to reduce the likelihood of an attack and to minimize the impact if one were to occur.

Question 31: **Skipped**

Which of the following is one of the roles of the management team in an IT business continuity plan?

- **To provide technical expertise for the plan**
- **To develop and implement the plan**
- **To ensure that the plan is tested regularly**
- **To provide overall direction and support for the plan**
- **(Correct)**

Explanation

he management team has several key roles in an IT business continuity plan, one of which is to provide overall direction and support for the plan. The management team should ensure that the plan is integrated into the overall operations of the organization and that it is adequately

supported and funded. The management team should also be actively involved in ensuring that the plan is tested regularly and that any necessary updates are made in a timely manner.

Question 32: **Skipped**

Which of the following is a method used by cryptanalysts to break encryption?

- **Frequency analysis**
- **(Correct)**
- **Key exchange**
- **Key generation**
- **Cryptography hashing**

Explanation

Cryptanalysts use various methods and techniques to break encryption, including brute-force attacks, mathematical analysis, and statistical analysis. Frequency analysis is a method used to analyze the frequency distribution of letters or symbols in an encrypted message and to deduce the key or plaintext based on the patterns of the distribution. Key generation and key exchange are methods used to generate or exchange cryptographic

keys, while cryptography hashing is a method used to convert data into a fixed-length code.

Question 33: **Skipped**

What are some examples of storage devices where data remanence can occur?

- **All options**
- **(Correct)**
- **Hard disk drives**
- **USB flash drives**
- **Solid-state drives**

Explanation

Data remanence can occur on a variety of storage devices, including hard disk drives (HDDs), solid-state drives (SSDs), and USB flash drives. When data is stored on these devices, it can leave traces that persist even after attempts have been made to delete it. This is why it is important to use secure data destruction techniques to ensure that data is completely erased and cannot be recovered by attackers.

Question 34: **Skipped**

Which of the following is an example of an administrative control?

- **Background checks for employees**
- **(Correct)**
- **Network-based Intrusion detection system**
- **Physical locks on doors**
- **Firewall**

Explanation

Background checks for employees are an example of an administrative control because they are a set of policies and procedures that are put in place to ensure that employees are suitable for their role. These checks typically involve verifying the employee's employment history and conducting a criminal background check.

Question 35: **Skipped**

What is the primary advantage of a Next-Generation Firewall that includes an application-aware component?

- **It can prioritize and allocate bandwidth to critical applications.**
- **It can block spam and other unwanted traffic at the application layer.**
- **It can detect and block unauthorized applications from entering the network.**
- **(Correct)**

- **It can provide visibility into application usage and performance.**

Explanation

An application-aware component of a Next-Generation Firewall can detect and block applications based on their specific protocols and behaviors. This allows the firewall to prevent unauthorized or malicious applications from entering the network.

Question 36: **Skipped**

What is a cyber disaster?

- **A disaster caused by a natural event such as a hurricane.**
- **A disaster caused by a failure of computer systems and networks.**
- **(Correct)**
- **A disaster caused by a widespread outbreak of a disease.**
- **A disaster caused by a nuclear explosion.**

Explanation

A cyber disaster is an event caused by a failure of computer systems and networks, such as a cyber-attack, a data breach, or a hardware failure. This type of disaster can have serious impacts on organizations, including loss

of data and intellectual property, loss of revenue, and damage to reputation. It is important for organizations to have a disaster recovery plan in place that addresses cyber disasters, in order to minimize the impact of such events on the organization and its stakeholders.

Question 37: **Skipped**

What are the key principles of privacy in the context of information security?

- **Transparency, control, and accountability.**
- **(Correct)**
- **Availability, confidentiality, and integrity.**
- **Trust, privacy, and responsibility.**
- **Security, privacy, and compliance.**

Explanation

The key principles of privacy in the context of information security are transparency, control, and accountability. Transparency refers to organizations being transparent about how they collect, use, and share personal information. Control refers to individuals having control over their personal information. Accountability refers to organizations being accountable for how they handle personal information. These three principles are

considered to be the cornerstone of privacy in the context of information security.

Question 38: **Skipped**

What is the purpose of a change request form in change management?

- **To provide a way for stakeholders to review and approve the change request**
- **All options**
- **(Correct)**
- **To provide documentation of the change request**
- **To provide a way to track the progress of the change request**

Explanation

A change request form is a document used to capture the details of a proposed change. It typically includes information such as the reason for the change, the impact of the change, and the risks associated with the change. The change request form is used to provide documentation of the change request, to track the progress of the change request, and to provide a way for stakeholders to review and approve the change request.

Question 39: **Skipped**

Which of the following is considered a type of physical security control that helps to prevent unauthorized access and provides a secure area for the authentication process?

- **Video Surveillance**
- **Electronic Keycard Access**
- **Motion Sensors**
- **Mantrap**
- **(Correct)**

Explanation

Mantrap is a type of physical security control that is used to secure an area and prevent unauthorized access. It consists of two secure doors or barriers that are interlocked and can only be unlocked if an authorized user enters the correct credentials. Mantraps provide a secure area for the authentication process, allowing organizations to verify the identity of individuals before granting access to restricted areas. The use of mantraps enhances the overall security of a facility by providing an extra layer of protection against unauthorized access.

Question 40: **Skipped**

What are some advantages of using a quantitative risk assessment tool?

- **Improved efficiency in prioritizing risks**
- **Improved ability to allocate resources effectively**
- **All of the above**
- **Improved accuracy in determining the likelihood and impact of risks**
- **(Correct)**

Explanation

One advantage of using a quantitative risk assessment tool is that it can provide improved accuracy in determining the likelihood and impact of risks. By using numerical data, organizations can quantify the risks they face and prioritize those risks based on their potential impact and likelihood.

Question 41: **Skipped**

How can a network or server protect against Fragment (Teardrop) attacks?

- **By using firewalls to block incoming traffic from known malicious sources**
- **By using intrusion detection systems to monitor network traffic for signs of an attack**

- **By regularly updating the operating system and software with the latest security patches**
- **(Correct)**
- **By installing antivirus software on all devices**

Explanation

To protect against Fragment (Teardrop) attacks, a network or server can regularly update the operating system and software with the latest security patches. This helps to ensure that any known vulnerabilities that can be exploited by the attack are patched and secure. Additionally, network and server administrators can implement measures such as rate limiting to limit the number of fragmented packets that can be sent to a system, as well as filtering rules to block traffic that is known to contain malformed packets.

Question 42: **Skipped**

What happens if an individual holding an ISC2 certification violates the Code of Ethics Canon 1: Protect society, the common good, necessary public trust and confidence, and the infrastructure?

- **he individual may face criminal charges for their actions, which could have a negative impact on their career and reputation.**
- **The individual may face disciplinary action from ISC2, which could result in revocation of their certification.**
- **(Correct)**
- **The individual may receive a warning or reprimand, but their certification will remain intact.**
- **The individual will be deemed to have fulfilled their professional obligations.**

Explanation

A violation of (ISC)2 Canons could result in disciplinary action and revocation of the individual's certification.

Question 43: **Skipped**

What is a risk mitigation strategy?

- **A strategy to eliminate all risks**
- **A strategy to transfer risk to another party**
- **A strategy to minimize the impact of risks**
- **(Correct)**
- **A strategy to increase risk exposure**

Explanation

A risk mitigation strategy is a strategy to minimize the impact of risks. Risk mitigation is the process of reducing

the impact of risks through various methods, such as implementing controls or transferring the risk to another party. By implementing risk mitigation strategies, organizations can reduce the impact of risks and minimize the potential damage to their operations, reputation, and financial stability.

Question 44: **Skipped**

What is the final step in the risk management process?

- **Identifying risks**
- **Implementing controls**
- **Monitoring and review**
- **(Correct)**
- **Assessing risks**

Explanation

The final step in the risk management process is monitoring and review. This involves regularly monitoring and reviewing the effectiveness of risk management controls, and making any necessary changes or improvements to those controls. The monitoring and review step is an important step in the risk management process, as it helps organizations to ensure that their risk management efforts are effective, and that they are able

to respond quickly to any changes in their risk environment.

Question 45: **Skipped**

What should be the outcome of the post-incident review?

- **A decision to terminate the incident response team.**
- **Recommendations for improvements to the incident response process.**
- **(Correct)**
- **None of the above.**
- **A report documenting the incident.**

Explanation

The outcome of the post-incident review should be recommendations for improvements to the incident response process. These recommendations should be used to make changes to the incident response process, and to improve the overall resilience and preparedness of the organization in the event of future incidents.

Question 46: **Skipped**

What is the purpose of risk identification?

- **To maximize the impact of risks**
- **To avoid addressing risks**
- **To minimize the impact of risks**
- **To understand the risks facing an organization**

- **(Correct)**

Explanation

The purpose of risk identification is to understand the risks facing an organization and to determine the likelihood and potential impact of those risks. This information is used to prioritize risks and determine the most effective approach to mitigating or managing those risks.

Question 47: **Skipped**

Which of the following best describes a Memorandum of Understanding (MOU)?

- **A document that outlines the terms of a partnership or collaboration between two parties**
- **(Correct)**
- **A document that outlines the terms of a non-disclosure agreement**
- **A document that outlines the terms of an employment contract**
- **A legally binding agreement between two parties**

Explanation

A Memorandum of Understanding (MOU) is a non-binding document that outlines the terms of a partnership or

collaboration between two or more parties when a disaster hits.

Question 48: **Skipped**

What is biometric authentication?

- **A method of authentication that uses a temporary code generated by a device**
- **A method of authentication that uses biometric characteristics, such as fingerprints**
- **(Correct)**
- **A method of authentication that uses a physical device, such as a smart card**
- **A method of authentication that uses a secret password**

Explanation

Biometric authentication is a method of authentication that uses biometric characteristics, such as fingerprints, facial recognition, or iris scans, to verify the identity of a user. This method provides a secure and convenient way to authenticate users, as biometric characteristics are unique to each individual and cannot be easily stolen or guessed like passwords. However, biometric authentication has some limitations, such as the need for specialized hardware and potential privacy concerns.

Question 49: **Skipped**

How can an organization determine its risk tolerance?

- **All of the above**
- **(Correct)**
- **By evaluating the risks it is facing**
- **By evaluating its stakeholders' risk tolerance**
- **By evaluating its goals and objectives**

Explanation

An organization can determine its risk tolerance by evaluating its goals and objectives, the risks it is facing, and the risk tolerance of its stakeholders. This can involve considering factors such as the organization's size, industry, goals and objectives, and the level of risk that its stakeholders are willing to accept. By considering these factors, organizations can determine the amount of risk that they are willing to accept in order to pursue their goals and objectives.

Question 50: **Skipped**

What is the main purpose of an Acceptable Use Policy (AUP)?

- **To restrict access to company resources.**

- **To allow employees to use company resources as they see fit.**
- **To provide guidelines for appropriate use of company resources.**
- **(Correct)**
- **To delegate responsibility for resource management to a third-party provider.**

Explanation

The main purpose of an Acceptable Use Policy (AUP) is to provide guidelines for appropriate use of company resources, such as computer systems, networks, and internet access. This policy outlines what is and isn't allowed, and defines the consequences of policy violations. It helps to protect company resources from abuse, minimize legal and security risks, and establish expectations for employee behavior.

Question 51: **Skipped**

Which of the following is an example of a preventative security control?

- **Network-based Intrusion detection system**
- **Encryption**
- **Host-based Intrusion detection system**
- **Firewall**

- **(Correct)**

Explanation

A firewall is a preventative security control because it is designed to prevent unauthorized access to a network. It works by enforcing rules and policies that dictate which types of incoming and outgoing network traffic are allowed.

Question 52: **Skipped**

What is the purpose of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in technical controls?

- **To encrypt sensitive data**
- **To enforce access control policies between a computer network and the internet**
- **To monitor network traffic for malicious activity**
- **(Correct)**
- **To securely store sensitive data**

Explanation

The purpose of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in technical controls is to monitor network traffic for malicious activity and alert administrators of any suspicious activity. They are

designed to detect and prevent cyber attacks on computer networks.

Question 53: **Skipped**

What is the purpose of NAT?

- **To provide security to a network**
- **To control network traffic**
- **To identify devices on the internet**
- **To map private IP addresses to public IP addresses**
- **(Correct)**

Explanation

The purpose of NAT is to enable devices in a private network to access the internet using a public IP address. It works by mapping private IP addresses to

Question 54: **Skipped**

What is the primary function of a firewall in technical controls?

- **To encrypt sensitive data**
- **To enforce access control policies between a computer network and the internet**
- **(Correct)**
- **To monitor network traffic for malicious activity**
- **To securely store sensitive data**

Explanation

The primary function of a firewall in technical controls is to enforce access control policies between a computer network and the internet. It acts as a barrier to block unauthorized access to a computer network while allowing authorized communication to pass through.

Question 55: **Skipped**

In a large warehouse, it is important to track the movement of personnel, vehicles, and products to ensure the safety and security of the assets. What type of log can be used for this purpose?

- **Environmental logs**
- **Inventory logs**
- **Surveillance logs**
- **Access logs**
- **(Correct)**

Explanation

Access logs record information about who entered and exited the warehouse and when, which can help to monitor the movement of personnel, vehicles, and products and ensure the safety and security of the assets.

Question 56: **Skipped**

In an organization that uses RBAC, which of the following is the best approach for granting temporary access to a user outside of their normal role?

- **Modify the user's existing role to grant access to the required resources.**
- **Grant the user temporary administrative privileges.**
- **Assign the user a new role that grants access to the required resources.**
- **(Correct)**
- **Deny the user access to the required resources.**

Explanation

In Role-based access control (RBAC), access control is based on the user's role or job function within the organization. To grant temporary access to a user outside of their normal role, a new role can be assigned to the user that grants access to the required resources. This ensures that the user only has access to the resources necessary for their temporary task.

Question 57: **Skipped**

Which of the following is true about hash functions?

- **They are used for encryption and decryption of data.**
- **They produce a fixed-size output for any input.**
- **(Correct)**

- **They can be used as a replacement for symmetric encryption.**
- **They are reversible functions that can be decrypted.**

Explanation

Hash functions are one-way functions that take an input (message or data) of any size and produce a fixed-size output (hash or digest) of a fixed length. The output cannot be used to retrieve the original input, making them useful for data integrity and digital signature verification.

Question 58: **Skipped**

What is the difference between high availability and fault tolerance?

- **High availability refers to the ability of a system to provide quick response times, while fault tolerance refers to the ability of a system to continue operating in the event of a failure.**
- **High availability refers to the ability of a system to withstand multiple failures without loss of data or disruption of service, while fault tolerance refers to the ability of a system to continue operating in the event of a failure.**
- **(Correct)**

- **High availability refers to the ability of a system to continue operating in the event of a failure, while fault tolerance refers to the ability of a system to withstand multiple failures without loss of data or disruption of service.**
- **High availability refers to the ability of a system to be accessible from multiple locations, while fault tolerance refers to the ability of a system to continue operating in the event of a failure.**

Explanation

High availability refers to the ability of a system to withstand multiple failures without loss of data or disruption of service. This is typically achieved through the use of redundancy and load balancing, which help to ensure that the system remains available even if one or more components fail. Fault tolerance refers to the ability of a system to continue operating in the event of a failure. This is typically achieved through the use of redundant components and failover mechanisms, which allow the system to continue operating even if one or more components fail.

Question 59: **Skipped**

Which of the following best describes the purpose of change management in cybersecurity?

- **To ensure that changes are implemented quickly and without review.**
- **To prevent any changes from being made to security measures.**
- **To ensure that changes are implemented in a way that minimizes risk and disruption.**
- **(Correct)**
- **To delegate responsibility for changes to a third-party provider.**

Explanation

The purpose of change management in cybersecurity is to ensure that any changes made to security measures are implemented in a way that minimizes risk and disruption. This involves careful planning, review, and testing to ensure that changes are effective and don't cause unintended consequences. By implementing changes in a thoughtful and deliberate way, organizations can ensure that their cybersecurity measures remain effective and their operations remain uninterrupted.

Question 60: **Skipped**

What is the purpose of the analysis step in incident response?

- **To stop the incident from spreading.**
- **To determine the cause of the incident.**
- **(Correct)**
- **To implement a solution to the incident.**
- **To notify relevant parties of the incident.**

Explanation

The purpose of the analysis step in incident response is to determine the root cause of the incident. This involves collecting and analyzing data from various sources, such as system logs, network traffic, and other relevant information, to understand what caused the incident to occur.

Question 61: **Skipped**

Which of the following is an effective defense against phishing and spear phishing attacks?

- **Disabling all email attachments and links.**
- **Using a simple and easy-to-guess password for all accounts.**
- **Enabling multi-factor authentication (MFA) for all online accounts.**
- **(Correct)**

- **Sharing sensitive information freely and openly with all contacts.**

Explanation

Multi-factor authentication (MFA) is an effective defense against phishing and spear phishing attacks because it requires an additional layer of authentication beyond just a username and password, such as a one-time code sent to a mobile device. Disabling all email attachments and links is not practical or effective, and using a simple password or sharing sensitive information freely and openly can increase the risk of a successful attack.

Question 62: **Skipped**

Which of the following is a potential security risk associated with connected Internet of Things (IoT) devices?

- **Inability to connect to the internet**
- **Vulnerabilities in software and firmware**
- **(Correct)**
- **Interference from other connected devices**
- **Limited battery life of devices**

Explanation

While the other options may be challenges or limitations associated with IoT devices, vulnerabilities in software and firmware can pose a serious security risk. Flaws in software or firmware can potentially allow attackers to gain access to sensitive data or control over the device, and IoT devices can be particularly vulnerable to such attacks.

Question 63: **Skipped**

What is the difference between data backup and data archiving?

- **There is no difference between data backup and data archiving.**
- **Data backup is for short-term storage of data, while data archiving is for long-term storage of data.**
- **(Correct)**
- **Data backup is for disaster recovery purposes, while data archiving is for regulatory compliance purposes.**
- **Data backup is for storing multiple versions of data, while data archiving is for storing only one version of data.**

Explanation

Data backup is for short-term storage of data to protect against data loss in the event of a disaster or system

failure. Data archiving is for long-term storage of data for regulatory compliance or historical preservation purposes.

Question 64: **Skipped**

Which of the following is an example of a detective security control?

- **Intrusion detection system**
- **(Correct)**
- **Antivirus software**
- **Encryption**
- **Firewall**

Explanation

An intrusion detection system is a detective security control because it is designed to detect signs of unauthorized access or other security incidents. It works by monitoring network traffic and alerts administrators when it detects suspicious activity.

Question 65: **Skipped**

Which of the following is a recommended approach for segmenting IoT devices from other network resources?

- **Using virtual private networks (VPNs) to isolate IoT devices**

- **Placing IoT devices on the same network segment as other network resources**
- **Implementing network segmentation based on the function of the device**
- **(Correct)**
- **Not segmenting IoT devices at all**

Explanation

Segmentation is an important strategy for protecting IoT devices from cyberattacks, and the best approach is to segment the network based on the function of the device. This allows for the implementation of security policies specific to the devices and their functions, and can help to limit the impact of a potential attack.

Question 66: **Skipped**

Which of the following is not considered a privacy concern?

- **Government surveillance**
- **Data tracking by companies for advertising purposes**
- **Data breaches**
- **Corporate transparency**
- **(Correct)**

Explanation

Corporate transparency refers to a company's willingness to be open and honest about its operations, which is generally considered a positive aspect of business practices, rather than a privacy concern. Options A, B, and C all have the potential to compromise an individual's privacy in some way.

Question 67: **Skipped**

Which of the following is a defense strategy against zero-day attacks?

- **Using strong passwords and multifactor authentication.**
- **Disabling all unnecessary services and ports.**
- **Implementing perimeter-based network security controls.**
- **Regularly updating software and systems.**
- **(Correct)**

Explanation

Regularly updating software and systems can help mitigate the risk of zero-day attacks by ensuring that known vulnerabilities are patched and new security features are implemented. While using strong passwords, disabling unnecessary services and ports, and

implementing perimeter-based security controls can also help enhance security, they do not necessarily protect against zero-day attacks.

Question 68: **Skipped**

What is the primary goal of network segmentation in a cybersecurity strategy?

- **To simplify network management**
- **To reduce the attack surface by isolating critical assets and sensitive data**
- **(Correct)**
- **To create a single point of failure**
- **To increase the attack surface by expanding the network**

Explanation

Network segmentation involves dividing a network into smaller subnetworks, which limits the ability of attackers to move laterally and access sensitive data or systems. This helps to prevent the spread of malware, unauthorized access, and other cyber threats.

Question 69: **Skipped**

What is the purpose of a Configuration Management Database (CMDB)?

- **To automate the process of deploying software updates and patches**
- **To manage the configuration of network switches and routers**
- **To store and manage information about the configuration items (CIs) in an IT environment**
- **(Correct)**
- **To provide a secure storage location for sensitive data**

Explanation

A CMDB is a database that contains information about the CIs in an IT environment, including their attributes, relationships, and dependencies. It is used to support IT service management processes, such as incident management, problem management, and change management. A CMDB can be used to track the status of CIs, manage changes to CIs, and support decision-making related to IT service management.

Question 70: **Skipped**

Which of the following is a requirement of the Payment Card Industry Data Security Standard (PCI DSS)?

- **Firewall configurations must be secure**
- **Cardholder data must be encrypted**

- **All of the above**
- **(Correct)**
- **Antivirus software must be installed and updated regularly**

Explanation

All of the above. The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of requirements for enhancing payment card data security. The standard requires organizations to implement a number of security measures, including secure firewall configurations, encryption of cardholder data, and regular updating of antivirus software. These measures are designed to help reduce the risk of payment card fraud and protect cardholder data from theft or misuse.

Question 71: **Skipped**

Company XYZ is concerned about the potential for fraud or errors in their accounting department. Which security control should be implemented to reduce this risk?

- **None of the above.**
- **Segregation of Duties and the Principle of Least Privilege**
- **Principle of Least Privilege**

- **Segregation of Duties**
- **(Correct)**

Explanation

The Segregation of Duties should be implemented to reduce the risk of fraud or errors in the accounting department. This control divides responsibilities among multiple employees, which helps ensure that no single employee has complete control over a particular process or resource. This reduces the risk of errors or malicious activities that could result in financial loss or other damage.

Question 72: **Skipped**

Which of the following is an example of a symmetric encryption algorithm?

- **Diffie-Hellman**
- **ECC**
- **AES**
- **(Correct)**
- **RSA**

Explanation

AES (Advanced Encryption Standard), which is a widely-used symmetric encryption algorithm. RSA,

Diffie-Hellman, and ECC are all examples of asymmetric encryption algorithms.

Question 73: **Skipped**

What is the main objective of Confidentiality in information security?

- **Availability**
- **Secrecy**
- **(Correct)**
- **Integrity**
- **Authentication**

Explanation

Secrecy (Confidentiality) is one of the main objectives of information security, and its main purpose is to ensure that sensitive or confidential information is protected from unauthorized access or disclosure. This objective aims to maintain the privacy of the information and keep it safe from potential threats or breaches.

Question 74: **Skipped**

Your organization has just suffered a major disaster, and you have been assigned the role of disaster recovery manager. What is the first step you should take in this role?

- **Establish a crisis management center and begin communications with key stakeholders.**
- **(Correct)**
- **Conduct a damage assessment of the organization's facilities and infrastructure.**
- **Identify the critical business processes that must be protected and prioritize their recovery.**
- **Begin the process of restoring normal business operations as quickly as possible.**

Explanation

The first step in the role of disaster recovery manager is to establish a crisis management center, which will serve as the central hub for coordinating and communicating the disaster recovery efforts. This center should be equipped with the necessary resources and technology to facilitate effective communication with key stakeholders, including employees, customers, partners, and suppliers. In a real-world scenario, the disaster recovery manager might take a combination of steps A, B, C, and D, or they might prioritize one step over another, depending on the specific needs of the organization and the impact of the disaster.

Question 75: **Skipped**

What is the purpose of conducting a Business Impact Analysis (BIA)?

- **To determine the likelihood of a disaster occurring**
- **To evaluate the costs and benefits of different security measures**
- **To assess the impact of a potential security breach**
- **To identify the critical functions and processes of an organization**
- **(Correct)**

Explanation

The purpose of conducting a Business Impact Analysis (BIA) is to identify the critical functions and processes of an organization and to assess the impact of a potential disruption to these processes. This information is used to prioritize the development of recovery plans and ensure the continued operations of the organization in the event of a disaster.

Question 76: **Skipped**

What is the purpose of system hardening?

- **To increase the performance of a system.**
- **To ensure that a system is always available and accessible.**

- **To make a system more resilient against attacks and intrusions.**
- **(Correct)**
- **To ensure that a system is compatible with all software and hardware.**

Explanation

System hardening involves implementing security measures to reduce the attack surface and increase the security of a system. This includes disabling unnecessary services, applying security patches and updates, configuring firewalls and access controls, and enforcing password policies, among other measures. The goal is to make it more difficult for attackers to gain access to the system and its data.

Question 77: **Skipped**

What is the first step in developing a disaster recovery plan?

- **Develop procedures for responding to and recovering from a disaster.**
- **Identify critical systems and processes that must be protected.**
- **(Correct)**
- **Establish a disaster recovery team.**

- **Conduct a risk assessment to identify potential disaster scenarios.**

Explanation

Identifying critical systems and processes that must be protected is an important step in the disaster recovery process, as it helps to inform the development of the disaster recovery plan and ensure that it is comprehensive and effective in the event of a disaster.

Question 78: **Skipped**

What is the primary disadvantage of a packet filtering firewall?

- **They are unable to block traffic based on IP addresses.**
- **They are unable to filter traffic based on application layer protocols.**
- **(Correct)**
- **They are unable to maintain state information about connections.**
- **They are vulnerable to attacks that exploit network-layer protocols.**

Explanation

Packet filtering firewalls are designed to filter traffic based on network layer information, such as IP addresses and

port numbers. This makes them less effective at filtering traffic that uses application layer protocols, such as HTTP or FTP. As a result, packet filtering firewalls are often used in combination with other security technologies, such as intrusion detection systems (IDS) or application layer firewalls.

Question 79: **Skipped**

As a network administrator, how can you protect a network or server against Oversized packet attacks?

- **By implementing rate limiting to limit the number of packets that can be sent to a system**
- **(Correct)**
- **By installing antivirus software on all devices**
- **By using firewalls to block incoming traffic from known malicious sources**
- **By using intrusion detection systems to monitor network traffic for signs of an attack**

Explanation

An Oversized packet attack is an attack that floods a network or server with packets that exceed the maximum allowed size. This can cause the victim's system to become overwhelmed and unresponsive. To protect

against Oversized packet attacks, a network or server can implement rate limiting to limit the number of packets that can be sent to a system. This helps to ensure that the system is not overwhelmed by a flood of packets that exceed the maximum allowed size. Additionally, network and server administrators can implement filtering rules to block traffic that contains oversized packets, as well as other security measures such as firewalls and intrusion detection systems to further protect against attacks.

Question 80: **Skipped**

Which of the following is an example of an active attack?

- **Running a script that repeatedly tries different login credentials**
- **(Correct)**
- **Monitoring network traffic to identify patterns of user behavior**
- **Using software to capture encrypted data and crack the encryption key**
- **Sending spam emails to deceive users into revealing sensitive information**

Explanation

An active attack involves a deliberate attempt to modify or disrupt data. In this case, running a script that repeatedly

tries different login credentials is an example of an active attack aimed at gaining unauthorized access to a system. The other options describe different types of passive attacks. Monitoring network traffic, sending spam emails, and capturing encrypted data are all forms of passive attack aimed at eavesdropping or observing data without making changes. While these attacks can still be dangerous, they are typically less immediate threats than active attacks since they don't result in direct modifications to data.

Question 81: **Skipped**

Which of the following statements is true regarding the three-way-handshake?

- **It is used to encrypt data during transmission**
- **It is only used for establishing a connection between servers and not between client and server**
- **It ensures both devices are ready and willing to communicate**
- **(Correct)**
- **It involves only two messages exchanged between two devices**

Explanation

The three-way-handshake involves three messages exchanged between two devices, and its purpose is to ensure that both sides are ready and willing to communicate. It is not used to encrypt data during transmission, and it is used for establishing connections between both servers and clients.

Question 82: **Skipped**

Which of the following is a key element of a rollback plan in change management?

- **Assigning a project manager to oversee the change**
- **Identifying the risks and impacts of the change**
- **Communicating the change to end-users**
- **Identifying the steps needed to undo the change**
- **(Correct)**

Explanation

One of the key elements of a rollback plan is to identify the steps needed to undo the change. This includes identifying the configuration items that were changed, the order in which they need to be rolled back, and any dependencies or impacts of the rollback on other systems or processes. By having a clear plan in place, the

organization can respond quickly and effectively to any issues that arise during the change management process.

Question 83: **Skipped**

What are the 4 principles of CPTED (Crime Prevention Through Environmental Design)?

- **Surveillance, Access control, Lighting, and Maintenance**
- **Access control, Territoriality, Lighting, and Maintenance**
- **Surveillance, Access control, Territoriality, and Maintenance**
- **(Correct)**
- **Surveillance, Territoriality, Lighting, and Maintenance**

Explanation

CPTED (Crime Prevention Through Environmental Design) is based on 4 principles, which include Surveillance, Access control, Territoriality, and Maintenance. These principles aim to increase natural surveillance and reduce opportunities for crime, establish ownership and control over the built environment, and ensure proper maintenance and upkeep of the environment to maintain its effectiveness in reducing crime.

Question 84: **Skipped**

Which of the following is a key benefit of using a UPS (Uninterruptible Power Supply) in the on-premises infrastructure?

- **It provides physical security for the data center**
- **It provides backup storage for the data**
- **It provides cooling for the servers**
- **It provides backup power during a power outage**
- **(Correct)**

Explanation

A UPS (Uninterruptible Power Supply) provides battery backup power in the event of a power outage, which helps prevent data loss or server damage due to sudden power loss.

Question 85: **Skipped**

What is the main purpose of using a badge system in a cybersecurity setting?

- **To prevent unauthorized access to secure areas**
- **(Correct)**
- **To track inventory levels**
- **To enforce dress code regulations**
- **To monitor employee attendance**

Explanation

The primary purpose of using a badge system in a cybersecurity setting is to prevent unauthorized access to secure areas, such as data centers, server rooms, or restricted areas. The system uses a unique identifier, such as an ID card or key fob, to grant or deny access to certain areas.

Question 86: **Skipped**

What is a supply chain disruption disaster?

- **A disaster caused by a natural event such as a hurricane.**
- **A disaster caused by a disruption in the flow of goods and materials.**
- **(Correct)**
- **A disaster caused by a nuclear explosion.**
- **A disaster caused by a widespread outbreak of a disease.**

Explanation

A supply chain disruption disaster is an event caused by a disruption in the flow of goods and materials, such as a transportation strike, a natural disaster, or a political crisis. This type of disaster can have serious impacts on organizations, including loss of revenue, difficulty

obtaining critical supplies, and damage to reputation. It is important for organizations to have a disaster recovery plan in place that addresses supply chain disruption disasters, in order to minimize the impact of such events on the organization and its stakeholders.

Question 87: **Skipped**

What is the purpose of installing bollards in a physical security plan?

- **To direct traffic flow**
- **To secure an area**
- **To provide a visual barrier**
- **All of the above**
- **(Correct)**

Explanation

Bollards can serve all of the above purposes, making them a versatile and effective tool in a physical security plan. By providing a visual barrier, directing traffic flow, and securing an area, bollards can help to deter unauthorized access and prevent unwanted intrusion.

Question 88: **Skipped**

What is the primary purpose of the Payment Card Industry Data Security Standard (PCI DSS)?

- **To promote ethical behavior in payment card usage**
- **To prevent fraud and theft in payment card transactions**
- **To regulate the use of payment card information**
- **To ensure the security of credit card information**
- **(Correct)**

Explanation

The Payment Card Industry Data Security Standard (PCI DSS) was created to ensure the security of credit card information in transactions and storage. Its primary purpose is to secure payment card information and prevent fraud and theft.

Question 89: **Skipped**

Which type of encryption is used for secure communication between a web server and a web browser?

- **Symmetric encryption**
- **Hash encryption**
- **SSL/TLS**
- **(Correct)**
- **Asymmetric encryption**

Explanation

SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a protocol that uses both symmetric and asymmetric encryption to provide secure communication between a web server and a web browser. Hash encryption is not typically used for secure communication, and while symmetric and asymmetric encryption can be used for secure communication, they are not typically used on their own for this purpose.

Question 90: **Skipped**

What are the four main phases of the data lifecycle?

- **Data creation, data storage, data use, data destruction**
- **Data creation, data storage, data modification, data destruction**
- **Data creation, data use, data sharing, data archiving**
- **Data creation, data use, data modification, data archiving**
- **(Correct)**

Explanation

The four main phases of the data lifecycle are data creation, data use, data modification, and data archiving.

Question 91: **Skipped**

What is the primary purpose of a policy in an organization's governance process?

- **To provide guidelines for decision making**
- **(Correct)**
- **To enforce regulations and laws**
- **To outline specific steps to be taken in a particular situation**
- **To ensure accountability**

Explanation

Policies are statements of an organization's intent and provide a framework for decision making. They establish guidelines for behavior and decision-making, without being prescriptive in the steps to be taken in a particular situation.

Question 92: **Skipped**

What should be considered when developing a physical security control plan?

- **The location of the assets.**
- **The type of assets being protected.**
- **The potential threat sources.**
- **All of the above.**
- **(Correct)**

Explanation

When developing a physical security control plan, it is important to consider the type of assets being protected, the location of the assets, and the potential threat sources. This helps to ensure that the physical security controls are appropriate for the specific assets and threat environment, and that they effectively protect against unauthorized access and other security incidents.

Question 93: **Skipped**

What is the purpose of a cold site?

- **To provide an unused facility that can be quickly converted to a functional backup site in the event of a disaster**
- **(Correct)**
- **To provide a means of recovering data in the event of a disaster**
- **To provide a plan for restoring normal business operations in the event of a disaster**
- **To provide a minimal level of infrastructure that can be used in the event of a disaster**

Explanation

A cold site is an unused facility with no equipment or infrastructure, which would require significant time and resources to be made operational in the event of a

disaster. The primary purpose of a cold site is to provide a location that can be quickly converted to a functional backup site in the event of a disaster.

Question 94: **Skipped**

Which of the following is an example of implementing the Segregation of Duties?

- **Allowing a single employee to manage and maintain all company databases.**
- **Having one employee responsible for both network security and system administration.**
- **llowing the same employee to approve and process financial transactions.**
- **Dividing the responsibilities for approving and processing financial transactions among multiple employees.**
- **(Correct)**

Explanation

Dividing the responsibilities for approving and processing financial transactions among multiple employees is an example of implementing the Segregation of Duties. This helps ensure that no single employee has complete control over the financial transaction process, which reduces the risk of fraud or errors.

Question 95: **Skipped**

Which of the following is a characteristic of cloud data centers?

- **High upfront capital expenditures**
- **Location-dependent resource availability**
- **Pay-per-use pricing models**
- **(Correct)**
- **Customized hardware configurations**

Explanation

One of the key characteristics of cloud data centers is their pay-per-use pricing model, which allows users to pay only for the resources they actually use. This is in contrast to on-premises infrastructure, which often requires high upfront capital expenditures. Cloud providers also typically offer standardized hardware configurations rather than customized options, and resource availability is not location-dependent in the same way it is for on-premises infrastructure.

Question 96: **Skipped**

What is the main difference between fail-safe and fail-secure mechanisms?

- **Fail-safe systems lock down in case of a failure, while fail-secure systems operate in a safe state in case of a failure.**
- **Fail-safe and fail-secure systems are the same thing.**
- **Neither fail-safe nor fail-secure systems are used in security applications.**
- **Fail-safe systems operate in a safe state in case of a failure, while fail-secure systems lock down in case of a failure.**
- **(Correct)**

Explanation

Fail-safe systems are designed to operate in a safe state in case of a failure, while fail-secure systems are designed to lock down in case of a failure. This means that fail-safe systems will continue to operate even if there is a failure, while fail-secure systems will shut down to prevent unauthorized access.

Question 97: **Skipped**

What is the main goal of the Payment Card Industry Data Security Standard (PCI DSS)?

- **To protect sensitive financial information of individual customers**
- **(Correct)**

- **To protect sensitive information stored, processed or transmitted by organizations**
- **To ensure the security of financial data of merchants**
- **To ensure the security of online transactions**

Explanation

The main goal of the Payment Card Industry Data Security Standard (PCI DSS) is to protect sensitive financial information (Credit Card Date) of individual customers stored, processed, or transmitted by organizations.

Question 98: **Skipped**

What is the primary objective of change management in cybersecurity?

- **To minimize the impact of changes to security measures.**
- **(Correct)**
- **To increase the complexity of security measures.**
- **To delegate responsibility for changes to a third-party provider.**
- **To eliminate all cybersecurity risks.**

Explanation

The primary objective of change management in cybersecurity is to minimize the impact of changes to security measures. Changes to security measures can

introduce new risks or increase existing ones, and can also disrupt an organization's operations if not implemented properly. Change management processes help to identify potential issues and plan for their mitigation, reducing the risk of disruption and ensuring that security measures continue to be effective.

Question 99: **Skipped**

Which of the following best describes the purpose of a data handling policy?

- **To prevent any access to data by employees.**
- **To delegate responsibility for data handling to a third-party provider.**
- **To ensure that data is accessible to all employees.**
- **To establish guidelines for the proper handling of data.**
- **(Correct)**

Explanation

The purpose of a data handling policy is to establish guidelines for the proper handling of data within an organization. This includes guidelines for data access, storage, transmission, and disposal, as well as guidelines for ensuring the confidentiality, integrity, and availability of

data. By establishing clear guidelines for data handling, organizations can reduce the risk of data breaches, ensure compliance with regulations, and protect their reputation.

Question 100: **Skipped**

What is the purpose of Crime Prevention Through Environmental Design (CPTED)?

- **To increase crime through physical design and management of the built environment**
- **To decrease crime through physical design and management of the built environment**
- **(Correct)**
- **To increase crime through law enforcement practices**
- **To have no impact on crime through physical design and management of the built environment**

Explanation

Crime Prevention Through Environmental Design (CPTED) is an evidence-based crime prevention strategy that aims to reduce crime through design and management of the built environment. It uses physical design and management practices to increase natural surveillance, reduce opportunities for crime, and create a sense of community ownership and pride in the built environment.

Question 101: **Skipped**

What is the process of protecting confidential information called?

- **Data protection**
- **(Correct)**
- **Data encryption**
- **Data backup**
- **Data recovery**

Explanation

Data protection is the process of protecting confidential information from unauthorized access or disclosure. This can include a variety of measures, such as encryption, access controls, user authentication, and physical security, among others. The goal of data protection is to maintain the confidentiality of the information and ensure that it remains private and secure.

Question 102: **Skipped**

Which of the following protocols is used for secure email communication?

- **POP3**
- **(Correct)**
- **IMAP**

- **HTTPS**
- **SMTP**

Explanation

POP3 (Post Office Protocol version 3) is used for receiving email messages from a server. When used with SSL/TLS encryption, it can provide secure email communication. SMTP (Simple Mail Transfer Protocol) is used for sending email messages, and can also be used with SSL/TLS encryption.

Question 103: **Skipped**

What is the main purpose of implementing dual control in a security system?

- **To reduce the risk of unauthorized access**
- **(Correct)**
- **To reduce the risk of data breaches**
- **To increase efficiency**
- **To increase transparency**

Explanation

Dual control is a security control in which access to a resource is granted only when two or more authorized individuals provide their approval. The main purpose of

dual control is to reduce the risk of unauthorized access and improve the security of sensitive information.

Question 104: **Skipped**

In an organization that uses RBAC, a user with administrative privileges is leaving the organization. What is the recommended action to ensure that access permissions are appropriately adjusted?

- **All roles with administrative privileges should be deleted.**
- **The user should be required to transfer administrative privileges to another user.**
- **The user's role should be modified to remove administrative privileges.**
- **(Correct)**
- **The user's access permissions should be revoked.**

Explanation

Role-based access control (RBAC) is an access control mechanism that is based on the user's role or job function within an organization. Access permissions are assigned to roles, and users are granted access based on their role. RBAC provides a number of benefits, including increased security and easier management of access permissions.

In an organization that uses RBAC, access permissions can be adjusted based on changes to a user's role or responsibilities. Temporary access can be granted by assigning a new role to a user, and access permissions can be revoked by modifying the user's role. When a user with administrative privileges is leaving the organization, their role should be modified to remove administrative privileges to ensure that access permissions are appropriately adjusted.

Question 105: **Skipped**

What is the purpose of having a disaster recovery plan in an organization?

- **To ensure the integrity of information**
- **To ensure the confidentiality of information**
- **To ensure the security of information**
- **To ensure the availability of information**
- **(Correct)**

Explanation

A disaster recovery plan is an important aspect of information security that helps to ensure the availability of information and services in the event of a disaster or other interruption. The plan outlines the procedures and

processes that an organization will follow to restore critical systems and services to normal operation as quickly as possible. The disaster recovery plan helps to ensure the availability of information and services, which is essential for the continued operation of the organization.

Question 106: **Skipped**

Which of the following is a major difference between IPv4 and IPv6?

- **IPv6 does not support multicast, while IPv4 does.**
- **IPv6 uses a simplified header compared to the header used in IPv4.**
- **(Correct)**
- **IPv6 uses 32-bit addresses, while IPv4 uses 128-bit addresses.**
- **IPv6 is backward compatible with IPv4, while IPv4 is not backward compatible with IPv6.**

Explanation

One of the major differences between IPv4 and IPv6 is that the IPv6 header is simplified compared to the IPv4 header, which improves performance and reduces processing

overhead. IPv6 also supports multicast and is not fully backward compatible with IPv4.

Question 107: **Skipped**

Which of the following is a limitation of MAC?

- **It can be difficult to implement and manage.**
- **It can be easily circumvented by malicious users.**
- **It can be too rigid and inflexible.**
- **(Correct)**
- **It can result in users having too much access to resources.**

Explanation

Mandatory Access Control (MAC) is a security mechanism that provides a centralized authority with control over access to resources based on predefined policies. In a MAC system, the central authority sets and enforces access controls, and users cannot change their own access permissions. The main benefit of implementing a MAC system is that it provides a high level of security and control over access to resources. However, one of the limitations of MAC is that it can be too rigid and inflexible, making it difficult to make changes to access permissions or to accommodate new access requirements. It is

important to implement other security mechanisms, such as Role-Based Access Control and the Principle of Least Privilege, in conjunction with MAC to ensure that access is granted at the appropriate level.

Question 108: **Skipped**

What are some best practices for data destruction?

- **Only deleting data when storage space is needed.**
- **Developing and implementing a data destruction policy, training employees on data destruction, and regularly auditing data destruction practices.**
- **(Correct)**
- **Storing all data indefinitely, regardless of its importance or sensitivity.**
- **None**

Explanation

Best practices for data destruction include developing and implementing a data destruction policy that outlines the organization's data destruction procedures, training employees on data destruction best practices, and regularly auditing data destruction practices to ensure compliance with policy and legal requirements. Additionally, organizations should consider using multiple

methods of data destruction to ensure that the data is properly erased or destroyed.

Question 109: **Skipped**

What is the main difference between a private cloud and a public cloud?

- **A public cloud is hosted by a third-party provider, while a private cloud is dedicated to a single organization**
- **(Correct)**
- **A private cloud is only accessible from a single location**
- **A public cloud is less secure than a private cloud**
- **A private cloud is more expensive than a public cloud**

Explanation

A public cloud is hosted by a third-party provider, while a private cloud is dedicated to a single organization. Private clouds are typically more expensive than public clouds due to the additional infrastructure and resources required to maintain them.

Question 110: **Skipped**

Which of the following is an example of a logical access control mechanism?

- **A security camera**
- **A security guard**
- **A biometric authentication system**
- **Role-based access control**
- **(Correct)**

Explanation

Role-based access control (RBAC) is an example of a logical access control mechanism, which is a type of access control that uses software-based tools to regulate access to resources.

Question 111: **Skipped**

What is the primary advantage of a Next-Generation Firewall that includes a sandboxing component?

- **It can detect and block zero-day threats that have not yet been identified.**
- **(Correct)**
- **It can prioritize and allocate bandwidth to critical applications.**
- **It can block known malware and viruses from entering the network.**
- **It can provide visibility into application usage and performance.**

Explanation

A sandboxing component of a Next-Generation Firewall can analyze suspicious files and URLs in a safe, isolated environment to determine if they are malicious. This allows the firewall to detect and block previously unknown threats that may evade traditional detection methods.

Question 112: **Skipped**

What type of lock is best for securing valuable items inside a building?

- **Keyed lock**
- **Smart lock**
- **Deadbolt lock**
- **(Correct)**
- **Padlock**

Explanation

Deadbolt locks are best for securing valuable items inside a building as they provide the highest level of security. Deadbolts typically have a longer and stronger bolt that extends further into the door frame, making it more difficult for a would-be intruder to force the door open. They are also difficult to pick, adding an extra layer of security for valuable items.

Question 113: **Skipped**

What is the territorial scope of the General Data Protection Regulation (GDPR)?

- **Applies to data controllers and processors located inside/outside the EU if they offer goods or services to data subjects within the EU**
- **(Correct)**
- **Applies only to data controllers located within the EU**
- **Applies only to data controllers and processors located within the European Union (EU)**
- **Applies only to data processors located within the EU**

Explanation

The GDPR applies to data controllers and processors located inside/outside the EU if they offer goods or services to data subjects within the EU. This means that organizations that process the personal data of EU citizens, regardless of their location, must comply with the provisions of the GDPR.

Question 114: **Skipped**

Which of the following is one of the roles of the IT department in an IT business continuity plan?

- **To provide technical expertise for the plan**
- **To develop and implement the plan**
- **(Correct)**

- **To ensure that the plan is tested regularly**
- **To provide overall direction and support for the plan**

Explanation

The IT department has several key roles in an IT business continuity plan, one of which is to develop and implement the plan. The IT department should ensure that the plan is comprehensive, technically sound, and aligned with the overall goals and objectives of the organization. The IT department should also be responsible for ensuring that the plan is tested regularly and that any necessary updates are made in a timely manner.

Question 115: **Skipped**

What is the role of employee training in implementing a data handling policy?

- **To ensure that all employees understand the guidelines for data handling.**
- **(Correct)**
- **To delegate responsibility for data handling to a third-party provider.**
- **To ensure that all employees have access to all data.**
- **To prevent employees from accessing data.**

Explanation

Employee training is a critical component of implementing a data handling policy. By ensuring that all employees understand the guidelines for data handling, organizations can reduce the risk of data breaches and ensure compliance with regulations. Training can also help to increase employee awareness of the importance of data security, which can help to reduce the likelihood of human error or intentional misconduct.

Question 116: **Skipped**

What is the purpose of privacy policies in the context of information security?

- **To ensure organizations are transparent about how they collect, use, and share personal information.**
- **(Correct)**
- **To provide individuals with control over their personal information.**
- **To protect sensitive information from unauthorized disclosure.**
- **To promote trust and confidence in the use of technology.**

Explanation

The purpose of privacy policies in the context of information security is to ensure organizations are

transparent about how they collect, use, and share personal information. Privacy policies help to set out an organization's commitment to privacy, and to provide individuals with information about what personal information is being collected, how it is being used, and who it is being shared with. Privacy policies are an important aspect of privacy in the context of information security, as they help to promote trust and confidence in the use of technology.

Question 117: **Skipped**

What are some common attributes used in Attribute-Based Access Control (ABAC) policies?

- **User age, gender, and location.**
- **User ID, department, and clearance level.**
- **(Correct)**
- **User interests, education level, and marital status.**
- **User role, job title, and organization.**

Explanation

Attribute-Based Access Control (ABAC) is a method of access control that uses attributes of users, objects, and the environment to make access control decisions. ABAC evaluates attributes such as user role, job title,

department, location, time, device type, resource type, and other contextual information to determine whether access should be granted or denied. The policies used in ABAC are typically defined using a set of rules or logical statements that specify the conditions under which access should be granted. This approach offers more granular control over access to resources than some other access control models, such as Role-Based Access Control (RBAC). ABAC is often used in large, complex environments where access control requirements are diverse and constantly changing.

Question 118: **Skipped**

What are some common authentication methods used in cybersecurity?

- **Encryption, compression, and error correction**
- **Passwords, biometrics, and smart cards**
- **(Correct)**
- **Network address translation, virtual private networks, and proxy servers**
- **Firewalls, intrusion detection systems, and antivirus software**

Explanation

Passwords, biometrics, and smart cards are common authentication methods used in cybersecurity. Passwords are the most widely used method of authentication and are simple and convenient to use. Biometrics involves the use of unique physical characteristics, such as fingerprints or facial recognition, for authentication. Smart cards contain a microprocessor that stores digital certificates and can be used for secure authentication.

Question 119: **Skipped**

Which of the following is a key component of a strong password policy?

- **Allowing users to reuse previous passwords.**
- **Mandating passwords that are at least 6 characters long.**
- **Mandating complex passwords with a mix of characters, symbols, and numbers.**
- **(Correct)**
- **Allowing employees to share their passwords.**

Explanation

A key component of a strong password policy is mandating complex passwords with a mix of characters, symbols, and numbers. Passwords that include these

elements are generally more difficult to guess or crack using automated tools. Allowing users to reuse previous passwords or mandating shorter passwords can increase the risk of a password being compromised. Allowing employees to share their passwords is also a security risk as it increases the likelihood of a password being compromised or misused.

Question 120: **Skipped**

Which of the following is a best practice for managing software updates and patches in a production environment?

- **Test updates and patches in a development environment before applying them to production**
- **(Correct)**
- **Apply all updates and patches as soon as they become available**
- **Apply updates and patches to all systems simultaneously**
- **Delay the installation of updates and patches until a critical issue is discovered**

Explanation

It is important to test updates and patches in a non-production environment before applying them to

production to ensure that they do not cause any unexpected issues. Applying updates and patches as soon as they become available without testing them can lead to system downtime and other issues. It is also not recommended to delay the installation of updates and patches, as this can leave systems vulnerable to security threats. Instead, updates and patches should be applied in a timely manner after they have been tested in a non-production environment.

Question 121: **Skipped**

What is the difference between the OSI model and the TCP/IP model?

- **The OSI model has more layers than the TCP/IP model.**
- **(Correct)**
- **The TCP/IP model has more layers than the OSI model.**
- **The OSI model is a theoretical model, while the TCP/IP model is a practical implementation.**
- **The OSI model and the TCP/IP model are essentially the same.**

Explanation

The OSI model has seven layers, while the TCP/IP model has four layers. TCP/IP Model is a communication protocols suite using which network devices can be connected to the Internet. On the other hand, the OSI Model is a conceptual framework using which the functioning of a network can be described.

Question 122: **Skipped**

What is the primary benefit of using a Software as a Service (SaaS) cloud service model?

- **Reduced operational overhead and maintenance costs**
- **(Correct)**
- **Reduced software licensing costs**
- **Access to scalable and flexible computing resources**
- **Improved application development and deployment speed**

Explanation

Software as a Service (SaaS) is a cloud service model that provides users with access to a complete software application that is hosted and managed by a third-party provider. This can help reduce operational overhead and maintenance costs for the user, as they do not have to

manage the underlying infrastructure or perform software upgrades themselves. While SaaS can also provide benefits such as improved scalability and reduced licensing costs, the primary advantage is its ability to simplify software management.

Question 123: **Skipped**

What is the primary goal of Business Continuity (BC)?

- **To maintain the status quo during unexpected events**
- **To maintain operations during unexpected events**
- **(Correct)**
- **To maximize profits during unexpected events**
- **To minimize expenses during unexpected events**

Explanation

The primary goal of Business Continuity is to ensure that the essential functions of an organization are maintained during and after an unexpected event such as a disaster, cyber attack or other crisis. This helps to minimize the impact of the event on the organization, its stakeholders, and its customers.

Question 124: **Skipped**

Which of the following is not a component of change management?

- **Change evaluation and planning**
- **Change advisory board**
- **Change request management**
- **Service desk management**
- **(Correct)**

Explanation

Service desk management is not a component of change management. It is a separate process that involves providing support and assistance to end-users for IT-related issues.

Question 125: **Skipped**

Which of the following is NOT a requirement for maintaining Integrity in information security?

- **Logging and monitoring**
- **User authentication**
- **(Correct)**
- **Data backup**
- **Data backup**

Explanation

User authentication is not a requirement for maintaining Integrity in information security, although it is an important aspect of ensuring the security of the information. Integrity is mainly concerned with ensuring that the

information is accurate and complete, and that it has not been altered or corrupted in any way. The other options, such as data backup, logging and monitoring, and access controls, are all important requirements for maintaining Integrity in information security.

Question 126: **Skipped**

One of the below is not a purpose of having a communication plan in a disaster recovery plan?

- **To record phone messages during a disaster.**
- **(Correct)**
- **To document all communications during a disaster.**
- **To provide a framework for communicating with external parties.**
- **To ensure effective communication between stakeholders.**

Explanation

The purpose of having a communication plan in a disaster recovery plan is to ensure effective communication between stakeholders, document all communications during a disaster, and provide a framework for communicating with external parties. Option D, to record phone messages during a disaster, is incorrect as

recording phone messages is not the primary purpose of a communication plan in a disaster recovery plan. The communication plan is designed to ensure that all stakeholders have access to accurate and up-to-date information during a disaster, and to minimize confusion and misunderstandings.

Question 127: **Skipped**

What is the difference between a log and an event?

- **A log is a specific occurrence, while an event is a record of events**
- **A log is a record of events, while an event is a specific occurrence**
- **(Correct)**
- **A log and an event are the same thing**
- **A log is a record of security-related events, while an event is a record of all types of events**

Explanation

A log is a record of events that occur on a system or network, while an event is a specific occurrence that is captured in a log. For example, a login attempt is an event, while the record of all login attempts is a log. Option (b) is

incorrect because it incorrectly defines a log as a specific occurrence.

Question 128: **Skipped**

Company QRS is implementing a new IT system and is concerned about potential security breaches. Which security control should be implemented to ensure that access to the system is restricted to only those who need it?

- **Segregation of Duties and the Principle of Least Privilege**
- **(Correct)**
- **None of the above.**
- **Principle of Least Privilege**
- **Segregation of Duties**

Explanation

Both the Segregation of Duties and the Principle of Least Privilege are important security controls that help ensure that access to resources is restricted to only those who need it. The Segregation of Duties divides responsibilities among multiple employees, while the Principle of Least Privilege grants employees access to the minimum resources necessary to perform their job functions. Both

of these controls can help reduce the risk of fraud, errors, and security breaches, and limit the potential damage from a breach or human error. The specific control that should be implemented depends on the nature of the resource or process being protected, as well as the potential risks and threats.

Question 129: **Skipped**

Which of the following is a key principle of Mandatory Access Control (MAC)?

- **Access to resources is determined by the user.**
- **Access to resources is determined by the system based on security labels.**
- **(Correct)**
- **Users are given access to resources at the discretion of the system owner.**
- **Access to resources is based on the user's job function.**

Explanation

Mandatory Access Control (MAC) is an access control mechanism that uses security labels to determine who can access resources. Access to resources is determined by the system based on security labels, which are

assigned to users and resources based on their security clearance.

Question 130: **Skipped**

What is an example of using something the user knows as an authentication factor in MFA?

- **A security token**
- **A smart card**
- **A fingerprint scan**
- **A password**
- **(Correct)**

Explanation

A password is an example of something the user knows that can be used as an authentication factor in MFA. Passwords are widely used and are a convenient method of verifying the identity of a user. However, passwords can be easily guessed or stolen, so they are often used in combination with other authentication factors for added security.

Question 131: **Skipped**

What is the purpose of using digital signatures in information security?

- **To provide integrity**

- **To provide authenticity**
- **(Correct)**
- **To provide confidentiality**
- **To provide availability**

Explanation

Digital signatures are used in information security to provide authenticity and integrity for electronic transactions and communications. A digital signature is a unique representation of the information that is generated using a private key and verified using a public key. The digital signature verifies the authenticity of the information and confirms that it has not been altered in any way during transmission.

Question 132: **Skipped**

How can data classification and labeling help with data governance and compliance?

- **By reducing the risk of data breaches and loss of intellectual property.**
- **All options**
- **(Correct)**
- **By demonstrating that the organization is handling data in a responsible and compliant manner.**

- **By providing a way to easily identify and track data based on its regulatory requirements.**

Explanation

Data classification and labeling can help organizations maintain good data governance practices and comply with regulatory requirements by reducing the risk of data breaches and loss of intellectual property, providing a way to easily identify and track data based on its regulatory requirements, and demonstrating that the organization is handling data in a responsible and compliant manner.

Question 133: **Skipped**

A company recently implemented a zero trust security model and an employee is attempting to access a sensitive database from their personal laptop at home. What action should the company take?

- **Require the employee to come into the office to access the database**
- **Deny access as the employee is not accessing from a company device**
- **Allow access as the employee is authorized to access the database**
- **Request the employee to use a VPN to access the database**

- **(Correct)**

Explanation

Zero trust security model assumes that no user or device can be trusted automatically, regardless of their location or authorization level. The employee's personal laptop is not a trusted device, and allowing access can lead to potential security risks. Therefore, the best practice is to request the employee to use a VPN, which can establish a secure connection between the laptop and the company's network, and ensure the employee is authenticated before accessing the database.

Question 134: **Skipped**

What is a Public IP Address?

- **An IP address that is reserved for use in a private network**
- **An IP address that is assigned by an internet service provider (ISP)**
- **An IP address that is used by a network router to connect to the internet**
- **An IP address that is publicly accessible on the internet**
- **(Correct)**

Explanation

A public IP address is a unique address that is assigned to a device on the internet. It is publicly accessible and can be used to connect to the device from anywhere in the world. Public IP addresses are assigned by an ISP and are used to identify devices on the internet.

Question 135: **Skipped**

What is the main purpose of a mantrap in physical security?

- **To store hazardous materials**
- **To serve as a waiting room**
- **To store valuable assets**
- **To allow entry of only one person at a time**
- **(Correct)**

Explanation

A mantrap is a secure room that allows the entry of only one person at a time. It is used to prevent unauthorized access and increase the level of security in high-risk areas by controlling the flow of people entering and exiting.

Question 136: **Skipped**

Which of the following is an advantage of using symmetric encryption algorithms?

- **They do not require a shared secret key**

- **They are more secure than asymmetric encryption algorithms**
- **They can be used for digital signatures and key exchange**
- **They are faster and more efficient than asymmetric encryption algorithms**
- **(Correct)**

Explanation

Symmetric encryption algorithms are generally faster and more efficient than asymmetric encryption algorithms because they do not involve complex mathematical operations or large key sizes. However, symmetric encryption algorithms require a shared secret key, which must be kept secure between the parties involved. Asymmetric encryption algorithms, on the other hand, do not require a shared secret key but are slower and less efficient.

Question 137: **Skipped**

What is the importance of testing an IT business continuity plan?

- **To identify and resolve potential problems before a disaster occurs**

- **To ensure that the plan is up-to-date and relevant to current business operations**
- **To determine the effectiveness of the plan in the event of a disaster**
- **All of the above**
- **(Correct)**

Explanation

Testing an IT business continuity plan is important for several reasons. It helps to identify and resolve potential problems before a disaster occurs, determine the effectiveness of the plan in the event of a disaster, and ensure that the plan is up-to-date and relevant to current business operations. Regular testing of the plan is essential to ensure its readiness and effectiveness in the event of a disaster.

Question 138: **Skipped**

How can security awareness training be integrated into everyday work activities?

- **By providing ongoing reminders and updates about security best practices through email or messaging systems**
- **(Correct)**

- **By providing employees with security-related tasks to complete as part of their job responsibilities**
- **By hosting regular in-person seminars or workshops**
- **By requiring employees to complete a training course before accessing company resources**

Explanation

Security awareness training can be integrated into everyday work activities by providing ongoing reminders and updates about security best practices through email or messaging systems. This approach can help reinforce key concepts and encourage employees to stay vigilant about security threats.

Question 139: **Skipped**

What is the primary function of a firewall in a network?

- **To filter and block unwanted network traffic**
- **(Correct)**
- **To provide wireless connectivity to devices**
- **To forward data between different networks**
- **To connect multiple devices in a LAN**

Explanation

A firewall is a security device that is used to filter and block unwanted network traffic. It can be used to protect a network from unauthorized access and to prevent attacks

such as denial-of-service (DoS) attacks and malware infections.

Question 140: **Skipped**

What type of gate is best for secure entry and exit to a property?

- **Automatic gate**
- **(Correct)**
- **Barrier gate**
- **Roll-up gate**
- **Ornamental iron gate**

Explanation

Automatic gates provide secure entry and exit to a property by controlling who has access and when. They can be integrated with security systems, such as card readers or biometric scanners, to further enhance security.

Question 141: **Skipped**

What is the first canon of the (ISC)² Code of Ethics?

- **Provide diligent and competent service to principals.**
- **Act honorably, honestly, justly, responsibly, and legally.**
- **Protect society, the common good, necessary public trust and confidence, and the infrastructure.**
- **(Correct)**

- **Advance and protect the profession.**

Explanation

The first canon of the (ISC)² Code of Ethics is "Protect society, the common good, necessary public trust and confidence, and the infrastructure." This means that the first priority for a cybersecurity professional is to ensure the safety and security of the public and their interests, and to maintain the trust and confidence placed in the professional.

Question 142: **Skipped**

What types of businesses or organizations are most likely to benefit from working with a managed service provider (MSP)?

- **Businesses with highly specialized IT requirements**
- **Small businesses with limited IT resources**
- **All options**
- **(Correct)**
- **Large organizations with complex IT needs**

Explanation

MSPs can provide benefits to a wide range of businesses and organizations, including small businesses with limited IT resources, large organizations with complex IT needs,

and businesses with highly specialized IT requirements. By working with an MSP, organizations can access specialized expertise and resources that they may not have in-house, while also reducing costs and improving efficiency.

Question 143: **Skipped**

What is one of the most important steps in protecting against ransomware attacks?

- **Being cautious of suspicious emails and websites**
- **Regularly backing up important data**
- **(Correct)**
- **Installing anti-virus software**
- **Keeping software up-to-date**

Explanation

Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for a decryption key. Backing up important data regularly is crucial in protecting against ransomware attacks, as it allows a user to restore their data if their files become encrypted. This helps mitigate the impact of a ransomware attack and reduces the chances of the victim being forced to pay the ransom.

Question 144: **Skipped**

Which of the following is an example of a technical control?

- **Background checks for employees**
- **Employee training programs**
- **Firewall**
- **(Correct)**
- **Physical locks on doors**

Explanation

A firewall is an example of a technical control because it is a software-based security measure that is designed to protect a network from unauthorized access. It works by enforcing rules and policies that dictate which types of incoming and outgoing network traffic are allowed.

Question 145: **Skipped**

What are some common physical security controls used in an organization?

- **Access control systems**
- **Surveillance cameras**
- **All of the above**
- **(Correct)**
- **Fire suppression systems**

Explanation

Common physical security controls used in organizations include access control systems, which restrict access to sensitive areas based on authorization, surveillance cameras, which monitor physical activity and provide a record of security incidents, and fire suppression systems, which prevent fires from spreading and protect equipment and other assets.

Question 146: **Skipped**

What is Egress monitoring?

- **Monitoring outgoing network traffic to detect and prevent unauthorized access**
- **(Correct)**
- **Monitoring the performance of network devices to detect and prevent unauthorized access**
- **Monitoring incoming network traffic to detect and prevent unauthorized access**
- **Monitoring the behavior of network users to detect and prevent unauthorized access**

Explanation

Egress monitoring is the practice of monitoring outgoing network traffic to detect and prevent unauthorized access to an organization's network resources. This can include monitoring for data exfiltration attempts, unauthorized

access to sensitive resources, and the use of unauthorized network services.

Question 147: **Skipped**

What is the primary goal of risk management?

- **To minimize the impact of risks**
- **(Correct)**
- **To increase risk exposure**
- **To maximize profits**
- **To eliminate all risks**

Explanation

The primary goal of risk management is to minimize the impact of risks. Risk management is the process of identifying, assessing, and controlling risks faced by an organization. The goal of risk management is not to eliminate all risks, as this is not always possible, but to minimize the impact of risks so that the organization can continue to operate effectively and efficiently. By minimizing the impact of risks, organizations can reduce the likelihood of negative events occurring and minimize the impact of those that do occur.

Question 148: **Skipped**

What is data destruction, and why is it important for organizations?

- **Data destruction is the process of permanently erasing or destroying data, and it is important for organizations because it helps them protect sensitive or confidential information from unauthorized access or disclosure.**
- **(Correct)**
- **Data destruction is not important for organizations.**
- **Data destruction is the process of encrypting data, and it is important for organizations because it ensures that the data is protected from hackers and other cyber threats.**
- **Data destruction is the process of temporarily deleting data, and it is important for organizations because it helps them free up storage space.**

Explanation

Data destruction is an important aspect of data management because it helps organizations ensure that sensitive or confidential information is not accessible to unauthorized individuals, even after the data is no longer needed. This is especially important for organizations that

handle sensitive information, such as financial institutions, healthcare providers, or government agencies.

Question 149: **Skipped**

What is the purpose of the remediation step in incident response?

- **To implement a solution to the incident.**
- **(Correct)**
- **To notify relevant parties of the incident.**
- **To determine the cause of the incident.**
- **To stop the incident from spreading.**

Explanation

The purpose of the remediation step in incident response is to implement a solution to the incident. This may involve patching systems, restoring data, or other measures to address the underlying cause of the incident and prevent it from happening again in the future.

Question 150: **Skipped**

What is the difference between a packet filtering firewall and a stateful firewall?

- **Packet filtering firewalls do not maintain state information, while stateful firewalls maintain state information.**

- (Correct)
- **Packet filtering firewalls use deep packet inspection to filter traffic, while stateful firewalls use basic packet filtering.**
- **Packet filtering firewalls filter traffic based on application layer protocols, while stateful firewalls filter traffic based on network layer protocols.**
- **Packet filtering firewalls filter traffic based on network layer protocols, while stateful firewalls filter traffic based on application layer protocols.**

Explanation

Packet filtering firewalls filter traffic based on rules that are applied to individual packets, without maintaining state information about the connection. Stateful firewalls, on the other hand, maintain state information about connections and can use this information to filter traffic more effectively. By maintaining state information, stateful firewalls can also provide additional security features, such as intrusion prevention and application layer filtering.

Question 151: **Skipped**

Which of the following is NOT a requirement for maintaining Confidentiality in information security?

- **User authentication**

- **Access control policies**
- **Data backup**
- **(Correct)**
- **Physical security**

Explanation

Data backup is not a requirement for maintaining Confidentiality in information security, although it is an important aspect of ensuring data availability and disaster recovery. Confidentiality is mainly concerned with the protection of sensitive or confidential information from unauthorized access or disclosure. The other options, such as access control policies, user authentication, and physical security, are all important requirements for maintaining Confidentiality in information security.

Question 152: **Skipped**

An organization is trying to determine the potential impact of a natural disaster on its operations. What type of risk assessment tool would be the most appropriate to use in this scenario?

- **Qualitative risk assessment**
- **Both quantitative and qualitative risk assessment**
- **(Correct)**

- **Quantitative risk assessment**
- **Digital risk assessment**

Explanation

In this scenario, it would be appropriate to use both quantitative and qualitative risk assessment tools. A qualitative assessment would be used to identify the potential risks posed by the natural disaster, while a quantitative assessment would be used to determine the potential financial impact. This would help the organization to develop a more comprehensive risk management plan, which would include measures to reduce the likelihood of the disaster occurring and to minimize its impact if it were to occur.

Question 153: **Skipped**

What is the purpose of physical security controls in an organization?

- **To protect against unauthorized access to physical assets.**
- **(Correct)**
- **To protect against all of the above.**
- **To protect against environmental hazards.**
- **To protect against cyber threats.**

Explanation

Physical security controls are designed to protect against unauthorized access to physical assets, such as buildings, equipment, and sensitive data. They help to ensure that only authorized individuals have access to these assets, and prevent unauthorized access that could result in theft, damage, or other security incidents.

Question 154: **Skipped**

Your organization is about to embark on a major IT project that involves the implementation of new software. What risk management strategy would you recommend to minimize the impact of risks associated with the project?

- **Implementing controls to reduce the likelihood of risks occurring**
- **(Correct)**
- **Ignoring the risks and hoping for the best**
- **Transferring the risk to another party**
- **Eliminating all risks**

Explanation

When embarking on a major IT project, it is important to minimize the impact of risks associated with the project. One effective way to do this is by implementing controls to

reduce the likelihood of risks occurring. This could involve conducting a risk assessment to identify potential risks and then implementing controls, such as project management methodologies and quality assurance processes, to reduce the likelihood of these risks occurring. By reducing the likelihood of risks occurring, organizations can minimize the impact of risks and ensure the success of the project.

Question 155: **Skipped**

What is the second canon of the (ISC)² Code of Ethics?

- **Advance and protect the profession.**
- **Act honorably, honestly, justly, responsibly, and legally.**
- **(Correct)**
- **Provide diligent and competent service to principals.**
- **Protect society, the common good, necessary public trust and confidence, and the infrastructure.**

Explanation

The second canon of the (ISC)² Code of Ethics is "Act honorably, honestly, justly, responsibly, and legally." This means that cybersecurity professionals must act in an ethical and lawful manner in all aspects of their work and

conduct themselves in a manner that is consistent with the principles of honesty and integrity.

Question 156: **Skipped**

Which of the following is an example of implementing the Principle of Least Privilege?

- **Limiting access to a file server to only those who need to use it for their job.**
- **(Correct)**
- **Giving all employees administrative access to their computers.**
- **Restricting access to sensitive information only to the CEO.**
- **Granting all employees access to the company's financial records.**

Explanation

Limiting access to a file server to only those who need to use it for their job is an example of implementing the Principle of Least Privilege. This ensures that employees only have access to the resources they need to do their job, which reduces the risk of unauthorized access or data breaches.

Question 157: **Skipped**

Which of the following parties is responsible for drafting a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA)?

- **Both parties involved in the agreement**
- **(Correct)**
- **The legal department of one of the parties involved in the agreement**
- **The party with the most negotiating power**
- **The party with the most to gain from the agreement**

Explanation

Both parties involved in the agreement are responsible for drafting a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA) and ensuring that the terms are acceptable to all parties involved.

Question 158: **Skipped**

One of the below is uncommon types of security events that should be logged and monitored?

- **Login attempts and failures**
- **Power outages**
- **(Correct)**
- **Malware infections**
- **Changes to system configurations**

Explanation

Login attempts and failures, changes to system configurations, and malware infections are all common types of security events that should be logged and monitored. By monitoring these events, organizations can identify potential security threats and take appropriate action to mitigate them. Power outages is incorrect because it is not related to security events.

Question 159: **Skipped**

Your company is planning to implement two-factor authentication (2FA) for its employees. What is the main advantage of 2FA over traditional password-based authentication?

- **2FA eliminates the risk of password theft**
- **2FA provides stronger security for the company's sensitive information**
- **(Correct)**
- **2FA eliminates the need for employees to remember their passwords**
- **2FA is more convenient for employees**

Explanation

The main advantage of 2FA over traditional password-based authentication is that it provides stronger

security for the company's sensitive information. 2FA adds an additional layer of security beyond just a password by requiring the user to provide a second factor, such as a security token or a temporary code, to complete the authentication process. This makes it much harder for attackers to gain access to sensitive information, as they would need to not only guess the password, but also gain access to the second factor.

Question 160: **Skipped**

What is a privacy policy?

- **A legal document that outlines an organization's data protection practices and how it handles personal information**
- **(Correct)**
- **A marketing tool used by organizations to promote their products or services**
- **A document that outlines an organization's employee benefits and compensation policies**
- **A document that outlines an organization's financial policies and procedures**

Explanation

A privacy policy is a legal document that outlines how an organization collects, uses, stores, and shares personal

information, and how it protects the privacy rights of individuals.

Question 161: **Skipped**

What is the first step in incident response?

- **Remediation**
- **Identification**
- **(Correct)**
- **Analysis**
- **Containment**

Explanation

The first step in incident response is to identify the incident. This involves recognizing that an incident has occurred and collecting information about the nature and scope of the incident. This information can then be used to make decisions about how to respond to the incident.

Question 162: **Skipped**

What is the difference between phishing and spear phishing?

- **Phishing targets a large number of victims, while spear phishing targets only a small group or individual.**
- **(Correct)**

- **Phishing involves impersonating a well-known company or institution, while spear phishing involves impersonating a specific individual or organization.**
- **Phishing is always carried out through email, while spear phishing can involve other communication methods, such as social media or instant messaging.**
- **Phishing requires the use of advanced hacking techniques, while spear phishing relies on simple social engineering tactics.**

Explanation

Phishing attacks involve targeting a large number of victims with a generic message, while spear phishing attacks are targeted at a specific individual or group and often involve personalized messages or information. Both types of attacks can involve impersonating well-known companies or institutions and can be carried out through various communication methods.

Question 163: **Skipped**

Why is it important to regularly evaluate and update physical security controls?

- **To ensure they are still effective.**
- **To meet regulatory requirements.**
- **All of the above.**

- **(Correct)**
- **To keep up with advances in technology.**

Explanation

All of the above. It is important to regularly evaluate and update physical security controls to ensure they are still effective, keep up with advances in technology, and meet regulatory requirements. This helps to maintain the security of physical assets, and prevent security incidents that could result in theft, damage, or other security incidents.

Question 164: **Skipped**

What is the most important aspect of maintaining confidentiality in information security?

- **All of the above**
- **(Correct)**
- **Physical security**
- **Administrative security**
- **Technical security**

Explanation

Maintaining confidentiality in information security requires a combination of physical security, technical security, and administrative security. Physical security is concerned

with the protection of the information from physical threats, such as theft or damage. Technical security involves the use of encryption and other security controls to protect the information from unauthorized access or disclosure. Administrative security refers to the policies, procedures, and guidelines that regulate access to the information and ensure that it remains confidential. All of these aspects are important for maintaining confidentiality in information security.

Question 165: **Skipped**

Your company is looking to implement a more secure authentication system for its employees. Which of the following methods would provide the highest level of security?

- **Token-based authentication**
- **Biometric authentication**
- **(Correct)**
- **Password-based authentication**
- **Smart card authentication**

Explanation

Biometric authentication provides the highest level of security compared to other authentication methods.

Biometric authentication uses unique physical characteristics, such as fingerprints or iris scans, to verify the identity of a user. This method is secure as biometric characteristics are unique to each individual and cannot be easily stolen or guessed like passwords. However, biometric authentication may require specialized hardware and has potential privacy concerns.

Question 166: **Skipped**

Which of the following is a limitation of DAC?

- **It can result in users having too much access to resources.**
- **(Correct)**
- **It is too rigid and inflexible.**
- **It is difficult to implement and manage.**
- **It can be easily circumvented by malicious users.**

Explanation

One of the limitations of DAC is that it can result in users having too much access to resources. Since the owner of the resource has complete control over access permissions, they can grant access to users who may not need it, leading to a potential security risk.

Question 167: **Skipped**

Company ABC has a new project that requires access to sensitive information. Which security control should be implemented to ensure that access to this information is restricted to only those who need it?

- **None of the above.**
- **Principle of Least Privilege**
- **(Correct)**
- **Segregation of Duties**
- **Segregation of Duties and the Principle of Least Privilege**

Explanation

The Principle of Least Privilege should be implemented to ensure that access to the sensitive information is restricted to only those who need it. This control grants employees access to the minimum resources necessary to perform their job functions, which limits the potential damage from a security breach or human error.

Question 168: **Skipped**

What is the purpose of the separation of duties control in cybersecurity?

- **To increase employee motivation**
- **To improve the speed of tasks completion**

- **To reduce the risk of fraud and errors**
- **(Correct)**
- **To increase accountability for specific tasks**

Explanation

The purpose of the separation of duties control in cybersecurity is to reduce the risk of fraud and errors by ensuring that no single individual has complete control over a particular process or system. This helps to prevent malicious activities by limiting the potential damage that can be done by a single person.

Question 169: **Skipped**

What is encryption?

- **The process of converting plaintext into gibberish**
- **The process of converting ciphertext into plaintext**
- **The process of converting plaintext into ciphertext**
- **(Correct)**
- **The process of hiding information in plain sight**

Explanation

Encryption is the process of converting plaintext, which is readable and understandable information, into ciphertext, which is unreadable and unintelligible information. This is done using a mathematical algorithm and a key that

makes it possible to decipher the ciphertext back into plaintext.

Question 170: **Skipped**

Which of the following is a common way that zero-day attacks are discovered?

- **Through analysis of network traffic logs.**
- **Through analysis of malware samples.**
- **(Correct)**
- **Through user reporting of suspicious activity.**
- **Through monitoring of system performance metrics.**

Explanation

Zero-day attacks are often discovered through the analysis of malware samples collected from infected systems. This analysis can help identify previously unknown malware variants and the vulnerabilities they exploit. While network traffic logs, system performance metrics, and user reporting can also provide valuable information, they may not necessarily lead to the discovery of zero-day exploits.

Question 171: **Skipped**

What is the purpose of the (ISC)² Code of Ethics?

- **To promote competition in the marketplace**
- **To enforce compliance with laws and regulations**

- **To provide guidance for resolving conflicts of interest**
- **To set standards for professional behavior in the information security field**
- **(Correct)**

Explanation

The (ISC)² Code of Ethics is designed to set standards for professional behavior in the information security field.

Question 172: **Skipped**

Which type of control is focused on securing the physical environment and ensuring that access to systems and data is restricted to authorized individuals?

- **Physical controls**
- **(Correct)**
- **Technical controls**
- **Administrative controls**
- **All of the above**

Explanation

Physical controls are focused on securing the physical environment and ensuring that access to systems and data is restricted to authorized individuals. Examples of physical controls include security cameras, locked doors, and security personnel.

Question 173: **Skipped**

What is the purpose of testing a BCP?

- **To ensure that the plan is foolproof and cannot fail**
- **To assess the financial impact of a disaster on the organization**
- **To verify that the plan conforms to legal and regulatory requirements**
- **To identify weaknesses and improve the plan**
- **(Correct)**

Explanation

The purpose of testing a BCP is to identify weaknesses, its effectiveness and improve the plan. This helps to ensure that the plan is effective and can be implemented successfully in the event of a disaster.

Question 174: **Skipped**

What is an availability zone in cloud computing, and can it include multiple data centers?

- **An availability zone is a set of tools for managing cloud resources, and it does not involve physical data centers.**
- **An availability zone is a group of data centers within a region that share resources and provide high availability.**

- **An availability zone is a single data center within a region, but it can include multiple data centers for additional redundancy and fault tolerance.**
- **(Correct)**
- **An availability zone is a single data center within a region, and it cannot include multiple data centers.**

Explanation

While the primary definition of an availability zone is a single, physically isolated data center within a region, some cloud providers may choose to have multiple data centers within an availability zone to further improve fault tolerance and high availability. Regardless of the specific implementation, the key concept is that an availability zone is designed to provide additional resilience and minimize the impact of potential outages or disasters.

Question 175: **Skipped**

What is the difference between an information asset inventory and an information asset catalog?

- **There is no difference between an inventory and a catalog.**
- **An inventory is used for risk assessment, while a catalog is used for incident response.**

- **An inventory is a list of all information assets, while a catalog provides detailed information about each asset.**
- **(Correct)**
- **An inventory tracks the physical location of each asset, while a catalog tracks the logical location of each asset.**

Explanation

An information asset inventory is a list of all information assets, while an information asset catalog provides detailed information about each asset, such as the asset's owner, classification, criticality, and sensitivity.

Question 176: **Skipped**

A company is migrating to a cloud-based solution and is considering using a zero trust security model. Which of the following is a characteristic of zero trust security that would benefit the company's migration?

- **The model assumes all users and devices are trustworthy.**
- **Access control is based on user roles and permissions.**
- **The model relies on network segmentation to protect against threats.**

- **Continuous monitoring and analysis of user and device behavior is a core feature.**
- **(Correct)**

Explanation

Zero trust security model assumes that no user or device can be trusted automatically, and continuous monitoring and analysis of user and device behavior is crucial to detect any suspicious activities or anomalies. This is particularly important in a cloud-based solution, as the network perimeter is blurred and traditional security measures such as firewalls and network segmentation may not be sufficient. Therefore, implementing a zero trust security model that includes continuous monitoring can help detect and prevent potential security breaches.

Question 177: **Skipped**

In which scenario would a fail-safe mechanism be more appropriate?

- **When security is the top priority.**
- **(Correct)**
- **When both security and availability are important.**
- **When availability is the top priority.**
- **When neither security nor availability are important.**

Explanation

Fail-safe mechanisms are more appropriate when security is the top priority, as they allow systems to continue operating even if there is a failure. This is important in situations where shutting down the system could cause more harm than allowing it to continue operating in a safe state.

Question 178: **Skipped**

What should be considered during the post-incident review?

- **The cost of the incident response.**
- **The accuracy of the incident response plan.**
- **The response time to the incident.**
- **All of the above.**
- **(Correct)**

Explanation

During the post-incident review, a variety of factors should be considered, including the response time to the incident, the cost of the incident response, and the accuracy of the incident response plan. This helps to evaluate the effectiveness of the response and identify areas for improvement in the incident response process.

Question 179: **Skipped**

What is the difference between a magnetic stripe badge and a smart card badge system?

- **Magnetic stripe badges are more secure than smart card badges.**
- **Magnetic stripe badges are less secure than smart card badges.**
- **Smart card badges can only be used for physical access control, while magnetic stripe badges can be used for both physical and logical access control.**
- **Magnetic stripe badges can only be used for physical access control, while smart card badges can be used for both physical and logical access control.**
- **(Correct)**

Explanation

Magnetic stripe badges store a static magnetic stripe that can be read when swiped through a reader. This makes them suitable for physical access control but they lack the security features required for logical access control. Smart card badges, on the other hand, have a microprocessor chip that can store and process information. This makes them suitable for both physical and logical access control, making them a more secure option.

Question 180: **Skipped**

What is the most common physical security control used to secure high-security areas?

- **Perimeter fencing**
- **Video surveillance**
- **Access control systems**
- **(Correct)**
- **All of the above**

Explanation

Access control systems are the most common physical security control used to secure high-security areas. They typically use a combination of technologies such as biometrics, smart cards, and keypads to control who can enter and exit the area. Video surveillance and perimeter fencing are also important components of high-security areas, but access control systems play a key role in controlling access.

Question 181: **Skipped**

What is the purpose of a digital certificate in relation to digital signatures?

- **To provide access control to the message or document**

- **To prevent unauthorized modification of the message or document**
- **To encrypt the message or document**
- **To verify the identity of the signer**
- **(Correct)**

Explanation

A digital certificate is a document that contains information about the identity of the signer and is used to verify the authenticity of the digital signature.

Question 182: **Skipped**

In an organization that uses both DAC and MAC, which security mechanism takes precedence?

- **The order of precedence is determined by the resource owner.**
- **DAC takes precedence over MAC.**
- **MAC takes precedence over DAC.**
- **(Correct)**
- **Both mechanisms are equal in priority and function independently.**

Explanation

Discretionary Access Control (DAC) and Mandatory Access Control (MAC) are two different access control mechanisms that can be used in an organization. In a DAC

system, the owner of the resource has the authority to grant or deny access to other users. In a MAC system, access control is determined by a central authority based on predefined policies. When both mechanisms are used in an organization, MAC takes precedence over DAC. This is because MAC is a more stringent access control mechanism, and its policies must be followed even if the owner of the resource has granted access to the user. In contrast, DAC is a more permissive mechanism, and its policies can be overridden by the central authority in a MAC system.

Question 183: **Skipped**

Which of the below is a security property that ensures that the origin of a message or transaction cannot be denied?

- **Non-repudiation**
- **(Correct)**
- **Confidentiality**
- **Integrity**
- **Availability**

Explanation

Non-repudiation is a security property that ensures that the origin of a message or transaction cannot be denied. The objective of non-repudiation is to provide proof of the authenticity of the source of a message or transaction, so that the recipient can be confident that it came from the claimed source and has not been altered in transit.

Question 184: **Skipped**

What is the Principle of Least Privilege?

- **A security control that grants employees access to all resources they request.**
- **A security control that ensures all employees have the same level of access to resources.**
- **A security control that ensures employees have access to the minimum resources necessary to perform their job functions.**
- **(Correct)**
- **A security control that grants employees access to resources based on their job title.**

Explanation

The Principle of Least Privilege is a security control that ensures employees have access to the minimum resources necessary to perform their job functions. This

helps limit potential damage from a security breach or human error.

Question 185: **Skipped**

What is the purpose of surveillance cameras in physical security control?

- **To deter theft and vandalism**
- **To enforce security policies**
- **To capture images of suspicious behavior**
- **(Correct)**
- **To monitor the entry and exit of personnel**

Explanation

The primary purpose of surveillance cameras in physical security control is to capture images of any suspicious behavior, so that the authorities can use it for investigation or evidence.

Question 186: **Skipped**

What is the primary purpose of a Virtual Private Network (VPN)?

- **To segment a physical network into multiple logical networks**
- **To encrypt network traffic between two endpoints**
- **(Correct)**

- **To provide redundancy and high availability for critical network resources**
- **To provide remote access to the network**

Explanation

VPNs allow organizations to provide secure, encrypted communication between two endpoints over an untrusted network, such as the internet.

Question 187: **Skipped**

Which of the following is a potential security risk associated with Virtual Local Area Networks (VLANs)?

- **Unauthorized access to confidential data**
- **(Correct)**
- **Interference between different logical networks**
- **Lack of visibility into network traffic**
- **Increased network latency**

Explanation

Virtual Local Area Networks (VLANs) can be a potential security risk if they are not properly configured, as attackers may be able to use them to gain access to confidential data that is not intended for their use. This risk can be mitigated through proper configuration and monitoring of the VLANs.

Question 188: **Skipped**

What is the primary function of bollards in physical security?

- **To protect against unauthorized entry or vehicle access**
- **(Correct)**
- **To secure buildings and outdoor areas**
- **To provide shade**
- **To direct traffic flow**

Explanation

The primary function of bollards in physical security is to serve as a barrier for buildings and outdoor areas to protect against unauthorized entry or vehicle access.

Question 189: **Skipped**

Which of the following is a key element of an effective SLA?

- **Ambiguous service availability guarantees.**
- **Vague, non-specific language.**
- **A lack of clear responsibilities for the service provider and the client.**
- **Clear, measurable performance metrics.**
- **(Correct)**

Explanation

An effective SLA (Service Level Agreement) should include clear, measurable performance metrics that allow both parties to assess whether the service is being delivered as promised, and to identify areas for improvement or dispute resolution. Vague or ambiguous language, as well as unclear responsibilities, can lead to misunderstandings and disagreements between the parties.

Question 190: **Skipped**

What is the primary difference between a hot site and a warm site?

- **A hot site is more expensive than a warm site.**
- **A hot site is used for short-term recovery while a warm site is used for long-term recovery.**
- **A hot site is located close to the main facility while a warm site is located farther away.**
- **A hot site is fully functional while a warm site is partially functional.**
- **(Correct)**

Explanation

A hot site is a fully operational backup facility that is ready to take over the operations of a business in the event of a disaster. A warm site has some limited functionality, such

as basic infrastructure, but may require some additional time to be fully operational.

Question 191: **Skipped**

Which of the following is an important consideration when implementing system hardening measures?

- **System performance should always be prioritized over security.**
- **All security measures should be disabled when performing software updates.**
- **System hardening measures should be tested and evaluated to ensure that they are effective.**
- **(Correct)**
- **Password policies should be relaxed to make it easier for users to access the system.**

Explanation

Implementing system hardening measures without testing and evaluating their effectiveness can lead to unexpected consequences, such as system downtime, user access issues, or increased risk of attacks. System performance should not be prioritized over security, and security measures should not be disabled during software updates. Password policies should not be relaxed as this can weaken the security of the system.

Question 192: **Skipped**

Which of the following is an example of a physical control?

- **Employee training programs**
- **Physical locks on doors**
- **(Correct)**
- **Background checks for employees**
- **Firewall**

Explanation

Physical locks on doors are an example of a physical control because they are a tangible barrier that is designed to prevent unauthorized access to a building or room. They are typically used in conjunction with other security measures, such as access control systems, to provide a comprehensive security solution.

Question 193: **Skipped**

Which of the following fire suppression systems uses water as the extinguishing agent?

- **Halon**
- **Wet chemical**
- **Dry chemical**
- **Sprinkler**
- **(Correct)**

Explanation

Sprinkler systems use water as the extinguishing agent to suppress fires. The water is discharged when a heat-sensitive element in the system is activated.

Question 194: **Skipped**

What does "safety first" mean in the workplace?

- **Safety is the responsibility of individual employees, not the organization**
- **Safety is important, but productivity is more important**
- **Safety is the top priority in all work activities**
- **(Correct)**
- **Safety is only important in high-risk industries**

Explanation

"Safety first" means that safety is the top priority in all work activities. This means that no job or task is more important than the safety of employees and others involved in the work.

Question 195: **Skipped**

What are the main options for risk treatment?

- **Elimination, avoidance, transfer**
- **Elimination, mitigation, transfer**
- **Acceptance, mitigation, transfer**

- **(Correct)**
- **Acceptance, avoidance, transfer**

Explanation

The main options for risk treatment are acceptance, mitigation, avoidance and transfer. Organizations can choose to accept risks and live with the consequences, take steps to reduce the likelihood or impact of risks, or transfer the risks to another party, such as through insurance. "Risks can't be eliminated"

Question 196: **Skipped**

Which of the following is a benefit of using IPv6 over IPv4?

- **IPv6 is easier to configure than IPv4.**
- **IPv6 is faster than IPv4.**
- **IPv6 supports a larger number of devices.**
- **(Correct)**
- **IPv6 is more secure than IPv4.**

Explanation

IPv6 has a much larger address space compared to IPv4, which allows for a larger number of unique addresses and supports the growing number of devices connected to the internet. While IPv6 does offer other benefits, such as

improved security and simplified addressing, the larger address space is one of its most significant advantages.

Question 197: **Skipped**

What is the difference between disaster recovery (DR) and business continuity (BC)?

- **Disaster recovery refers to the process of restoring information systems and services after a disaster, while business continuity refers to the process of reducing the impact of a disaster on an organization.**
- **Disaster recovery refers to the process of restoring information systems and services after a disaster, while business continuity refers to the ability of an organization to continue operating in the event of a disaster.**
- **Disaster recovery refers to the process of reducing the impact of a disaster on an organization, while business continuity refers to the ability of an organization to continue operating in the event of a disaster.**
- **Disaster recovery refers to the ability of an organization to continue operating in the event of a disaster, while business continuity refers to the process of restoring information systems and services after a disaster.**

- **(Correct)**

Explanation

Disaster recovery refers to the ability of an organization to continue operating in the event of a disaster, such as a natural disaster, cyberattack, or other disruption. Business continuity refers to the process of restoring information systems and services after a disaster, with the goal of minimizing the impact of the disaster on the organization. Disaster recovery and business continuity are closely related, but they focus on different aspects of ensuring the availability of information and services in the event of a disaster

Question 198: **Skipped**

What is the main purpose of the ISC2 Code of Ethics Preamble?

- **To ensure the safety and welfare of society and the common good**
- **(Correct)**
- **To advance the cybersecurity profession**
- **To promote ethical standards of behavior**
- **To protect the infrastructure and public trust**

Explanation

The main purpose of the ISC2 Code of Ethics Preamble is to ensure the safety and welfare of society and the common good, and to promote ethical standards of behavior by strict adherence to the Code.

Question 199: **Skipped**

What is the primary function of regulations and laws in governance processes?

- **To enforce policies and procedures**
- **To set standards for performance and behavior**
- **To ensure legal compliance**
- **(Correct)**
- **To provide guidelines for decision making**

Explanation

Regulations and laws are legally binding and enforceable rules that organizations must comply with. They are designed to ensure that organizations operate in a manner that is in line with the laws of the country and to protect the rights of individuals and the public. Failure to comply with regulations and laws can result in penalties and legal action.

Question 200: **Skipped**

Which of the following is a limitation of Network Intrusion Detection Systems (NIDS)?

- **They are only effective for detecting external attacks, not internal attacks.**
- **They can only detect known signatures and patterns of malicious behavior.**
- **They cannot detect attacks that originate from inside the network.**
- **They can only detect attacks on the network layer, not the application layer.**
- **(Correct)**

Explanation

Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic and detect anomalies in network traffic that may indicate an intrusion or unauthorized access attempt. However, NIDS are limited in their ability to detect attacks on the application layer. While NIDS can detect internal attacks, they are also limited in their ability to detect unknown or zero-day attacks that do not have a known signature or pattern of malicious behavior.

(Domain 2) - Business Continuity, Disaster Recovery & Incident Response - Results

Return to review

Chart

Pie chart with 4 slices.

End of interactive chart.

Attempt 1

All knowledge areas
All questions

Question 1: **Skipped**

What is the role of disaster recovery in an IT business continuity plan?

- **To provide a plan for restoring normal business operations in the event of a disaster**
- **To provide a means of recovering data in the event of a disaster**
- **(Correct)**
- **To minimize the impact of a disaster on a business**
- **To ensure the survival of a business in the event of a disaster**

Explanation

Disaster recovery is an important component of an IT business continuity plan and is focused on the recovery of data and systems in the event of a disaster. The goal of disaster recovery is to ensure that data and systems are restored to a functional state as quickly as possible to minimize the impact of a disaster on a business.

Question 2: **Skipped**

What is the difference between disaster recovery (DR) and business continuity (BC)?

- **Disaster recovery refers to the process of restoring information systems and services after a disaster, while business continuity refers to the ability of an organization to continue operating in the event of a disaster.**
- **Disaster recovery refers to the process of reducing the impact of a disaster on an organization, while business continuity refers to the ability of an organization to continue operating in the event of a disaster.**
- **Disaster recovery refers to the process of restoring information systems and services after a disaster, while business continuity refers to the process of reducing the impact of a disaster on an organization.**

- **Disaster recovery refers to the ability of an organization to continue operating in the event of a disaster, while business continuity refers to the process of restoring information systems and services after a disaster.**
- **(Correct)**

Explanation

Disaster recovery refers to the ability of an organization to continue operating in the event of a disaster, such as a natural disaster, cyberattack, or other disruption. Business continuity refers to the process of restoring information systems and services after a disaster, with the goal of minimizing the impact of the disaster on the organization. Disaster recovery and business continuity are closely related, but they focus on different aspects of ensuring the availability of information and services in the event of a disaster

Question 3: **Skipped**

Who is typically responsible for developing and implementing an IT business continuity plan?

- **A dedicated business continuity team**
- **The IT department**

- **(Correct)**
- **All departments within the organization**
- **The Chief Executive Officer (CEO)**

Explanation

The IT department is typically responsible for developing and implementing an IT business continuity plan. However, the plan should involve input and participation from all departments within the organization to ensure that it is comprehensive and meets the needs of the business.

Question 4: **Skipped**

What is a communication plan in the context of incident response?

- **A plan for communicating with government agencies during an incident.**
- **A plan for communicating with employees during an incident.**
- **A plan for communicating with customers and stakeholders during an incident.**
- **All of the above**
- **(Correct)**

Explanation

A communication plan in the context of incident response is a documented process that outlines the steps that an

organization will take to communicate with key stakeholders, such as customers, employees, and government agencies, during an incident. This plan should be well-rehearsed and practiced, in order to ensure a rapid and effective response in the event of an incident.

Question 5: **Skipped**

What is the importance of testing an IT business continuity plan?

- **To identify and resolve potential problems before a disaster occurs**
- **To determine the effectiveness of the plan in the event of a disaster**
- **To ensure that the plan is up-to-date and relevant to current business operations**
- **All of the above**
- **(Correct)**

Explanation

Testing an IT business continuity plan is important for several reasons. It helps to identify and resolve potential problems before a disaster occurs, determine the effectiveness of the plan in the event of a disaster, and ensure that the plan is up-to-date and relevant to current

business operations. Regular testing of the plan is essential to ensure its readiness and effectiveness in the event of a disaster.

Question 6: **Skipped**

What should be the outcome of the post-incident review?

- **A report documenting the incident.**
- **None of the above.**
- **A decision to terminate the incident response team.**
- **Recommendations for improvements to the incident response process.**
- **(Correct)**

Explanation

The outcome of the post-incident review should be recommendations for improvements to the incident response process. These recommendations should be used to make changes to the incident response process, and to improve the overall resilience and preparedness of the organization in the event of future incidents.

Question 7: **Skipped**

What is the role of a risk assessment in an IT disaster recovery plan?

- **All of the above**

- **(Correct)**
- **To develop a strategy for mitigating the risks and threats identified in the assessment**
- **To prioritize the critical business processes that must be protected**
- **To identify the potential risks and threats to the organization's operations**

Explanation

A risk assessment is a critical component of an IT disaster recovery plan. It is used to identify the potential risks and threats to the organization's operations, prioritize the critical business processes that must be protected, and develop a strategy for mitigating the risks and threats identified in the assessment. The risk assessment should be conducted regularly to ensure that it remains relevant and up-to-date.

Question 8: **Skipped**

Who is responsible for determining the scope of the disaster recovery plan and identifying the critical systems and processes that must be protected?

- **The Information Technology department**
- **The Disaster Recovery Team**
- **The Chief Executive Officer**

- **The Business Continuity Manager**
- **(Correct)**

Explanation

The business continuity manager is responsible for overseeing the development and implementation of the disaster recovery plan, and as such, they should be the one to determine the scope of the plan and identify the critical systems and processes that must be protected. This information will help inform the development of the disaster recovery plan and ensure that the plan is comprehensive and effective in the event of a disaster.

Question 9: **Skipped**

What should be considered during the post-incident review?

- **The accuracy of the incident response plan.**
- **All of the above.**
- **(Correct)**
- **The cost of the incident response.**
- **The response time to the incident.**

Explanation

During the post-incident review, a variety of factors should be considered, including the response time to the incident,

the cost of the incident response, and the accuracy of the incident response plan. This helps to evaluate the effectiveness of the response and identify areas for improvement in the incident response process.

Question 10: **Skipped**

What is the purpose of the analysis step in incident response?

- **To stop the incident from spreading.**
- **To notify relevant parties of the incident.**
- **To determine the cause of the incident.**
- **(Correct)**
- **To implement a solution to the incident.**

Explanation

The purpose of the analysis step in incident response is to determine the root cause of the incident. This involves collecting and analyzing data from various sources, such as system logs, network traffic, and other relevant information, to understand what caused the incident to occur.

Question 11: **Skipped**

What are the key components of a Business Continuity plan?

- **Risk assessment, Business Impact Analysis, and Disaster Recovery Plan**
- **Disaster Recovery Plan, Business Impact Analysis, and Incident Response Plan**
- **Incident Response Plan, Business Impact Analysis, and Risk assessment**
- **Business Impact Analysis, Risk assessment, and Disaster Recovery Plan**
- **(Correct)**

Explanation

The key components of a Business Continuity plan include a Business Impact Analysis (BIA), which assesses the potential impact of different types of events on the organization; a Risk assessment, which identifies potential threats to the organization; and a Disaster Recovery Plan (DRP), which outlines the steps that will be taken to recover critical business functions after an event. These three components work together to ensure the organization is prepared to respond effectively to unexpected events and maintain operations.

Question 12: **Skipped**

What is the purpose of testing a BCP?

- **To identify weaknesses and improve the plan**

- **(Correct)**
- **To assess the financial impact of a disaster on the organization**
- **To ensure that the plan is foolproof and cannot fail**
- **To verify that the plan conforms to legal and regulatory requirements**

Explanation

The purpose of testing a BCP is to identify weaknesses, its effectiveness and improve the plan. This helps to ensure that the plan is effective and can be implemented successfully in the event of a disaster.

Question 13: **Skipped**

What is an incident response plan?

- **A plan for responding to workplace accidents.**
- **A plan for responding to security incidents.**
- **(Correct)**
- **A plan for responding to medical emergencies.**
- **A plan for responding to natural disasters.**

Explanation

An incident response plan is a documented process that outlines the steps an organization will take in the event of a security incident, such as a cyber-attack, a data breach, or a system failure. This plan should be well-rehearsed and

practiced, in order to ensure a rapid and effective response in the event of an incident.

Question 14: **Skipped**

What is a cyber disaster?

- **A disaster caused by a widespread outbreak of a disease.**
- **A disaster caused by a nuclear explosion.**
- **A disaster caused by a natural event such as a hurricane.**
- **A disaster caused by a failure of computer systems and networks.**
- **(Correct)**

Explanation

A cyber disaster is an event caused by a failure of computer systems and networks, such as a cyber-attack, a data breach, or a hardware failure. This type of disaster can have serious impacts on organizations, including loss of data and intellectual property, loss of revenue, and damage to reputation. It is important for organizations to have a disaster recovery plan in place that addresses cyber disasters, in order to minimize the impact of such events on the organization and its stakeholders.

Question 15: **Skipped**

What is a supply chain disruption disaster?

- **A disaster caused by a natural event such as a hurricane.**
- **A disaster caused by a nuclear explosion.**
- **A disaster caused by a disruption in the flow of goods and materials.**
- **(Correct)**
- **A disaster caused by a widespread outbreak of a disease.**

Explanation

A supply chain disruption disaster is an event caused by a disruption in the flow of goods and materials, such as a transportation strike, a natural disaster, or a political crisis. This type of disaster can have serious impacts on organizations, including loss of revenue, difficulty obtaining critical supplies, and damage to reputation. It is important for organizations to have a disaster recovery plan in place that addresses supply chain disruption disasters, in order to minimize the impact of such events on the organization and its stakeholders.

Question 16: **Skipped**

What is the first step in developing a disaster recovery plan?

- **Conduct a risk assessment to identify potential disaster scenarios.**
- **Identify critical systems and processes that must be protected.**
- **(Correct)**
- **Develop procedures for responding to and recovering from a disaster.**
- **Establish a disaster recovery team.**

Explanation

Identifying critical systems and processes that must be protected is an important step in the disaster recovery process, as it helps to inform the development of the disaster recovery plan and ensure that it is comprehensive and effective in the event of a disaster.

Question 17: **Skipped**

What is the purpose of a cold site?

- **To provide a minimal level of infrastructure that can be used in the event of a disaster**
- **To provide a means of recovering data in the event of a disaster**

- **To provide an unused facility that can be quickly converted to a functional backup site in the event of a disaster**
- **(Correct)**
- **To provide a plan for restoring normal business operations in the event of a disaster**

Explanation

A cold site is an unused facility with no equipment or infrastructure, which would require significant time and resources to be made operational in the event of a disaster. The primary purpose of a cold site is to provide a location that can be quickly converted to a functional backup site in the event of a disaster.

Question 18: **Skipped**

Your organization has just suffered a major disaster, and you have been assigned the role of disaster recovery manager. What is the first step you should take in this role?

- **Identify the critical business processes that must be protected and prioritize their recovery.**
- **Establish a crisis management center and begin communications with key stakeholders.**
- **(Correct)**

- **Begin the process of restoring normal business operations as quickly as possible.**
- **Conduct a damage assessment of the organization's facilities and infrastructure.**

Explanation

The first step in the role of disaster recovery manager is to establish a crisis management center, which will serve as the central hub for coordinating and communicating the disaster recovery efforts. This center should be equipped with the necessary resources and technology to facilitate effective communication with key stakeholders, including employees, customers, partners, and suppliers. In a real-world scenario, the disaster recovery manager might take a combination of steps A, B, C, and D, or they might prioritize one step over another, depending on the specific needs of the organization and the impact of the disaster.

Question 19: **Skipped**

Which of the following is one of the roles of the management team in an IT business continuity plan?

- **To develop and implement the plan**
- **To provide overall direction and support for the plan**
- **(Correct)**

- **To ensure that the plan is tested regularly**
- **To provide technical expertise for the plan**

Explanation

he management team has several key roles in an IT business continuity plan, one of which is to provide overall direction and support for the plan. The management team should ensure that the plan is integrated into the overall operations of the organization and that it is adequately supported and funded. The management team should also be actively involved in ensuring that the plan is tested regularly and that any necessary updates are made in a timely manner.

Question 20: **Skipped**

What is the role of a business impact analysis in an IT disaster recovery plan?

- **To identify the critical business processes that must be protected**
- **To develop a strategy for restoring normal business operations as quickly as possible**
- **All of the above**
- **(Correct)**
- **To determine the impact of a disaster on the organization's operations**

Explanation

A business impact analysis is a critical component of an IT disaster recovery plan. It is used to determine the impact of a disaster on the organization's operations, identify the critical business processes that must be protected, and develop a strategy for restoring normal business operations as quickly as possible. The business impact analysis should take into account the specific needs and requirements of the organization, as well as the potential consequences of a disaster.

Question 21: **Skipped**

What is a pandemic disaster?

- **A disaster caused by a widespread outbreak of a disease.**
- **(Correct)**
- **A disaster caused by a cyber-attack.**
- **A disaster caused by a nuclear explosion.**
- **A disaster caused by an earthquake.**

Explanation

A pandemic disaster is an event caused by a widespread outbreak of a disease, such as the flu or COVID-19. This type of disaster can have far-reaching impacts, including

widespread illness and death, economic disruption, and social and political upheaval. It is important for organizations to have a disaster recovery plan in place that addresses pandemic disasters, in order to minimize the impact of such events on the organization and its stakeholders.

Question 22: **Skipped**

One of the below is not a purpose of having a communication plan in a disaster recovery plan?

- **To provide a framework for communicating with external parties.**
- **To record phone messages during a disaster.**
- **(Correct)**
- **To document all communications during a disaster.**
- **To ensure effective communication between stakeholders.**

Explanation

The purpose of having a communication plan in a disaster recovery plan is to ensure effective communication between stakeholders, document all communications during a disaster, and provide a framework for communicating with external parties. Option D, to record

phone messages during a disaster, is incorrect as recording phone messages is not the primary purpose of a communication plan in a disaster recovery plan. The communication plan is designed to ensure that all stakeholders have access to accurate and up-to-date information during a disaster, and to minimize confusion and misunderstandings.

Question 23: **Skipped**

What is the primary purpose of an IT business continuity plan?

- **To provide a plan for restoring normal business operations in the event of a disaster**
- **(Correct)**
- **To provide a means of recovering data in the event of a disaster**
- **To minimize the impact of a disaster on a business**
- **To ensure the survival of a business in the event of a disaster**

Explanation

The primary purpose of an IT business continuity plan is to ensure that a business is able to resume its normal

operations as quickly as possible in the event of a disaster, such as a cyber attack, natural disaster, or power failure.

Question 24: **Skipped**

What is a containment plan in the context of incident response?

- **A plan for containing the spread of a virus.**
- **A plan for containing the spread of a fire.**
- **A plan for containing the spread of an incident.**
- **(Correct)**
- **A plan for containing the spread of an environmental hazard.**

Explanation

A containment plan in the context of incident response is a documented process that outlines the steps that an organization will take to contain the spread of an incident, such as a cyber-attack or a data breach. This plan should be well-rehearsed and practiced, in order to ensure that the incident does not escalate and cause further harm to the organization and its stakeholders.

Question 25: **Skipped**

What is the primary difference between a hot site and a warm site?

- **A hot site is located close to the main facility while a warm site is located farther away.**
- **A hot site is more expensive than a warm site.**
- **A hot site is used for short-term recovery while a warm site is used for long-term recovery.**
- **A hot site is fully functional while a warm site is partially functional.**
- **(Correct)**

Explanation

A hot site is a fully operational backup facility that is ready to take over the operations of a business in the event of a disaster. A warm site has some limited functionality, such as basic infrastructure, but may require some additional time to be fully operational.

Question 26: **Skipped**

What is the purpose of conducting a Business Impact Analysis (BIA)?

- **To assess the impact of a potential security breach**
- **To determine the likelihood of a disaster occurring**
- **To evaluate the costs and benefits of different security measures**
- **To identify the critical functions and processes of an organization**

- **(Correct)**

Explanation

The purpose of conducting a Business Impact Analysis (BIA) is to identify the critical functions and processes of an organization and to assess the impact of a potential disruption to these processes. This information is used to prioritize the development of recovery plans and ensure the continued operations of the organization in the event of a disaster.

Question 27: **Skipped**

What is the primary goal of Business Continuity (BC)?

- **To maintain operations during unexpected events**
- **(Correct)**
- **To maintain the status quo during unexpected events**
- **To maximize profits during unexpected events**
- **To minimize expenses during unexpected events**

Explanation

The primary goal of Business Continuity is to ensure that the essential functions of an organization are maintained during and after an unexpected event such as a disaster, cyber attack or other crisis. This helps to minimize the

impact of the event on the organization, its stakeholders, and its customers.

Question 28: **Skipped**

What is the purpose of the containment step in incident response?

- **To identify the root cause of the incident.**
- **To stop the incident from spreading.**
- **(Correct)**
- **To implement a solution to the incident.**
- **To analyze the incident.**

Explanation

The purpose of the containment step in incident response is to stop the incident from spreading and to limit the damage that it can cause. This may involve isolating affected systems, disconnecting from networks, or other measures to prevent the incident from causing further harm.

Question 29: **Skipped**

What is the first step in incident response?

- **Containment**
- **Identification**
- **(Correct)**

- **Analysis**
- **Remediation**

Explanation

The first step in incident response is to identify the incident. This involves recognizing that an incident has occurred and collecting information about the nature and scope of the incident. This information can then be used to make decisions about how to respond to the incident.

Question 30: **Skipped**

What is the difference between a hot site, warm site, and cold site?

- **A hot site is a fully functional backup facility, a warm site is an unused facility with no equipment, and a cold site has limited functionality.**
- **A hot site is an unused facility with no equipment, a warm site has limited functionality, and a cold site is a fully functional backup facility.**
- **A hot site has limited functionality, a warm site is a fully functional backup facility, and a cold site is an unused facility with no equipment.**
- **A hot site is a fully functional backup facility, a warm site has limited functionality, and a cold site is an unused facility with no equipment.**

- **(Correct)**

Explanation

A hot site is a fully functional backup facility, a warm site has limited functionality, and a cold site is an unused facility with no equipment. A hot site is a fully operational backup facility that is ready to take over the operations of a business in the event of a disaster. A warm site has some limited functionality, such as basic infrastructure, but may require some additional time to be fully operational. A cold site is an unused facility with no equipment or infrastructure, which would require significant time and resources to be made operational in the event of a disaster.

Question 31: **Skipped**

What is the role of the CEO in an IT business continuity plan?

- **To ensure that the plan is implemented and tested regularly**
- **To provide overall direction and support for the plan**
- **To oversee the development of the plan**
- **All of the above**
- **(Correct)**

Explanation

The Chief Executive Officer (CEO) has a critical role in an IT business continuity plan. The CEO is responsible for providing overall direction and support for the plan, ensuring that it is implemented and tested regularly, and overseeing its development. The CEO should ensure that the plan is aligned with the overall goals and objectives of the organization and that it is adequately supported and funded.

Question 32: **Skipped**

What is the final step in incident response?

- **Analysis**
- **Post-incident review**
- **(Correct)**
- **Containment**
- **Identification**

Explanation

The final step in incident response is the post-incident review. This involves reviewing the response to the incident, evaluating its effectiveness, and making recommendations for improvements that can be made to the incident response process. This step is critical for

improving the overall resilience and preparedness of the organization in the event of future incidents.

Question 33: **Skipped**

Which of the following is one of the roles of the IT department in an IT business continuity plan?

- **To develop and implement the plan**
- **(Correct)**
- **To ensure that the plan is tested regularly**
- **To provide technical expertise for the plan**
- **To provide overall direction and support for the plan**

Explanation

The IT department has several key roles in an IT business continuity plan, one of which is to develop and implement the plan. The IT department should ensure that the plan is comprehensive, technically sound, and aligned with the overall goals and objectives of the organization. The IT department should also be responsible for ensuring that the plan is tested regularly and that any necessary updates are made in a timely manner.

Question 34: **Incorrect**

What is the purpose of the remediation step in incident response?

- **To notify relevant parties of the incident.**
- **To stop the incident from spreading.**
- **To determine the cause of the incident.**
- **(Incorrect)**
- **To implement a solution to the incident.**
- **(Correct)**

Explanation

The purpose of the remediation step in incident response is to implement a solution to the incident. This may involve patching systems, restoring data, or other measures to address the underlying cause of the incident and prevent it from happening again in the future.

Question 35: **Skipped**

What is the difference between a natural disaster and a man-made disaster?

- **Natural disasters are less severe than man-made disasters.**
- **Natural disasters are caused by events outside of human control, while man-made disasters are caused by human actions.**
- **(Correct)**
- **Natural disasters only occur in rural areas, while man-made disasters only occur in urban areas.**

- **Natural disasters are caused by human activities, while man-made disasters are not.**

Explanation

A natural disaster is an event caused by natural causes such as hurricanes, earthquakes, or floods. A man-made disaster, on the other hand, is an event caused by human actions, such as cyber-attacks, oil spills, or industrial accidents. The severity of a disaster can depend on a variety of factors, and it is not always the case that one type of disaster is more severe than another.

(Domain 3) - Access Controls - Results

Question 1: **Skipped**

What is the main difference between fail-safe and fail-secure mechanisms?

- **Fail-safe systems lock down in case of a failure, while fail-secure systems operate in a safe state in case of a failure.**
- **Fail-safe and fail-secure systems are the same thing.**

- **Fail-safe systems operate in a safe state in case of a failure, while fail-secure systems lock down in case of a failure.**
- **(Correct)**
- **Neither fail-safe nor fail-secure systems are used in security applications.**

Explanation

Fail-safe systems are designed to operate in a safe state in case of a failure, while fail-secure systems are designed to lock down in case of a failure. This means that fail-safe systems will continue to operate even if there is a failure, while fail-secure systems will shut down to prevent unauthorized access.

Question 2: **Skipped**

What should be considered when developing a physical security control plan?

- **All of the above.**
- **(Correct)**
- **The potential threat sources.**
- **The location of the assets.**
- **The type of assets being protected.**

Explanation

When developing a physical security control plan, it is important to consider the type of assets being protected, the location of the assets, and the potential threat

sources. This helps to ensure that the physical security controls are appropriate for the specific assets and threat environment, and that they effectively protect against unauthorized access and other security incidents.

Question 3: **Skipped**

What is the purpose of using a mantrap in an access control system?

- **To provide a means of escape in case of emergency**
- **To increase the speed of entry into a building**
- **To reduce the number of doors in a building**
- **To provide additional security to a high secure area**
- **(Correct)**

Explanation

A mantrap is used in an access control system to provide additional security to a high secure area by controlling access through two secure doors and verifying the identity of individuals before they are granted access to the secure area.

Question 4: **Skipped**

Which of the following best describes the main benefit of implementing a MAC system?

- **It allows for flexible and dynamic access permissions.**
- **It provides a high level of security and control over access to resources.**

- **(Correct)**
- **It is resistant to attacks and exploits.**
- **It is easy to implement and manage.**

Explanation

The main benefit of implementing a MAC system is that it provides a high level of security and control over access to resources. Since access control is determined by a central authority based on policies, access is granted only to authorized users, and is limited to the minimum necessary level.

Question 5: **Skipped**

In which scenario would a fail-safe mechanism be more appropriate?

- **When neither security nor availability are important.**
- **When availability is the top priority.**
- **When both security and availability are important.**
- **When security is the top priority.**
- **(Correct)**

Explanation

Fail-safe mechanisms are more appropriate when security is the top priority, as they allow systems to continue operating even if there is a failure. This is important in situations where shutting down the system could cause more harm than allowing it to continue operating in a safe state.

Question 6: **Skipped**

Which of the following is a key principle of Mandatory Access Control (MAC)?

- **Access to resources is determined by the system based on security labels.**
- **(Correct)**
- **Users are given access to resources at the discretion of the system owner.**
- **Access to resources is based on the user's job function.**
- **Access to resources is determined by the user.**

Explanation

Mandatory Access Control (MAC) is an access control mechanism that uses security labels to determine who can access resources. Access to resources is determined by the system based on security labels, which are assigned to users and resources based on their security clearance.

Question 7: **Skipped**

What is the primary function of bollards in physical security?

- **To protect against unauthorized entry or vehicle access**
- **(Correct)**
- **To provide shade**

- **To secure buildings and outdoor areas**
- **To direct traffic flow**

Explanation

The primary function of bollards in physical security is to serve as a barrier for buildings and outdoor areas to protect against unauthorized entry or vehicle access.

Question 8: **Skipped**

Company ABC has a new project that requires access to sensitive information. Which security control should be implemented to ensure that access to this information is restricted to only those who need it?

- **None of the above.**
- **Principle of Least Privilege**
- **(Correct)**
- **Segregation of Duties**
- **Segregation of Duties and the Principle of Least Privilege**

Explanation

The Principle of Least Privilege should be implemented to ensure that access to the sensitive information is restricted to only those who need it. This control grants employees access to the minimum resources necessary to perform their job functions, which limits the potential damage from a security breach or human error.

Question 9: **Skipped**

What is the purpose of Crime Prevention Through Environmental Design (CPTED)?

- **To have no impact on crime through physical design and management of the built environment**
- **To decrease crime through physical design and management of the built environment**
- **(Correct)**
- **To increase crime through physical design and management of the built environment**
- **To increase crime through law enforcement practices**

Explanation

Crime Prevention Through Environmental Design (CPTED) is an evidence-based crime prevention strategy that aims to reduce crime through design and management of the built environment. It uses physical design and management practices to increase natural surveillance, reduce opportunities for crime, and create a sense of community ownership and pride in the built environment.

Question 10: **Skipped**

In an organization that uses RBAC, a user with administrative privileges is leaving the organization. What is the recommended action to ensure that access permissions are appropriately adjusted?

- **The user should be required to transfer administrative privileges to another user.**

- **The user's role should be modified to remove administrative privileges.**
- **(Correct)**
- **All roles with administrative privileges should be deleted.**
- **The user's access permissions should be revoked.**

Explanation

Role-based access control (RBAC) is an access control mechanism that is based on the user's role or job function within an organization. Access permissions are assigned to roles, and users are granted access based on their role. RBAC provides a number of benefits, including increased security and easier management of access permissions. In an organization that uses RBAC, access permissions can be adjusted based on changes to a user's role or responsibilities. Temporary access can be granted by assigning a new role to a user, and access permissions can be revoked by modifying the user's role. When a user with administrative privileges is leaving the organization, their role should be modified to remove administrative privileges to ensure that access permissions are appropriately adjusted.

Question 11: **Skipped**

What is the Segregation of Duties?

- **A security control that ensures employees have access to all resources they need to perform their job functions.**
- **A security control that requires employees to work in separate physical locations.**
- **A security control that divides responsibilities among multiple employees to reduce the risk of fraud or errors.**
- **(Correct)**
- **A security control that allows employees to perform multiple roles within an organization.**

Explanation

The Segregation of Duties is a security control that divides responsibilities among multiple employees to reduce the risk of fraud or errors. This means that no single employee has complete control over a particular process or resource, which helps prevent errors or malicious activities.

Question 12: **Skipped**

Which of the following is an example of a logical access control mechanism?

- **A security camera**
- **A biometric authentication system**
- **A security guard**
- **Role-based access control**

- **(Correct)**

Explanation

Role-based access control (RBAC) is an example of a logical access control mechanism, which is a type of access control that uses software-based tools to regulate access to resources.

Question 13: **Skipped**

What is the purpose of installing bollards in a physical security plan?

- **To direct traffic flow**
- **To secure an area**
- **To provide a visual barrier**
- **All of the above**
- **(Correct)**

Explanation

Bollards can serve all of the above purposes, making them a versatile and effective tool in a physical security plan. By providing a visual barrier, directing traffic flow, and securing an area, bollards can help to deter unauthorized access and prevent unwanted intrusion.

Question 14: **Skipped**

Which of the following is a limitation of MAC?

- **It can be easily circumvented by malicious users.**
- **It can result in users having too much access to resources.**

- **It can be difficult to implement and manage.**
- **It can be too rigid and inflexible.**
- **(Correct)**

Explanation

Mandatory Access Control (MAC) is a security mechanism that provides a centralized authority with control over access to resources based on predefined policies. In a MAC system, the central authority sets and enforces access controls, and users cannot change their own access permissions. The main benefit of implementing a MAC system is that it provides a high level of security and control over access to resources. However, one of the limitations of MAC is that it can be too rigid and inflexible, making it difficult to make changes to access permissions or to accommodate new access requirements. It is important to implement other security mechanisms, such as Role-Based Access Control and the Principle of Least Privilege, in conjunction with MAC to ensure that access is granted at the appropriate level.

Question 15: **Skipped**

What is the difference between a magnetic stripe badge and a smart card badge system?

- **Magnetic stripe badges can only be used for physical access control, while smart card badges can be used for both physical and logical access control.**

- **(Correct)**
- **Magnetic stripe badges are less secure than smart card badges.**
- **Smart card badges can only be used for physical access control, while magnetic stripe badges can be used for both physical and logical access control.**
- **Magnetic stripe badges are more secure than smart card badges.**

Explanation

Magnetic stripe badges store a static magnetic stripe that can be read when swiped through a reader. This makes them suitable for physical access control but they lack the security features required for logical access control. Smart card badges, on the other hand, have a microprocessor chip that can store and process information. This makes them suitable for both physical and logical access control, making them a more secure option.

Question 16: **Skipped**

What is the most common physical security control used to secure high-security areas?

- **Video surveillance**
- **Perimeter fencing**
- **All of the above**
- **Access control systems**
- **(Correct)**

Explanation

Access control systems are the most common physical security control used to secure high-security areas. They typically use a combination of technologies such as biometrics, smart cards, and keypads to control who can enter and exit the area. Video surveillance and perimeter fencing are also important components of high-security areas, but access control systems play a key role in controlling access.

Question 17: **Skipped**

In an organization that uses both DAC and MAC, which security mechanism takes precedence?

- **DAC takes precedence over MAC.**
- **Both mechanisms are equal in priority and function independently.**
- **MAC takes precedence over DAC.**
- **(Correct)**
- **The order of precedence is determined by the resource owner.**

Explanation

Discretionary Access Control (DAC) and Mandatory Access Control (MAC) are two different access control mechanisms that can be used in an organization. In a DAC system, the owner of the resource has the authority to grant or deny access to other users. In a MAC system,

access control is determined by a central authority based on predefined policies. When both mechanisms are used in an organization, MAC takes precedence over DAC. This is because MAC is a more stringent access control mechanism, and its policies must be followed even if the owner of the resource has granted access to the user. In contrast, DAC is a more permissive mechanism, and its policies can be overridden by the central authority in a MAC system.

Question 18: **Skipped**

Which type of control is focused on securing the physical environment and ensuring that access to systems and data is restricted to authorized individuals?

- **All of the above**
- **Administrative controls**
- **Physical controls**
- **(Correct)**
- **Technical controls**

Explanation

Physical controls are focused on securing the physical environment and ensuring that access to systems and data is restricted to authorized individuals. Examples of physical controls include security cameras, locked doors, and security personnel.

Question 19: **Skipped**

What are the 4 principles of CPTED (Crime Prevention Through Environmental Design)?

- **Access control, Territoriality, Lighting, and Maintenance**
- **Surveillance, Access control, Territoriality, and Maintenance**
- **(Correct)**
- **Surveillance, Access control, Lighting, and Maintenance**
- **Surveillance, Territoriality, Lighting, and Maintenance**

Explanation

CPTED (Crime Prevention Through Environmental Design) is based on 4 principles, which include Surveillance, Access control, Territoriality, and Maintenance. These principles aim to increase natural surveillance and reduce opportunities for crime, establish ownership and control over the built environment, and ensure proper maintenance and upkeep of the environment to maintain its effectiveness in reducing crime.

Question 20: **Skipped**

Company QRS is implementing a new IT system and is concerned about potential security breaches. Which security control should be implemented to ensure that access to the system is restricted to only those who need it?

- **None of the above.**
- **Segregation of Duties and the Principle of Least Privilege**
- **(Correct)**
- **Principle of Least Privilege**
- **Segregation of Duties**

Explanation

Both the Segregation of Duties and the Principle of Least Privilege are important security controls that help ensure that access to resources is restricted to only those who need it. The Segregation of Duties divides responsibilities among multiple employees, while the Principle of Least Privilege grants employees access to the minimum resources necessary to perform their job functions. Both of these controls can help reduce the risk of fraud, errors, and security breaches, and limit the potential damage from a breach or human error. The specific control that should be implemented depends on the nature of the resource or process being protected, as well as the potential risks and threats.

Question 21: **Skipped**

An organization wants to monitor the temperature and humidity levels in a data center to prevent equipment damage. What type of log can be used for this purpose?

- **Inventory logs**

- **Surveillance logs**
- **Access logs**
- **Environmental logs**
- **(Correct)**

Explanation

Environmental logs record information about the temperature, humidity, and other environmental factors in the data center, which can help to monitor the conditions and prevent equipment damage.

Question 22: **Skipped**

How does the use of surveillance cameras improve physical security?

- **By deterring potential attackers**
- **By recording events for future use**
- **By providing real-time monitoring**
- **All of the above**
- **(Correct)**

Explanation

Surveillance cameras provide real-time monitoring, deter potential attackers and also record events for future use, thereby improving the physical security of the premises.

Question 23: **Skipped**

In an organization that uses Discretionary Access Control (DAC), a user wants to grant access to a file to a colleague. What is the user's next step?

- **The user must obtain approval from the resource owner before granting access to the colleague.**
- **The user can grant the access to the colleague without any additional approval.**
- **(Correct)**
- **The user must obtain approval from the system administrator before granting access to the colleague.**
- **The user must modify the file permissions and add the colleague to the access control list.**

Explanation

In a Discretionary Access Control (DAC) system, the owner of the resource has the authority to grant or deny access to other users. Therefore, the user can grant the access to the colleague without any additional approval.

Question 24: **Skipped**

Which of the following is an example of Discretionary Access Control (DAC)?

- **A user is only given access to resources based on their job function.**
- **A user's access to resources is determined by an administrator.**
- **A company's CEO has access to all resources in the organization.**

- **A user can modify the permissions of files and folders that they own.**
- **(Correct)**

Explanation

Discretionary Access Control (DAC) is an access control mechanism that allows users to determine who can access resources that they own. In this example, the user can modify the permissions of files and folders that they own.

Question 25: **Skipped**

Which of the following is a limitation of DAC?

- **It is difficult to implement and manage.**
- **It can result in users having too much access to resources.**
- **(Correct)**
- **It is too rigid and inflexible.**
- **It can be easily circumvented by malicious users.**

Explanation

One of the limitations of DAC is that it can result in users having too much access to resources. Since the owner of the resource has complete control over access permissions, they can grant access to users who may not need it, leading to a potential security risk.

Question 26: **Skipped**

Which of the following is a key principle of the Principle of Least Privilege?

- **Users should only be given access to resources that are necessary to perform their job functions.**
- **(Correct)**
- **Users should be given unrestricted access to all resources.**
- **All users should be given the same level of access to resources.**
- **All users should be granted administrative privileges by default.**

Explanation

The Principle of Least Privilege is a key security principle that requires that users should only be given access to resources that are necessary to perform their job functions. This limits the potential damage that could be caused if a user's account is compromised.

Question 27: **Skipped**

What type of gate is best for secure entry and exit to a property?

- **Automatic gate**
- **(Correct)**
- **Ornamental iron gate**
- **Roll-up gate**
- **Barrier gate**

Explanation

Automatic gates provide secure entry and exit to a property by controlling who has access and when. They can be integrated with security systems, such as card readers or biometric scanners, to further enhance security.

Question 28: **Skipped**

In a DAC system, who has control over the access permissions of a resource?

- **The system administrator**
- **Owner and system admin**
- **None of the above.**
- **The owner of the resource**
- **(Correct)**

Explanation

In a DAC system, the owner of the resource has control over the access permissions of that resource. The owner determines who is granted access and what level of access they are granted.

Question 29: **Skipped**

In an organization that uses RBAC, which of the following is the best approach for granting temporary access to a user outside of their normal role?

- **Deny the user access to the required resources.**
- **Assign the user a new role that grants access to the required resources.**

- (Correct)
- **Grant the user temporary administrative privileges.**
- **Modify the user's existing role to grant access to the required resources.**

Explanation

In Role-based access control (RBAC), access control is based on the user's role or job function within the organization. To grant temporary access to a user outside of their normal role, a new role can be assigned to the user that grants access to the required resources. This ensures that the user only has access to the resources necessary for their temporary task.

Question 30: **Skipped**

What is the purpose of surveillance cameras in physical security control?

- **To capture images of suspicious behavior**
- (Correct)
- **To enforce security policies**
- **To monitor the entry and exit of personnel**
- **To deter theft and vandalism**

Explanation

The primary purpose of surveillance cameras in physical security control is to capture images of any suspicious behavior, so that the authorities can use it for investigation or evidence.

Question 31: **Skipped**

What is the benefit of implementing the Principle of Least Privilege?

- **It increases the risk of data breaches.**
- **It reduces the potential damage from a security breach or human error.**
- **(Correct)**
- **It makes it easier for employees to do their jobs.**
- **It increases the amount of access employees have to sensitive information.**

Explanation

The Principle of Least Privilege is an important security control that helps limit the potential damage from security breaches or human errors. It works by restricting access to resources only to those who need it for their job functions. This helps reduce the risk of unauthorized access or data breaches, as well as limits the damage that can be caused by human errors. Implementing this principle can help ensure that employees have access to only the resources necessary to perform their jobs, which can make it easier to manage access control and reduce the risk of security incidents.

Question 32: **Skipped**

Which of the following best describes the main benefit of implementing a DAC system?

- **It provides a high level of security and control over access to resources.**
- **(Correct)**
- **It is easy to implement and manage.**
- **It allows for flexible and dynamic access permissions.**
- **It is resistant to attacks and exploits.**

Explanation

Discretionary Access Control (DAC) is a security mechanism that provides owners of resources with control over who can access those resources and what level of access they are granted. In a DAC system, owners determine the access permissions of their resources based on their own discretion. The main benefit of implementing DAC is that it provides a high level of security and control over access to resources. However, one of the limitations of DAC is that it can result in users having too much access to resources if owners grant access to users who may not need it. It is important to implement other security mechanisms, such as the Principle of Least Privilege and Role-Based Access Control, to ensure that access is granted at the appropriate level.

Question 33: **Skipped**

Which of the following is an example of implementing the Segregation of Duties?

- **Dividing the responsibilities for approving and processing financial transactions among multiple employees.**
- **(Correct)**
- **llowing the same employee to approve and process financial transactions.**
- **Having one employee responsible for both network security and system administration.**
- **Allowing a single employee to manage and maintain all company databases.**

Explanation

Dividing the responsibilities for approving and processing financial transactions among multiple employees is an example of implementing the Segregation of Duties. This helps ensure that no single employee has complete control over the financial transaction process, which reduces the risk of fraud or errors.

Question 34: **Skipped**

What is the Principle of Least Privilege?

- **A security control that ensures all employees have the same level of access to resources.**
- **A security control that grants employees access to resources based on their job title.**

- **A security control that ensures employees have access to the minimum resources necessary to perform their job functions.**
- **(Correct)**
- **A security control that grants employees access to all resources they request.**

Explanation

The Principle of Least Privilege is a security control that ensures employees have access to the minimum resources necessary to perform their job functions. This helps limit potential damage from a security breach or human error.

Question 35: **Skipped**

What are some common attributes used in Attribute-Based Access Control (ABAC) policies?

- **User age, gender, and location.**
- **User interests, education level, and marital status.**
- **User ID, department, and clearance level.**
- **(Correct)**
- **User role, job title, and organization.**

Explanation

Attribute-Based Access Control (ABAC) is a method of access control that uses attributes of users, objects, and the environment to make access control decisions. ABAC evaluates attributes such as user role, job title,

department, location, time, device type, resource type, and other contextual information to determine whether access should be granted or denied. The policies used in ABAC are typically defined using a set of rules or logical statements that specify the conditions under which access should be granted. This approach offers more granular control over access to resources than some other access control models, such as Role-Based Access Control (RBAC). ABAC is often used in large, complex environments where access control requirements are diverse and constantly changing.

Question 36: **Skipped**

In an organization that uses Mandatory Access Control (MAC), a user wants to access a file that has been classified as "Top Secret". What level of clearance does the user need to access the file?

- **The user needs to have a clearance level equal to or higher than "Top Secret".**
- **(Correct)**
- **The user needs to have a clearance level lower than "Top Secret".**
- **The user cannot access the file.**
- **The user needs to have a "Top Secret" clearance.**

Explanation

In a Mandatory Access Control (MAC) system, access control is determined by a central authority based on predefined policies. The policies typically specify the clearance level required to access a resource. In this case, the user needs to have a clearance level equal to or higher than "Top Secret" to access the file.

Question 37: **Skipped**

What are the types of alarms used in physical security?

- **All of the above**
- **(Correct)**
- **Burglar alarms**
- **Panic alarms**
- **Fire alarms**

Explanation

Physical security systems use a variety of alarms to alert authorities of different types of potential threats. Fire alarms are used to alert authorities of a potential fire, burglar alarms are used to alert authorities of a potential intrusion, and panic alarms are used to alert authorities of an emergency situation where immediate assistance is required. All of these types of alarms play a critical role in maintaining the security of a secure area.

Question 38: **Skipped**

Which of the following is an example of implementing the Principle of Least Privilege?

- **Giving all employees administrative access to their computers.**
- **Restricting access to sensitive information only to the CEO.**
- **Granting all employees access to the company's financial records.**
- **Limiting access to a file server to only those who need to use it for their job.**
- **(Correct)**

Explanation

Limiting access to a file server to only those who need to use it for their job is an example of implementing the Principle of Least Privilege. This ensures that employees only have access to the resources they need to do their job, which reduces the risk of unauthorized access or data breaches.

Question 39: **Skipped**

What type of lock is best for securing valuable items inside a building?

- **Padlock**
- **Keyed lock**
- **Smart lock**
- **Deadbolt lock**
- **(Correct)**

Explanation

Deadbolt locks are best for securing valuable items inside a building as they provide the highest level of security. Deadbolts typically have a longer and stronger bolt that extends further into the door frame, making it more difficult for a would-be intruder to force the door open. They are also difficult to pick, adding an extra layer of security for valuable items.

Question 40: **Skipped**

What is the main purpose of a mantrap in physical security?

- **To allow entry of only one person at a time**
- **(Correct)**
- **To serve as a waiting room**
- **To store hazardous materials**
- **To store valuable assets**

Explanation

A mantrap is a secure room that allows the entry of only one person at a time. It is used to prevent unauthorized access and increase the level of security in high-risk areas by controlling the flow of people entering and exiting.

Question 41: **Skipped**

In a MAC system, access control is determined by:

- **The owner of the resource**
- **A central authority**
- **(Correct)**

- **The system administrator**
- **The user requesting access**

Explanation

In a MAC system, access control is determined by a central authority. The central authority sets and enforces access controls based on policies that have been defined.

Question 42: **Skipped**

What is the main purpose of using a badge system in a cybersecurity setting?

- **To track inventory levels**
- **To monitor employee attendance**
- **To prevent unauthorized access to secure areas**
- **(Correct)**
- **To enforce dress code regulations**

Explanation

The primary purpose of using a badge system in a cybersecurity setting is to prevent unauthorized access to secure areas, such as data centers, server rooms, or restricted areas. The system uses a unique identifier, such as an ID card or key fob, to grant or deny access to certain areas.

Question 43: **Skipped**

What are some common physical security controls used in an organization?

- **Access control systems**

- **Surveillance cameras**
- **Fire suppression systems**
- **All of the above**
- **(Correct)**

Explanation

Common physical security controls used in organizations include access control systems, which restrict access to sensitive areas based on authorization, surveillance cameras, which monitor physical activity and provide a record of security incidents, and fire suppression systems, which prevent fires from spreading and protect equipment and other assets.

Question 44: **Skipped**

In an organization that uses Role-based access control (RBAC), a user has been promoted to a new position. Which action should be taken to adjust the user's access permissions?

- **The user's access permissions should remain the same.**
- **The user should be given unrestricted access to all resources.**
- **The user's access permissions should be modified based on their new job duties.**
- **(Correct)**

- **The user should be required to reapply for access to all resources.**

Explanation

In Role-based access control (RBAC), access control is based on the user's role or job function within the organization. When a user is promoted to a new position, their job duties and associated access permissions may change. The user's access permissions should be modified to reflect their new role and responsibilities.

Question 45: **Skipped**

What is the main purpose of an alarm in physical security?

- **To alert authorities of a potential threat**
- **(Correct)**
- **To provide a backup power source**
- **To deter theft**
- **To scare off intruders**

Explanation

An alarm system in physical security is primarily used to alert authorities or security personnel of a potential threat or intrusion in a secure area. The sound of the alarm acts as a deterrent, but the primary purpose is to notify those who can respond to the threat.

Question 46: **Skipped**

Why is it important to regularly evaluate and update physical security controls?

- **To meet regulatory requirements.**
- **To keep up with advances in technology.**
- **All of the above.**
- **(Correct)**
- **To ensure they are still effective.**

Explanation

All of the above. It is important to regularly evaluate and update physical security controls to ensure they are still effective, keep up with advances in technology, and meet regulatory requirements. This helps to maintain the security of physical assets, and prevent security incidents that could result in theft, damage, or other security incidents.

Question 47: **Skipped**

What type of bollards are best suited for high security areas?

- **Removable bollards**
- **Fixed bollards**
- **(Correct)**
- **Decorative bollards**
- **Retractable bollards**

Explanation

Fixed bollards are best suited for high security areas as they provide the highest level of protection against unauthorized vehicle access and are permanently installed into the ground.

Question 48: **Skipped**

Which of the following is an example of a physical control?

- **Physical locks on doors**
- **(Correct)**
- **Background checks for employees**
- **Employee training programs**
- **Firewall**

Explanation

Physical locks on doors are an example of a physical control because they are a tangible barrier that is designed to prevent unauthorized access to a building or room. They are typically used in conjunction with other security measures, such as access control systems, to provide a comprehensive security solution.

Question 49: **Skipped**

Which of the following is considered a type of physical security control that helps to prevent unauthorized access and provides a secure area for the authentication process?

- **Video Surveillance**

- **Mantrap**
- **(Correct)**
- **Motion Sensors**
- **Electronic Keycard Access**

Explanation

Mantrap is a type of physical security control that is used to secure an area and prevent unauthorized access. It consists of two secure doors or barriers that are interlocked and can only be unlocked if an authorized user enters the correct credentials. Mantraps provide a secure area for the authentication process, allowing organizations to verify the identity of individuals before granting access to restricted areas. The use of mantraps enhances the overall security of a facility by providing an extra layer of protection against unauthorized access.

Question 50: **Skipped**

In a large warehouse, it is important to track the movement of personnel, vehicles, and products to ensure the safety and security of the assets. What type of log can be used for this purpose?

- **Environmental logs**
- **Inventory logs**
- **Access logs**
- **(Correct)**
- **Surveillance logs**

Explanation

Access logs record information about who entered and exited the warehouse and when, which can help to monitor the movement of personnel, vehicles, and products and ensure the safety and security of the assets.

Question 51: **Skipped**

Company XYZ is concerned about the potential for fraud or errors in their accounting department. Which security control should be implemented to reduce this risk?

- **Segregation of Duties**
- **(Correct)**
- **Principle of Least Privilege**
- **Segregation of Duties and the Principle of Least Privilege**
- **None of the above.**

Explanation

The Segregation of Duties should be implemented to reduce the risk of fraud or errors in the accounting department. This control divides responsibilities among multiple employees, which helps ensure that no single employee has complete control over a particular process or resource. This reduces the risk of errors or malicious activities that could result in financial loss or other damage.

Question 52: **Correct**

What is the purpose of physical security controls in an organization?

- **To protect against cyber threats.**
- **To protect against unauthorized access to physical assets.**
- **(Correct)**
- **To protect against environmental hazards.**
- **To protect against all of the above.**

Explanation

Physical security controls are designed to protect against unauthorized access to physical assets, such as buildings, equipment, and sensitive data. They help to ensure that only authorized individuals have access to these assets, and prevent unauthorized access that could result in theft, damage, or other security incidents.

(Domain 4) - Network Security - Results

Question 1: **Skipped**

Which of the following ports is typically used for insecure communication?

- **Port 22**

- **Port 80**
- **(Correct)**
- **Port 3389**
- **Port 443**

Explanation

Port 80 is typically used for insecure communication using the HTTP protocol. HTTP is not encrypted, which means that data transmitted between the client and server can be intercepted and read by unauthorized parties.

Question 2: **Skipped**

Which of the following is a recommended approach for deploying applications across regions and availability zones?

- **Deploying all resources in the same region**
- **Deploying critical resources across multiple regions**
- **(Correct)**
- **Using a single availability zone for all resources**
- **Deploying critical resources across multiple availability zones in the same region**

Explanation

Deploying critical resources across multiple regions provides the highest level of availability and disaster recovery capabilities. By spreading resources across multiple regions, the impact of a potential outage is minimized, and resources can be quickly shifted to

another region in the event of a disaster. While deploying critical resources across multiple availability zones in the same region can also provide increased fault tolerance, deploying across multiple regions is the most comprehensive approach.

Question 3: **Skipped**

What is the primary difference between signature-based detection and behavioral-based detection in an Intrusion Detection System (IDS)?

- **Signature-based detection looks for known patterns of malicious behavior, while behavioral-based detection looks for abnormal behavior patterns.**
- **(Correct)**
- **Signature-based detection is more accurate than behavioral-based detection.**
- **Behavioral-based detection can only be used for network-based IDS.**
- **Signature-based detection relies on pre-configured rules, while behavioral-based detection uses machine learning to detect abnormal behavior.**

Explanation

Signature-based detection relies on pre-configured rules that look for known patterns of malicious behavior, while behavioral-based detection looks for abnormal behavior patterns that deviate from what is considered normal

activity. While signature-based detection can be more accurate in identifying known threats, behavioral-based detection can help detect unknown threats that may not have a pre-configured signature.

Question 4: **Skipped**

What is the primary purpose of a Virtual Local Area Network (VLAN)?

- **To provide remote access to the network**
- **To segment a physical network into multiple logical networks**
- **(Correct)**
- **To encrypt network traffic between two endpoints**
- **To provide redundancy and high availability for critical network resources**

Explanation

Virtual Local Area Networks (VLANs) allow organizations to segment their networks without the need for separate physical switches, which can reduce costs and increase flexibility.

Question 5: **Skipped**

Which of the following protocols is used for file transfers?

- **FTP**
- **(Correct)**
- **UDP**
- **HTTP**

- **TCP**

Explanation

FTP (File Transfer Protocol) is a protocol used for transferring files between computers on a network. It is built on top of TCP and provides additional features such as authentication, encryption, and file management.

Question 6: **Skipped**

Which of the following is a recommended approach for segmenting IoT devices from other network resources?

- **Using virtual private networks (VPNs) to isolate IoT devices**
- **Placing IoT devices on the same network segment as other network resources**
- **Not segmenting IoT devices at all**
- **Implementing network segmentation based on the function of the device**
- **(Correct)**

Explanation

Segmentation is an important strategy for protecting IoT devices from cyberattacks, and the best approach is to segment the network based on the function of the device. This allows for the implementation of security policies specific to the devices and their functions, and can help to limit the impact of a potential attack.

Question 7: **Skipped**

Which of the following is an example of a zero-day attack?

- **A new malware variant that exploits a previously unknown vulnerability.**
- **(Correct)**
- **A malware variant that uses an existing exploit.**
- **A brute-force attack that attempts to guess a user's password.**
- **A phishing email that contains a malicious attachment.**

Explanation

Zero-day attacks typically involve the use of new or unknown malware variants that exploit vulnerabilities that have not yet been discovered or patched. While phishing attacks and brute-force attacks can be effective, they do not necessarily involve zero-day exploits.

Question 8: **Skipped**

What is the primary advantage of Next-Generation Firewalls over traditional firewalls?

- **Next-Generation Firewalls are simpler and easier to manage than traditional firewalls.**
- **Next-Generation Firewalls are faster and more scalable than traditional firewalls.**
- **Next-Generation Firewalls are more effective at blocking spam and other unwanted traffic.**

- **Next-Generation Firewalls are better at detecting and blocking advanced threats.**
- **(Correct)**

Explanation

Next-Generation Firewalls use more advanced techniques than traditional firewalls to inspect traffic and detect threats. This may include deep packet inspection, intrusion prevention, and application awareness, among other features.

Question 9: **Skipped**

Which of the following parties is responsible for drafting a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA)?

- **The legal department of one of the parties involved in the agreement**
- **The party with the most to gain from the agreement**
- **Both parties involved in the agreement**
- **(Correct)**
- **The party with the most negotiating power**

Explanation

Both parties involved in the agreement are responsible for drafting a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA) and ensuring that the terms are acceptable to all parties involved.

Question 10: **Skipped**

In addition to removing leading zeros, what other method can be used to shorten an IPv6 address?

- **By removing trailing zeros from each block**
- **By adding a hyphen between each block**
- **By replacing consecutive blocks of zeros with a double colon**
- **(Correct)**
- **By replacing each block with a single character**

Explanation

Another method for shortening IPv6 addresses is to replace consecutive blocks of zeros with a double colon. This is known as the "compressed" or "collapsed" format and can greatly reduce the length of the address. However, it's important to note that this can also make the address ambiguous if not done correctly.

Question 11: **Skipped**

How does IPv6 support better security than IPv4?

- **By supporting stronger authentication methods**
- **(Correct)**
- **By using a larger address space**
- **By providing more efficient use of radio resources**
- **By using encryption for all network traffic**

Explanation

IPv6 supports stronger authentication methods, such as IPsec, which provides encryption and authentication for

network traffic. This can help to improve network security and protect against unauthorized access and interception of data.

Question 12: **Skipped**

What is a WLAN?

- **A Wired Local Area Network that connects devices using Ethernet cables**
- **A Wireless Local Area Network that connects devices using Wi-Fi technology**
- **(Correct)**
- **A network that connects devices using cellular data**
- **A network that connects devices using satellite technology**

Explanation

A Wireless Local Area Network (WLAN) is a type of LAN that uses wireless technology such as Wi-Fi to connect devices. It allows for greater mobility and flexibility as devices can connect to the network without being physically connected by cables.

Question 13: **Skipped**

What is the purpose of a Demilitarized Zone (DMZ) in a network?

- **To enable remote access to the internal network**
- **To improve network performance by reducing network latency**

- **To protect the internal network from untrusted external networks**
- **(Correct)**
- **To provide a secure area for confidential data**

Explanation

The Demilitarized Zone (DMZ) acts as a buffer zone between the internal network and the internet, allowing organizations to provide services to the public while keeping their internal network secure.

Question 14: **Skipped**

What is sandboxing and how does it protect against malware?

- **A technique for backing up data**
- **A method for detecting malware**
- **A method for encrypting sensitive information**
- **An isolated environment for executing untrusted code**
- **(Correct)**

Explanation

Sandboxing is a technique in which untrusted code, such as downloaded software or emails, is executed in an isolated environment, separate from the main system. This helps prevent malware from infecting the main system, as any malicious code is contained within the

sandbox and cannot access sensitive information or cause harm to the system.

Question 15: **Skipped**

Which layer of the OSI model is responsible for the logical addressing of devices in a network?

- **Data Link Layer**
- **Transport Layer**
- **Physical Layer**
- **Network Layer**
- **(Correct)**

Explanation

The Network Layer (Layer 3) of the OSI model is responsible for logical addressing and routing of data between different networks. This layer defines the IP protocol, which provides logical addressing and routing for devices in a network.

Question 16: **Skipped**

How can nmap be used for network mapping?

- **By testing the strength of user passwords on a network.**
- **By identifying potential vulnerabilities based on version information of software running on network devices.**
- **By identifying hosts and services on a network.**
- **(Correct)**

- **By scanning for open ports on network devices.**

Explanation

Nmap can be used for network mapping by scanning a network and identifying hosts and services. This information can be used to create a map of the network and to identify potential vulnerabilities and misconfigurations. Nmap can also be used to identify the operating system of network devices, which can be useful for network administrators in managing and maintaining the network.

Question 17: **Skipped**

Which device initiates the three-way-handshake?

- **The server**
- **Both devices simultaneously**
- **The network router**
- **The client**
- **(Correct)**

Explanation

In the three-way-handshake, the client initiates the process by sending a SYN message to the server. The server responds with a SYN-ACK message, and then the client sends an ACK message to complete the handshake. The network router is not involved in the three-way-handshake.

Question 18: **Skipped**

Which layer of the OSI model is responsible for identifying and authenticating users?

- **Application layer**
- **(Correct)**
- **Presentation layer**
- **Session layer**
- **Transport layer**

Explanation

The Application layer of the OSI model is responsible for identifying and authenticating users. The Application layer is the topmost layer of the OSI model and provides services that are directly accessible to end users. It includes application protocols, such as HTTP and SMTP, that allow users to interact with networked applications. Identification and authentication are typically provided by application-layer protocols, such as Kerberos and LDAP.

Question 19: **Skipped**

What is a Trojan horse?

- **A type of malware that disguises itself as a useful program**
- **(Correct)**
- **A type of virus that can destroy data**
- **A type of spyware that tracks a user's activities**
- **A type of worm that can spread quickly**

Explanation

A Trojan horse is a type of malware that disguises itself as a harmless or useful program, but once executed, it can cause harm to the system, such as stealing sensitive information or compromising the security of the system.

Question 20: **Skipped**

What is the primary goal of network segmentation in a cybersecurity strategy?

- **To create a single point of failure**
- **To simplify network management**
- **To reduce the attack surface by isolating critical assets and sensitive data**
- **(Correct)**
- **To increase the attack surface by expanding the network**

Explanation

Network segmentation involves dividing a network into smaller subnetworks, which limits the ability of attackers to move laterally and access sensitive data or systems. This helps to prevent the spread of malware, unauthorized access, and other cyber threats.

Question 21: **Skipped**

Which of the following is a characteristic of a multi-tenant cloud data center?

- **Dedicated hardware for each tenant**
- **Location-dependent resource availability**

- **High upfront capital expenditures**
- **Shared hardware resources**
- **(Correct)**

Explanation

A multi-tenant cloud data center is one that serves multiple customers or tenants, with each tenant sharing the same underlying hardware resources. This allows for greater efficiency and cost savings compared to dedicated hardware for each tenant, which is a characteristic of a single-tenant cloud data center. Multi-tenant cloud data centers also typically offer a pay-per-use pricing model, rather than requiring high upfront capital expenditures, and resource availability is not location-dependent.

Question 22: **Skipped**

Which of the following fire suppression systems is not recommended for use in occupied spaces due to the health risks associated with the extinguishing agent?

- **Halon**
- **(Correct)**
- **Dry chemical**
- **Carbon dioxide**
- **Wet chemical**

Explanation

Halon fire suppression systems are not recommended for use in occupied spaces due to the health risks associated

with the extinguishing agent. Halon is a Class I ozone-depleting substance and has been phased out of use in many countries.

Question 23: **Skipped**

What is a serverless cloud, and what are some benefits of using it?

- **Serverless clouds are only suitable for small applications**
- **Serverless clouds require extensive IT resources to maintain**
- **Benefits of using a serverless cloud include reduced costs and increased scalability**
- **A serverless cloud is a cloud computing model where the cloud provider manages the infrastructure and automatically allocates resources to the application**
- **(Correct)**

Explanation

A serverless cloud is a cloud computing model where the cloud provider manages the infrastructure and automatically allocates resources to the application. Benefits of using a serverless cloud include reduced costs and increased scalability.

Question 24: **Skipped**

What is the primary challenge of deploying a Cloud Next-Generation Firewall?

- **Dealing with limited visibility into cloud-based applications and services.**
- **Managing multiple security vendors and solutions.**
- **Dealing with complex and ever-changing threat landscapes.**
- **Ensuring consistent security policies across multiple cloud environments.**
- **(Correct)**

Explanation

One of the primary challenges of deploying a Cloud Next-Generation Firewall is ensuring that security policies are consistent across all cloud environments. This can be difficult because different cloud providers have different security features and requirements.

Question 25: **Skipped**

How can you protect your computer from malware such as viruses, worms, and Trojans?

- **By avoiding suspicious email attachments and downloads**
- **By keeping your operating system and software up-to-date**
- **By installing anti-virus software**
- **All options**
- **(Correct)**

Explanation

To protect your computer from malware, it is recommended to install anti-virus software, keep your operating system and software up-to-date, and avoid suspicious email attachments and downloads. Additionally, practicing safe browsing habits and being cautious of clicking on unknown links can also help protect your system from malware attacks.

Question 26: **Skipped**

What is one of the best ways to protect against phishing attacks?

- **Keeping software up-to-date**
- **Being cautious of suspicious emails and websites**
- **(Correct)**
- **Installing anti-virus software**
- **Regularly backing up data**

Explanation

Phishing attacks are typically carried out through emails or websites that appear to be from a trusted source, but are actually fraudulent. To protect against phishing attacks, it's important to be cautious of emails and websites that ask for sensitive information and to verify the authenticity of any requests before entering personal or financial information.

Question 27: **Skipped**

Which of the following is a potential security risk associated with a Demilitarized Zone (DMZ)?

- **Increased network latency**
- **Reduced availability of services to the public**
- **Lack of visibility into network traffic**
- **Unauthorized access to confidential data**
- **(Correct)**

Explanation

A Demilitarized Zone (DMZ) can be a potential security risk if it is not properly configured, as attackers may be able to use it as a stepping stone to gain access to the internal network and sensitive data. This risk can be mitigated through proper configuration and monitoring of the DMZ.

Question 28: **Skipped**

Which type of VPN requires the installation of client software on each endpoint?

- **MPLS VPN**
- **Remote Access VPN**
- **(Correct)**
- **SSL VPN**
- **Site-to-Site VPN**

Explanation

Remote Access VPNs require client software to be installed on each endpoint in order to establish a secure connection between the remote user and the network.

Question 29: **Skipped**

Which of the following is a key advantage of using a host-based IPS (HIPS) over a network-based IPS (NIPS)?

- **HIPS can monitor all network traffic, while NIPS can only monitor traffic that passes through the network perimeter.**
- **HIPS has lower false positive rates than NIPS.**
- **HIPS is easier to deploy and manage than NIPS.**
- **HIPS can block threats that originate from inside the network, while NIPS can only block external threats.**
- **(Correct)**

Explanation

A HIPS is installed on individual devices and can detect and block threats that originate from inside or outside the network, while a NIPS is installed at the network perimeter and can only detect and block external threats. While HIPS may be more complex to deploy and manage, the benefit of being able to block threats that originate from inside the network outweighs the cost.

Question 30: **Skipped**

Which of the following is a key function of an antivirus program?

- **Protecting against zero-day attacks.**
- **Preventing denial-of-service attacks.**
- **Blocking unauthorized access to the network.**
- **Detecting and removing malware.**
- **(Correct)**

Explanation

An antivirus program is designed to detect and remove various types of malware such as viruses, worms, trojans, and spyware. While some antivirus programs may include features to protect against zero-day attacks or prevent unauthorized access, their primary function is to detect and remove malware.

Question 31: **Skipped**

How many bits are used for the address in IPv4?

- **32 bits**
- **(Correct)**
- **16 bits**
- **128 bits**
- **64 bits**

Explanation

IPv4 uses 32 bits for its address, which allows for approximately 4.3 billion unique addresses. Due to the limited number of available addresses, IPv6 was introduced with a much larger address space. IPv6 uses 128 bit for its address

Question 32: **Skipped**

Which of the following is a key benefit of cloud data centers compared to on-premises infrastructure?

- **More control over data**
- **Lower latency**
- **Better security**
- **Greater scalability**
- **(Correct)**

Explanation

One of the main benefits of cloud data centers is their ability to offer greater scalability compared to on-premises infrastructure. Cloud providers can quickly allocate resources as needed to meet the demands of a workload, while on-premises infrastructure may require more time and resources to scale up. Better security and control over data are potential benefits of on-premises infrastructure, while lower latency is not necessarily a benefit of either option.

Question 33: **Skipped**

What is one of the most important steps in protecting against ransomware attacks?

- **Regularly backing up important data**
- **(Correct)**
- **Installing anti-virus software**
- **Being cautious of suspicious emails and websites**

- **Keeping software up-to-date**

Explanation

Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for a decryption key. Backing up important data regularly is crucial in protecting against ransomware attacks, as it allows a user to restore their data if their files become encrypted. This helps mitigate the impact of a ransomware attack and reduces the chances of the victim being forced to pay the ransom.

Question 34: **Skipped**

Which of the following is a disadvantage of using a dry chemical fire suppression system?

- **It is ineffective on Class A fires**
- **It can cause damage to electronics**
- **(Correct)**
- **It is expensive to install and maintain**
- **It requires a lot of storage space**

Explanation

Dry chemical fire suppression systems can cause damage to electronics and other sensitive equipment due to the residue left behind after use.

Question 35: **Skipped**

What is the primary function of a traditional firewall?

- **To encrypt network traffic to prevent interception.**

- **To block all incoming and outgoing network traffic.**
- **To filter network traffic based on predefined rules.**
- **(Correct)**
- **To monitor network traffic for signs of malware.**

Explanation

The primary function of a traditional firewall is to filter network traffic based on predefined rules. This allows the firewall to block unwanted traffic and allow legitimate traffic to pass through. By filtering network traffic, traditional firewalls can help to protect networks from attacks and unauthorized access.

Question 36: **Skipped**

What is the main purpose of a rootkit?

- **To conceal logs and other system events**
- **(Correct)**
- **To scan for and remove malware from a system**
- **To encrypt data to prevent unauthorized access**
- **To log system events for forensic purposes**

Explanation

The main purpose of a rootkit is to conceal its presence on a system, including logs and other system events, in order to remain undetected and allow an attacker to maintain persistent access to the system.

Question 37: **Skipped**

What is the primary function of a router in a network?

- **To provide wireless connectivity to devices**
- **To filter and block unwanted network traffic**
- **To connect multiple devices in a LAN**
- **To forward data between different networks**
- **(Correct)**

Explanation

A router (operates in layer 3) is a networking device that is used to forward data between different networks (connects two or more packet-switched networks or subnetworks). It uses logical addressing to route data to its destination and can also perform other functions such as filtering and security.

Question 38: **Skipped**

What is the difference between rule-based and statistical anomaly detection in an Intrusion Detection Systems (IDS)?

- **Rule-based detection is more effective than statistical anomaly detection.**
- **Statistical anomaly detection is faster than rule-based detection.**
- **Rule-based detection is used only for network-based IDS.**
- **Rule-based detection relies on pre-configured rules, while statistical anomaly detection looks for anomalies in statistical data.**

- **(Correct)**

Explanation

Rule-based detection uses pre-configured rules that look for specific patterns of malicious behavior or known attacks, while statistical anomaly detection looks for deviations from normal statistical behavior that may indicate an attack. Both methods have their advantages and disadvantages and can be used in conjunction with each other for effective IDS detection.

Question 39: **Skipped**

Which of the following messages is not part of the three-way-handshake?

- **ACK**
- **SYN**
- **RST**
- **FIN**
- **(Correct)**

Explanation

The three-way-handshake involves three messages: SYN (synchronize), SYN-ACK (synchronize-acknowledge), and ACK (acknowledge). FIN (finish) and RST (reset) are not part of the three-way-handshake, although they can be used to terminate a connection.

Question 40: **Skipped**

Which of the following is a common technique used in DDoS attacks?

- **SQL injection**
- **Botnets**
- **(Correct)**
- **Cross-site scripting (XSS)**
- **DNS spoofing**

Explanation

Botnets are a common technique used in DDoS attacks. A botnet is a network of computers that have been infected with malware and can be controlled remotely by an attacker. The attacker can then use the botnet to launch a coordinated DDoS attack, generating a large volume of traffic or requests that overwhelm the target system. DNS spoofing, cross-site scripting, and SQL injection are all techniques used in other types of attacks, but are not typically associated with DDoS attacks.

Question 41: **Skipped**

Why is segmentation important for embedded systems?

- **To prevent unauthorized access to sensitive data**
- **(Correct)**
- **To improve device battery life**
- **To reduce energy consumption**
- **To improve network performance**

Explanation

Segmentation is important for embedded systems because it helps to limit the impact of a potential cyberattack and protect the integrity of the system and its functions. By segmenting the network, access to sensitive data can be restricted, and security policies can be implemented that are specific to the functions of the system. While network performance, energy consumption, and device battery life are also important considerations for embedded systems, preventing unauthorized access to sensitive data is the primary concern.

Question 42: **Skipped**

An organization has implemented network segmentation as part of their defense in depth strategy. Which of the following is an example of an advantage of network segmentation?

- **It increases network performance and speed**
- **It limits the spread of malware and other security threats**
- **(Correct)**
- **It allows all users to access all network resources**
- **It reduces the need for strong passwords and authentication mechanisms**

Explanation

Network segmentation is a technical control that can be used as part of defense in depth to limit the impact of a

security breach by containing the threat within a specific segment of the network.

Question 43: **Skipped**

An organization discovers that a hacker has been accessing its systems for several months and exfiltrating sensitive data. The attacker has used several different methods to gain access, including phishing emails and exploiting unpatched vulnerabilities. What is the most likely type of threat actor responsible for this Advanced persistent threat (APT)?

- **Activists seeking to disrupt the organization's operations or reputation.**
- **Hacktivists seeking to steal sensitive data for political or ideological reasons.**
- **Nation-state actors engaged in espionage or sabotage.**
- **(Correct)**
- **Cybercriminals seeking to steal valuable data for financial gain.**

Explanation

APTs are often associated with nation-state actors seeking to gather intelligence or engage in espionage or sabotage. While cybercriminals, activists, and hacktivists may also engage in APT-style attacks, nation-state actors

are generally considered to be the most advanced and well-resourced threat actors.

Question 44: **Skipped**

Which of the following is a valid shortening of the IPv6 address "2001:0db8:85a3:0000:0000:8a2e:0370:7334"?

- **"2:01:d:b:8:85:a3:0:0:8:a2:e:3:7:0:73:34"**
- **"20:01:db:8:85:a3:0:0:8a:2e:37:0:73:34"**
- **"2001:db8:85a3::8a2e:370:7334"**
- **(Correct)**
- **"2001:db8:85a3:0:0:8a2e:370:7334"**

Explanation

This is a valid shortening of the IPv6 address "2001:0db8:85a3:0000:0000:8a2e:0370:7334", in which the consecutive blocks of zeros have been replaced with a double colon.

Question 45: **Skipped**

Which of the following is a major difference between IPv4 and IPv6?

- **IPv6 uses a simplified header compared to the header used in IPv4.**
- **(Correct)**
- **IPv6 is backward compatible with IPv4, while IPv4 is not backward compatible with IPv6.**
- **IPv6 uses 32-bit addresses, while IPv4 uses 128-bit addresses.**

- **IPv6 does not support multicast, while IPv4 does.**

Explanation

One of the major differences between IPv4 and IPv6 is that the IPv6 header is simplified compared to the IPv4 header, which improves performance and reduces processing overhead. IPv6 also supports multicast and is not fully backward compatible with IPv4.

Question 46: **Skipped**

What is the purpose of a Security Information and Event Management (SIEM) system?

- **To collect, analyze, and correlate security events and alerts from different sources.**
- **(Correct)**
- **To prevent unauthorized access to network devices and resources.**
- **To manage software updates and patching on network devices.**
- **To configure and manage firewalls and access control lists.**

Explanation

A Security Information and Event Management (SIEM) system collects and analyzes security-related data from various sources, such as network devices, servers, and applications, to detect and respond to security incidents in

real-time. It helps to identify and respond to security incidents and threats proactively.

Question 47: **Skipped**

What is the main difference between active and passive attacks?

- **Passive attacks are more dangerous than active attacks**
- **Active attacks are more difficult to detect than passive attacks**
- **Active attacks involve modification or disruption of data, while passive attacks involve monitoring or eavesdropping**
- **(Correct)**
- **Active attacks are carried out by an attacker who is physically present, while passive attacks are carried out remotely**

Explanation

Active attacks are carried out with the goal of modifying or disrupting data in some way. This can involve actions like injecting malware into a system, deleting files, or intercepting and modifying network traffic. In contrast, passive attacks involve monitoring or eavesdropping on data without making any changes. Examples of passive attacks include sniffing network traffic, monitoring user activity, or reading encrypted data. The key difference

between the two is that active attacks seek to actively manipulate data, while passive attacks aim to observe data without detection. While both types of attacks can be dangerous and damaging, active attacks are typically seen as more immediate threats since they can result in more direct harm to systems and data.

Question 48: **Skipped**

Which of the following is an example of a security event that can be detected by a SIEM system?

- **A server running out of disk space.**
- **A printer running low on toner.**
- **An intrusion attempt on a network device.**
- **(Correct)**
- **A user logging into a system with an incorrect password.**

Explanation

A Security Information and Event Management (SIEM) system can detect security events and incidents such as attempted intrusions, malware infections, data exfiltration, and policy violations. It collects logs and events from different sources and correlates them to identify security incidents.

Question 49: **Skipped**

Which of the following protocols is connection-oriented?

- **HTTP**

- **UDP**
- **FTP**
- **TCP**
- **(Correct)**

Explanation

TCP is a connection-oriented protocol. It establishes a connection between the sender and receiver before transmitting data, and it ensures that all packets are delivered in the correct order without loss or duplication.

Question 50: **Skipped**

Which of the following is a key advantage of using both host-based and network-based Intrusion Detection Systems (IDS)?

- **Increased accuracy in detecting threats.**
- **(Correct)**
- **Reduced cost of deployment and maintenance.**
- **Increased network performance.**
- **Reduced false positives.**

Explanation

Host-based IDS (HIDS) monitor individual devices for signs of intrusion, while network-based IDS (NIDS) monitor network traffic for signs of intrusion. By using both types of IDS, you can increase the accuracy of detecting threats and minimize false positives. While deploying and maintaining both types of IDS may be more expensive, the

benefit of increased accuracy in detecting threats outweighs the cost.

Question 51: **Skipped**

Which of the following is a potential challenge with implementing microsegmentation?

- **Increased complexity in network management**
- **(Correct)**
- **Lowered compliance with regulatory requirements**
- **Higher cost of implementing and maintaining network security controls**
- **Reduced network performance**

Explanation

Microsegmentation can make network management more complex as there are more policies and controls to manage. However, this is typically outweighed by the security benefits of microsegmentation.

Question 52: **Skipped**

Which of the following is a common frequency band used for Wi-Fi networks?

- **2.4 GHz & 5 GHz**
- **(Correct)**
- **2.5 GHz**
- **5 GHz**
- **20 GHz**

Explanation

The most common frequency bands used for Wi-Fi networks are 2.4 GHz and 5 GHz. These bands are often divided into multiple channels, which can be used to increase network capacity and reduce interference.

Question 53: **Skipped**

Which of the following protocols is not commonly used for remote access?

- **SSH**
- **Telnet**
- **HTTP**
- **(Correct)**
- **FTP**

Explanation

HTTP (port 80, 8080) is not commonly used for remote access because it is a protocol used for web browsing and does not provide a way to remotely access a device's command line interface. Telnet and SSH are commonly used for remote access, while FTP (File Transfer Protocol) is commonly used for transferring files between devices.

Question 54: **Skipped**

What is the main difference between a DoS and a DDoS attack?

- **A DoS attack is designed to overwhelm a single server, while a DDoS attack is designed to overwhelm multiple servers.**

- **There is no difference between a DoS and a DDoS attack.**
- **A DoS attack is launched from a single computer, while a DDoS attack uses multiple computers.**
- **(Correct)**
- **A DDoS attack is carried out by a single attacker, while a DoS attack involves multiple attackers.**

Explanation

The main difference between a DoS and a DDoS attack is the number of computers involved in the attack. A DoS attack is typically launched from a single computer, while a DDoS attack involves multiple computers that have been infected with malware or hijacked by an attacker. This allows the attacker to generate a much larger volume of traffic or requests, making it more difficult to mitigate the attack.

Question 55: **Skipped**

What is the primary function of a network switch?

- **To provide wireless connectivity to devices**
- **To connect multiple networks together**
- **To forward data between devices on a network**
- **(Correct)**
- **To filter and block unwanted network traffic**

Explanation

A network switch is a networking device that is used to connect devices on a network and to forward data between them. It operates at the Data Link Layer (Layer 2) of the OSI model and uses MAC addresses to forward data between devices.

Question 56: **Skipped**

What is the primary advantage of a Next-Generation Firewall that includes an application-aware component?

- **It can block spam and other unwanted traffic at the application layer.**
- **It can prioritize and allocate bandwidth to critical applications.**
- **It can detect and block unauthorized applications from entering the network.**
- **(Correct)**
- **It can provide visibility into application usage and performance.**

Explanation

An application-aware component of a Next-Generation Firewall can detect and block applications based on their specific protocols and behaviors. This allows the firewall to prevent unauthorized or malicious applications from entering the network.

Question 57: **Skipped**

How does a virus spread to other systems?

- **Through instant messaging**
- **Through infected software downloads**
- **All options**
- **(Correct)**
- **Through email attachments**

Explanation

A virus can spread through various methods, including email attachments, infected software downloads, and instant messaging. It can also spread through removable media such as USB drives or through networks.

Question 58: **Skipped**

How does microsegmentation differ from traditional network segmentation?

- **Microsegmentation is focused on isolating individual workloads or applications, while traditional network segmentation is based on factors such as departments or functions.**
- **(Correct)**
- **Microsegmentation is less effective at preventing lateral movement within the network than traditional network segmentation.**
- **Microsegmentation is used primarily in cloud environments, while traditional network segmentation is used in on-premises networks.**

- **Microsegmentation does not require the use of software-defined networking (SDN), while traditional network segmentation does.**

Explanation

Microsegmentation is focused on isolating individual workloads or applications, while traditional network segmentation is based on factors such as departments or functions. Microsegmentation takes network segmentation to a more granular level, isolating individual workloads or applications with their own set of security controls.

Question 59: **Skipped**

Which of the following is a typical component of a Demilitarized Zone (DMZ)?

- **Domain controller**
- **Web server**
- **(Correct)**
- **Database server**
- **File server**

Explanation

A web server is a typical component of a DMZ, as it is used to provide services to the public while keeping the internal network secure. Database servers and file servers are typically located in the internal network, while domain

controllers are used for user authentication and are also typically located in the internal network.

Question 60: **Skipped**

Which protocol operates at the Transport layer and provides reliable, connection-oriented data transfer?

- **TCP**
- **(Correct)**
- **HTTP**
- **FTP**
- **UDP**

Explanation

TCP (Transmission Control Protocol) operates at the Transport layer and provides reliable, connection-oriented data transfer. TCP provides a reliable, ordered, and error-checked delivery of data by establishing a connection between two devices and exchanging packets until all the data is successfully delivered.

Question 61: **Skipped**

Which of the following is not a benefit of implementing Network Access Control (NAC)?

- **Identifying unauthorized devices attempting to access the network**
- **Mitigating the risk of data breaches and malware infections**

- **Enforcing security policies on all devices accessing the network**
- **Enhancing network performance by reducing network traffic**
- **(Correct)**

Explanation

While NAC can help to identify and mitigate security risks, it can also add overhead to the network and potentially slow down network performance.

Question 62: **Skipped**

Which of the following is a limitation of Network Intrusion Detection Systems (NIDS)?

- **They are only effective for detecting external attacks, not internal attacks.**
- **They can only detect known signatures and patterns of malicious behavior.**
- **They can only detect attacks on the network layer, not the application layer.**
- **(Correct)**
- **They cannot detect attacks that originate from inside the network.**

Explanation

Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic and detect anomalies in network traffic that may indicate an intrusion or unauthorized

access attempt. However, NIDS are limited in their ability to detect attacks on the application layer. While NIDS can detect internal attacks, they are also limited in their ability to detect unknown or zero-day attacks that do not have a known signature or pattern of malicious behavior.

Question 63: **Skipped**

What is IP Spoofing?

- **An attack that intercepts communication between two parties to steal or manipulate data**
- **An attack that floods a network or server with packets that exceed the maximum allowed size**
- **An attack that involves altering the source IP address in a packet to hide the identity of the sender**
- **(Correct)**
- **An attack that impersonates a legitimate website or service to steal sensitive information**

Explanation

IP Spoofing is an attack that involves altering the source IP address in a packet to hide the identity of the sender. This can be used to launch various types of attacks, such as Denial-of-Service attacks, by flooding a target network with traffic that appears to be coming from legitimate sources.

Question 64: **Skipped**

Which cloud service model is most suitable for organizations that want to develop and deploy custom software applications?

- **Infrastructure as a Service (IaaS)**
- **None.**
- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **(Correct)**

Explanation

Platform as a Service (PaaS) is a cloud service model that provides developers with a platform for building, testing, and deploying applications without having to worry about the underlying infrastructure. This makes it an ideal choice for organizations that want to develop and deploy custom software applications, as it can provide the necessary tools and services to support the software development lifecycle. SaaS and IaaS may be suitable for other types of applications or workloads, but they do not offer the same level of platform services.

Question 65: **Skipped**

What is a region in cloud computing?

- **A set of data centers located in different geographical locations**
- **(Correct)**
- **A set of tools for managing cloud resources**

- **A collection of databases that share resources**
- **A group of virtual machines with similar configurations**

Explanation

In cloud computing, a region refers to a geographic area where cloud resources are hosted. A region typically consists of multiple data centers, which are located in different geographical locations to provide redundancy and improve fault tolerance. By spreading resources across multiple data centers in different regions, cloud providers can offer higher levels of availability and disaster recovery capabilities.

Question 66: **Skipped**

What is the purpose of an Intrusion Detection System (IDS)?

- **To prevent all unauthorized access to a network or system.**
- **To block incoming network traffic from known malicious sources.**
- **To detect and alert administrators to potential security breaches.**
- **(Correct)**
- **To monitor user activity and enforce compliance policies.**

Explanation

Intrusion Detection System (IDS) is designed to detect and alert administrators to potential security breaches or unauthorized access attempts to a system or network. While IDS can help prevent security breaches, they are not foolproof and cannot prevent all unauthorized access.

Question 67: **Skipped**

What is the main purpose of a Memorandum of Understanding (MOU)?

- **To outline the terms and conditions of a business transaction**
- **To specify the ownership of intellectual property**
- **To establish a working relationship between two organizations**
- **(Correct)**
- **To provide legal protection for parties involved in a business transaction**

Explanation

The main purpose of a Memorandum of Understanding (MOU) is to establish a working relationship between two organizations and define the terms and conditions of the collaboration.

Question 68: **Skipped**

Which of the following is a common way that zero-day attacks are discovered?

- **Through analysis of network traffic logs.**

- **Through user reporting of suspicious activity.**
- **Through monitoring of system performance metrics.**
- **Through analysis of malware samples.**
- **(Correct)**

Explanation

Zero-day attacks are often discovered through the analysis of malware samples collected from infected systems. This analysis can help identify previously unknown malware variants and the vulnerabilities they exploit. While network traffic logs, system performance metrics, and user reporting can also provide valuable information, they may not necessarily lead to the discovery of zero-day exploits.

Question 69: **Skipped**

What is the difference between a LAN and a WAN?

- **A LAN provides greater security than a WAN**
- **A LAN connects devices in a small geographical area, while a WAN connects devices over a large geographical area**
- **(Correct)**
- **A LAN uses Wi-Fi technology, while a WAN uses cellular technology**
- **A LAN is typically faster than a WAN**

Explanation

A Local Area Network (LAN) is a network that connects devices in a local area, while a WAN (Wide Area Network)

connects devices over a larger geographical area such as a city, state, or country. WANs typically use internet or other long-distance networks to connect devices.

Question 70: **Skipped**

What is a SSID in a Wi-Fi network?

- **A security protocol used to encrypt network traffic**
- **A unique identifier for each device on the network**
- **(Correct)**
- **A unique name used to identify the network**
- **A password used to access the network**

Explanation

The SSID (Service Set Identifier) is a unique name used to identify a Wi-Fi network. This name is used by devices to connect to the network and can be set by the network administrator

Question 71: **Skipped**

Which of the following protocols is considered to be more secure for remote access?

- **SSH**
- **(Correct)**
- **Telnet**
- **HTTP**
- **FTP**

Explanation

SSH (Secure Shell) is considered to be more secure for remote access because it encrypts data transmitted between the client and server, while Telnet does not. This means that sensitive information, such as login credentials, is protected from interception and unauthorized access.

Question 72: **Skipped**

Which of the following is a key element of an effective SLA?

- **Clear, measurable performance metrics.**
- **(Correct)**
- **Ambiguous service availability guarantees.**
- **Vague, non-specific language.**
- **A lack of clear responsibilities for the service provider and the client.**

Explanation

An effective SLA (Service Level Agreement) should include clear, measurable performance metrics that allow both parties to assess whether the service is being delivered as promised, and to identify areas for improvement or dispute resolution. Vague or ambiguous language, as well as unclear responsibilities, can lead to misunderstandings and disagreements between the parties.

Question 73: **Skipped**

A company is migrating to a cloud-based solution and is considering using a zero trust security model. Which of the following is a characteristic of zero trust security that would benefit the company's migration?

- **The model assumes all users and devices are trustworthy.**
- **Continuous monitoring and analysis of user and device behavior is a core feature.**
- **(Correct)**
- **The model relies on network segmentation to protect against threats.**
- **Access control is based on user roles and permissions.**

Explanation

Zero trust security model assumes that no user or device can be trusted automatically, and continuous monitoring and analysis of user and device behavior is crucial to detect any suspicious activities or anomalies. This is particularly important in a cloud-based solution, as the network perimeter is blurred and traditional security measures such as firewalls and network segmentation may not be sufficient. Therefore, implementing a zero trust security model that includes continuous monitoring can help detect and prevent potential security breaches.

Question 74: **Skipped**

Which of the following is true about zero-day attacks?

- **They are well-known and widely documented.**
- **They exploit vulnerabilities that have not yet been discovered or patched.**
- **(Correct)**
- **They can be detected and prevented using signature-based detection methods.**
- **They exploit vulnerabilities that have been previously disclosed and patched.**

Explanation

Zero-day attacks are exploits that target unknown vulnerabilities in software or systems. Since these vulnerabilities are unknown to the software vendor and are not yet patched, zero-day attacks can be difficult to detect and prevent.

Question 75: **Skipped**

Which component of the on-premises infrastructure is responsible for providing backup power in case of a power outage?

- **HVAC**
- **Environmental**
- **Power Generator**
- **(Correct)**
- **Data center/closets**

Explanation

The power generator component of the on-premises infrastructure is responsible for providing backup power in case of a power outage. This is important because a power outage can cause servers to shut down and data to be lost.

Question 76: **Skipped**

Which of the following best describes Network Access Control (NAC)?

- **A security strategy that monitors network traffic for suspicious activity**
- **A security strategy that uses encryption to secure network traffic**
- **A security strategy that restricts access to a network based on device identity**
- **(Correct)**
- **A security strategy that limits access to a network based on user identity**

Explanation

The Network Access Control (NAC) is a security strategy that enforces security policies on devices attempting to access a network, based on their identity and compliance status.

Question 77: **Skipped**

Which of the following best describes the difference between passive and active side-channel attacks?

- **Passive attacks involve only monitoring of signals, while active attacks involve injecting noise or manipulating signals.**
- **(Correct)**
- **Passive attacks can only be carried out against wired devices, while active attacks can target wireless devices.**
- **Passive attacks rely on physical access to the target device, while active attacks do not.**
- **Passive attacks are more difficult to detect than active attacks.**

Explanation

Passive attacks involve only monitoring of signals, while active attacks involve injecting noise or manipulating signals. Passive side-channel attacks rely on monitoring signals emitted by a device, such as power consumption, electromagnetic radiation, or acoustic emissions, to extract sensitive information. Active side-channel attacks, on the other hand, involve injecting noise or manipulating signals to cause the device to leak information.

Question 78: **Skipped**

How can a SIEM system help with compliance requirements?

- **By configuring and managing firewalls and access control lists.**

- **By preventing unauthorized access to network devices and resources.**
- **By managing software updates and patching on network devices.**
- **By generating reports and alerts for compliance violations.**
- **(Correct)**

Explanation

A Security Information and Event Management (SIEM) system can help organizations to comply with regulations such as HIPAA, PCI-DSS, and GDPR by collecting and analyzing log data from different sources and generating compliance reports. It can also provide real-time alerts for compliance violations and help organizations to detect and respond to security incidents that may lead to non-compliance.

Question 79: **Skipped**

Which of the following protocols can be used with public key authentication?

- **SSH**
- **(Correct)**
- **HTTP**
- **FTP**
- **Telnet**

Explanation

SSH supports public key authentication, which provides a more secure and convenient method of authentication compared to passwords. Public key authentication uses a public key and private key pair, where the private key is kept by the user and the public key is uploaded to the server.

Question 80: **Skipped**

Which component of the on-premises infrastructure is responsible for providing redundancy in case of a hardware failure?

- **Data center/closets**
- **Redundancy**
- **(Correct)**
- **HVAC**
- **Power Generator**

Explanation

The redundancy component of the on-premises infrastructure is responsible for providing backup hardware in case of a hardware failure. This is important because hardware failures can cause downtime and data loss if not properly addressed.

Question 81: **Skipped**

A manufacturing company needs to run compute-intensive simulations and modeling for product design. The company has a dedicated IT team and needs

to maintain control over its data. Which cloud model would be the best fit for this scenario?

- **Private cloud**
- **(Correct)**
- **Community cloud**
- **Hybrid cloud**
- **Public cloud**

Explanation

The best cloud model for this scenario would be a private cloud, as it allows the company to maintain full control over its compute resources and data, which is crucial for running compute-intensive simulations and modeling for product design.

Question 82: **Skipped**

Which component of the on-premises infrastructure is responsible for maintaining a stable and consistent temperature for the servers?

- **Environmental**
- **HVAC**
- **(Correct)**
- **Data center/closets**
- **Power**

Explanation

he Heating, Ventilation, and Air Conditioning (HVAC) component of the on-premises infrastructure is

responsible for maintaining a stable and consistent temperature for the servers. This is important because servers can overheat and malfunction if the temperature is not properly controlled.

Question 83: **Skipped**

What is the primary function of a firewall in a network?

- **To filter and block unwanted network traffic**
- **(Correct)**
- **To connect multiple devices in a LAN**
- **To provide wireless connectivity to devices**
- **To forward data between different networks**

Explanation

A firewall is a security device that is used to filter and block unwanted network traffic. It can be used to protect a network from unauthorized access and to prevent attacks such as denial-of-service (DoS) attacks and malware infections.

Question 84: **Skipped**

What is the main difference between a virus and a worm?

- **A virus is a program that is attached to a file, while a worm is a standalone program.**
- **A worm can replicate itself, while a virus cannot.**
- **(Correct)**
- **A virus is designed to harm a computer system, while a worm is not.**

- **A worm spreads through email, while a virus spreads through instant messaging.**

Explanation

A worm is a standalone program that can replicate itself and spread to other systems without human intervention, while a virus needs a host file to infect and spread to other systems.

Question 85: **Skipped**

Which of the following fire suppression systems uses a gas as the extinguishing agent?

- **Clean agent**
- **(Correct)**
- **Dry chemical**
- **Foam**
- **Wet chemical**

Explanation

Clean agent systems use a gas as the extinguishing agent to suppress fires. These systems are commonly used to protect sensitive equipment and electronics.

Question 86: **Skipped**

Which of the following is an example of a Side-channel attack that targets a device's power consumption?

- **Timing attack**
- **Acoustic attack**
- **Differential power analysis**

- **(Correct)**
- **Electromagnetic attack**

Explanation

Differential power analysis is a side-channel attack that involves analyzing a device's power consumption during cryptographic operations to infer information about the secret key being used. Electromagnetic and acoustic attacks are also side-channel attacks, but they target different types of signals emitted by the device. Timing attacks involve measuring the time it takes for a device to perform certain operations.

Question 87: **Skipped**

Which of the following is a key benefit of IPv6?

- **Lower network security**
- **Increased network latency**
- **Reduced bandwidth**
- **More efficient routing**
- **(Correct)**

Explanation

IPv6 offers more efficient routing than IPv4, which can improve network performance and reduce congestion. The larger address space of IPv6 can also help to reduce the size of routing tables and the amount of network traffic required for routing.

Question 88: **Skipped**

Which of the following is a potential security risk associated with connected Internet of Things (IoT) devices?

- **Interference from other connected devices**
- **Vulnerabilities in software and firmware**
- **(Correct)**
- **Limited battery life of devices**
- **Inability to connect to the internet**

Explanation

While the other options may be challenges or limitations associated with IoT devices, vulnerabilities in software and firmware can pose a serious security risk. Flaws in software or firmware can potentially allow attackers to gain access to sensitive data or control over the device, and IoT devices can be particularly vulnerable to such attacks.

Question 89: **Skipped**

What are some common use cases for IaaS (Infrastructure as a Service)?

- **Email marketing, online advertising, and content management**
- **Social media management, video editing, and mobile app development**
- **Development and testing environments, website hosting, and data backup and recovery**

- **(Correct)**
- **Customer relationship management (CRM), supply chain management, and enterprise resource planning (ERP)**

Explanation

Common use cases for IaaS include development and testing environments, website hosting, and data backup and recovery. IaaS provides businesses with on-demand access to computing resources, allowing them to quickly and easily scale their infrastructure as needed.

Question 90: **Skipped**

What is the difference between a managed service provider (MSP) and a cloud service provider (CSP)?

- **MSPs and CSPs are the same thing**
- **CSPs provide SaaS, PaaS, or IaaS, while MSPs provide managed IT services**
- **(Correct)**
- **MSPs manage IT infrastructure, while CSPs provide cloud-based services**
- **MSPs provide IT consulting services, while CSPs manage cloud infrastructure**

Explanation

While MSPs and CSPs can both provide IT-related services, they are not the same thing. MSPs typically provide managed IT services, which can include managing IT

infrastructure, providing support for hardware and software issues, and offering other IT-related services. CSPs, on the other hand, provide cloud-based services such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

Question 91: **Skipped**

Which protocol is used for online gaming?

- **DNS**
- **UDP**
- **(Correct)**
- **ICMP**
- **TCP**

Explanation

UDP (User Datagram Protocol) is a protocol used for online gaming. It is a connectionless protocol that allows for fast and efficient data transmission, which is important for online gaming. Unlike TCP, UDP does not guarantee delivery of data, but this is not as important for online gaming as it is for other applications. In online gaming, speed is often more important than reliability, and UDP allows for faster transmission of data.

Question 92: **Skipped**

What is Spoofing?

- **An attack that floods a network or server with packets that exceed the maximum allowed size**

- **An attack that intercepts communication between two parties to steal or manipulate data**
- **An attack that impersonates a legitimate website or service to steal sensitive information**
- **(Correct)**
- **An attack that targets a specific person or organization to steal sensitive information**

Explanation

Spoofing is an attack that involves impersonating a legitimate website or service to steal sensitive information. This can include email spoofing, DNS spoofing, or IP address spoofing, among others.

Question 93: **Skipped**

As a network administrator, how can you protect a network or server against Oversized packet attacks?

- **By installing antivirus software on all devices**
- **By implementing rate limiting to limit the number of packets that can be sent to a system**
- **(Correct)**
- **By using firewalls to block incoming traffic from known malicious sources**
- **By using intrusion detection systems to monitor network traffic for signs of an attack**

Explanation

An Oversized packet attack is an attack that floods a network or server with packets that exceed the maximum allowed size. This can cause the victim's system to become overwhelmed and unresponsive. To protect against Oversized packet attacks, a network or server can implement rate limiting to limit the number of packets that can be sent to a system. This helps to ensure that the system is not overwhelmed by a flood of packets that exceed the maximum allowed size. Additionally, network and server administrators can implement filtering rules to block traffic that contains oversized packets, as well as other security measures such as firewalls and intrusion detection systems to further protect against attacks.

Question 94: **Skipped**

What is the purpose of NAT?

- **To provide security to a network**
- **To control network traffic**
- **To map private IP addresses to public IP addresses**
- **(Correct)**
- **To identify devices on the internet**

Explanation

The purpose of NAT is to enable devices in a private network to access the internet using a public IP address. It works by mapping private IP addresses to

Question 95: **Skipped**

Which OSI layer is responsible for compressing and encrypting data?

- **Application layer**
- **Transport layer**
- **Presentation layer**
- **(Correct)**
- **Session layer**

Explanation

The Presentation layer of the OSI model is responsible for compressing and encrypting data. The Presentation layer is responsible for the formatting and encryption of data for transmission between applications. It ensures that the data is in a format that the application can understand, and may also provide compression and encryption services to reduce the amount of data being transmitted and to secure it against unauthorized access.

Question 96: **Skipped**

What is a repeater in a WLAN?

- **A device that amplifies and retransmits wireless signals**
- **(Correct)**
- **A device that connects two LANs together**
- **A device that provides wireless access to devices**
- **A device that blocks unwanted network traffic**

Explanation

A repeater is a device that receives a wireless signal and amplifies it, then retransmits the signal to extend the range of the wireless network. It is often used in large WLANs to ensure that all devices are within range of the wireless access point.

Question 97: **Skipped**

Which of the following is a key difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?

- **An IDS detects and logs potential threats, while an IPS blocks potential threats.**
- **(Correct)**
- **An IDS is deployed at the network perimeter, while an IPS is deployed on individual devices.**
- **An IDS uses signature-based detection, while an IPS uses behavioral-based detection.**
- **An IDS monitors network traffic, while an IPS monitors system files and logs.**

Explanation

An IDS detects potential threats and logs information about them, while an IPS not only detects potential threats but also takes action to block them. An IPS can be deployed at the network perimeter or on individual devices and can use various methods such as signature-based detection and behavioral-based detection.

Question 98: **Skipped**

Which of the following statements is true regarding the three-way-handshake?

- **It is used to encrypt data during transmission**
- **It ensures both devices are ready and willing to communicate**
- **(Correct)**
- **It involves only two messages exchanged between two devices**
- **It is only used for establishing a connection between servers and not between client and server**

Explanation

The three-way-handshake involves three messages exchanged between two devices, and its purpose is to ensure that both sides are ready and willing to communicate. It is not used to encrypt data during transmission, and it is used for establishing connections between both servers and clients.

Question 99: **Skipped**

What is the purpose of an SLA?

- **To establish clear expectations and responsibilities for both the service provider and the client.**
- **(Correct)**
- **To provide a guarantee of 100% uptime for a service.**

- **To ensure that the service provider can charge as much as possible for their services.**
- **To protect the service provider from liability in case of service disruptions.**

Explanation

An SLA (Service Level Agreement) is intended to establish clear expectations and responsibilities for both the service provider and the client, and to provide a framework for resolving disputes and ensuring that the service is delivered in a consistent and reliable manner.

Question 100: **Skipped**

What is NAT?

- **Network Administration Tool**
- **Network Access Technology**
- **Network Authentication Token**
- **Network Address Translation**
- **(Correct)**

Explanation

Network Address Translation (NAT) is a networking technique that enables devices in a private network to access the internet using a public IP address. It works by mapping private IP addresses to a public IP address, allowing multiple devices to share a single public IP address.

Question 101: **Skipped**

Which of the following is a benefit of using IPv6 over IPv4?

- **IPv6 is easier to configure than IPv4.**
- **IPv6 supports a larger number of devices.**
- **(Correct)**
- **IPv6 is faster than IPv4.**
- **IPv6 is more secure than IPv4.**

Explanation

IPv6 has a much larger address space compared to IPv4, which allows for a larger number of unique addresses and supports the growing number of devices connected to the internet. While IPv6 does offer other benefits, such as improved security and simplified addressing, the larger address space is one of its most significant advantages.

Question 102: **Skipped**

Which OSI layer is responsible for detecting and correcting errors in data transmission?

- **Network layer**
- **Data Link layer**
- **(Correct)**
- **Transport layer**
- **Presentation layer**

Explanation

The Data Link layer of the OSI model is responsible for detecting and correcting errors in data transmission. The

Data Link layer is responsible for the reliable transmission of data across a physical link. It provides services such as error detection and correction, flow control, and framing of data for transmission over the physical link.

Question 103: **Skipped**

Which layer of the OSI model is responsible for establishing and maintaining communication sessions between applications?

- **Transport layer**
- **Data Link layer**
- **Session layer**
- **(Correct)**
- **Network layer**

Explanation

The Session layer of the OSI model is responsible for establishing and maintaining communication sessions between applications. The Session layer provides services that allow applications to establish, manage, and terminate communication sessions. This includes the coordination of the session and the synchronization of data exchange between the applications.

Question 104: **Skipped**

Which of the following is an example of an active attack?

- **Interfering with wireless signals to disrupt network communication**

- **Monitoring a user's internet activity to gather data on their behavior**
- **Running a port scan to identify open network ports**
- **Installing a keylogger on a target computer to capture login credentials**
- **(Correct)**

Explanation

Active attacks involve a deliberate attempt to modify or disrupt data. Installing a keylogger on a target computer is an example of an active attack aimed at capturing login credentials. The other options describe different types of passive attacks. Monitoring internet activity, interfering with wireless signals, and running a port scan are all forms of passive attack aimed at eavesdropping or observing data without making changes.

Question 105: **Skipped**

What is the primary purpose of IPSec protocol?

- **To provide redundancy and high availability for critical network resources**
- **To provide remote access to the network**
- **To encrypt network traffic between two endpoints**
- **(Correct)**
- **To segment a physical network into multiple logical networks**

Explanation

IPSec is a protocol suite used to provide security services, including authentication and encryption, for IP-based communication.

Question 106: **Skipped**

Which of the following protocols is used for web browsing?

- **UDP**
- **TCP**
- **FTP**
- **HTTP**
- **(Correct)**

Explanation

HTTP (Hypertext Transfer Protocol) is a protocol used for web browsing. It is built on top of TCP and is used for transferring web page content, such as HTML, images, and video. HTTP is a request-response protocol, where a client sends a request to a server, and the server responds with the requested content.

Question 107: **Skipped**

A government agency needs to host a web application that requires high availability and scalability. The agency has a dedicated IT team and needs to maintain control over its data. Which cloud model would be the best fit for this scenario?

- **Public cloud**

- **Community cloud**
- **Hybrid cloud**
- **(Correct)**
- **Private cloud**

Explanation

The best cloud model for this scenario would be a hybrid cloud, as it allows the agency to leverage the scalability and cost-effectiveness of public cloud resources, while maintaining control over its data with a private cloud. High availability can be achieved by load balancing across both cloud models.

Question 108: **Skipped**

How can you protect yourself from a Man-in-the-Middle (MITM) attack?

- **Use the same password for multiple accounts**
- **Click on any link or attachment in an email from a trusted source**
- **Only visit websites with a valid SSL/TLS certificate**
- **(Correct)**
- **Always use public Wi-Fi hotspots to access sensitive information**

Explanation

Websites with a valid SSL/TLS certificate encrypt the communication between your computer and the website, making it more difficult for an attacker to intercept the

communication and steal sensitive information. Using unique passwords for each account and avoiding public Wi-Fi hotspots can also help protect against MITM attacks. It's important to avoid clicking on links or attachments in emails from untrusted sources, as they could lead to fake websites or malware that can compromise your security.

Question 109: **Skipped**

Which of the following is a potential privacy concern when using CCTV (Closed Circuit Television) in the on-premises infrastructure?

- **The cameras may not have enough storage space**
- **The cameras may not be secured properly**
- **The cameras may not be installed correctly**
- **The cameras may capture sensitive information**
- **(Correct)**

Explanation

CCTV (Closed Circuit Television) cameras may capture sensitive information, such as personal data, that may be subject to privacy regulations. Proper measures should be taken to secure and protect this information.

Question 110: **Skipped**

A group of healthcare providers wants to share patient data securely and in compliance with regulatory

requirements. Which cloud model is best suited for their needs?

- **Public cloud**
- **Private cloud**
- **Hybrid cloud**
- **Community cloud**
- **(Correct)**

Explanation

Community cloud allows a group of organizations with similar requirements to share resources and infrastructure while maintaining control over their data. In this scenario, a community cloud model is suitable for the healthcare providers to share patient data securely and comply with regulatory requirements.

Question 111: **Skipped**

What is the Open Systems Interconnection (OSI) model?

- **A model for network communications that defines a five-layer architecture.**
- **A network architecture model that defines the communications protocol used by the internet.**
- **A network protocol used for wireless communication.**
- **A model for network communications that defines a seven-layer architecture.**
- **(Correct)**

Explanation

The OSI model is a model for network communications that defines a seven-layer architecture. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Question 112: **Skipped**

Which of the following is not an advantage of implementing defense in depth security strategy?

- **Reducing the likelihood of a successful attack**
- **Providing multiple layers of protection to ensure complete security**
- **Allowing for quick and easy access to resources**
- **(Correct)**
- **Minimizing the impact of a successful attack**

Explanation

One of the main goals of defense in depth is to provide multiple layers of protection to ensure complete security, which often comes at the cost of quick and easy access to resources.

Question 113: **Skipped**

What is the loopback address and what is its purpose?

- **It is a private IP address used for communication within a local network**
- **It is a reserved IP address used for network administration purposes**
- **It is a special IP address used for establishing a connection between a client and a server running on the same device**
- **(Correct)**
- **It is a public IP address used for connecting to the internet**

Explanation

The loopback address, 127.0.0.1, is a reserved IP address that is used to establish a connection between a client and a server running on the same device. It is often used for testing and debugging purposes, where a program needs to communicate with itself.

Question 114: **Skipped**

What is WPA2, a common security protocol used for Wi-Fi networks?

- **Wireless Power Amplification 2**
- **Wi-Fi Packet Analyzer 2**
- **Wireless Policy Authentication 2**
- **Wi-Fi Protected Access 2**
- **(Correct)**

Explanation

WPA2 (Wi-Fi Protected Access 2) is a security protocol used to encrypt network traffic and protect Wi-Fi networks from unauthorized access. It is a widely used security standard for Wi-Fi networks and provides strong encryption and authentication mechanisms.

Question 115: **Skipped**

Which of the following is not a common method used for Network Access Control?

- **MAC address filtering**
- **802.1x authentication**
- **Password authentication**
- **(Correct)**
- **IP address filtering**

Explanation

While passwords are commonly used for user authentication, they are not typically used as a method of Network Access Control. Instead, NAC typically uses methods such as 802.1x authentication, MAC address filtering, and IP address filtering to enforce security policies on devices attempting to access the network.

Question 116: **Skipped**

Which of the following is an example of network segmentation?

- **Installing antivirus software on all devices in the network**
- **Setting up a firewall to block incoming traffic**
- **Using a password manager to securely store login credentials**
- **Separating the finance department's network from the rest of the organization**
- **(Correct)**

Explanation

Separating the finance department's network from the rest of the organization. This is an example of logical network segmentation, where different parts of the network are isolated from each other to prevent unauthorized access or data breaches.

Question 117: **Skipped**

Which type of VPN is typically used to connect multiple sites together?

- **SSL VPN**
- **MPLS VPN**
- **Site-to-Site VPN**
- **(Correct)**
- **Remote Access VPN**

Explanation

Site-to-Site VPNs are typically used to connect multiple sites together and allow communication between networks over a secure, encrypted connection.

Question 118: **Skipped**

What is a Private IP Address?

- **An IP address that is reserved for use in a private network**
- **(Correct)**
- **An IP address that is assigned by an internet service provider (ISP)**
- **An IP address that is publicly accessible on the internet**
- **An IP address that is used by a network router to connect to the internet**

Explanation

Private IP addresses are reserved for use in private networks and are not publicly accessible on the internet. They are used to identify devices within a network and are not unique globally, which means that multiple networks can use the same private IP address range.

Question 119: **Skipped**

What is the purpose of a DoS or DDoS attack?

- **To modify or manipulate data on a target system**
- **To steal sensitive data from a target system**
- **To disrupt or disable a target system or network**

- **(Correct)**
- **To establish a persistent presence on a target system**

Explanation

The primary purpose of a DoS or DDoS attack is to overwhelm a target system or network with traffic or requests, making it unavailable to users. This can be done for a variety of reasons, including to extort money, to protest against an organization or government, or simply to cause chaos and disruption. The other options are not typically associated with DoS or DDoS attacks.

Question 120: **Skipped**

Which of the following is an example of an On-Path attack?

- **Cross-site scripting (XSS) attack**
- **SQL injection attack**
- **Distributed Denial of Service (DDoS) attack**
- **Man-in-the-middle (MitM) attack**
- **(Correct)**

Explanation

Man-in-the-middle (MitM) attack is a type of On-Path attack that involves intercepting and possibly modifying network traffic between two communicating parties. This can be accomplished by impersonating one or both parties, or by redirecting traffic through an attacker-controlled device.

Question 121: **Skipped**

What is the primary purpose of a Virtual Private Network (VPN)?

- **To segment a physical network into multiple logical networks**
- **To provide redundancy and high availability for critical network resources**
- **To encrypt network traffic between two endpoints**
- **(Correct)**
- **To provide remote access to the network**

Explanation

VPNs allow organizations to provide secure, encrypted communication between two endpoints over an untrusted network, such as the internet.

Question 122: **Skipped**

Which of the following is a benefit of using multiple availability zones?

- **Lower cost**
- **Increased fault tolerance**
- **(Correct)**
- **Reduced network latency**
- **Improved scalability**

Explanation

Using multiple availability zones helps to increase fault tolerance by spreading resources across multiple data

centers in different locations. By ensuring that resources are not concentrated in a single data center, the impact of a potential outage is minimized. While using multiple availability zones may provide benefits such as reduced network latency and improved scalability, the primary benefit is increased fault tolerance.

Question 123: **Skipped**

Can the loopback address be used to communicate with other devices on a network?

- **No, it can only be used to communicate with the device it is running on**
- **(Correct)**
- **It can be used to communicate with other devices on a network, but it requires additional configuration**
- **Yes, it can be used to communicate with any device on a network**
- **It depends on the type of network being used**

Explanation

The loopback address is used to establish a connection between a client and a server running on the same device, and cannot be used to communicate with other devices on a network. It is a reserved IP address that always points to the local machine, so any packets sent to the loopback address are immediately looped back to the same machine.

Question 124: **Skipped**

Which of the following best describes a Memorandum of Understanding (MOU)?

- **A document that outlines the terms of an employment contract**
- **A document that outlines the terms of a partnership or collaboration between two parties**
- **(Correct)**
- **A legally binding agreement between two parties**
- **A document that outlines the terms of a non-disclosure agreement**

Explanation

A Memorandum of Understanding (MOU) is a non-binding document that outlines the terms of a partnership or collaboration between two or more parties when a disaster hits.

Question 125: **Skipped**

Which cloud service model is most commonly associated with the "pay-as-you-go" pricing model?

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**
- **(Correct)**
- **All options**

Explanation

Infrastructure as a Service (IaaS) is often associated with the "pay-as-you-go" pricing model, where users only pay for the computing resources they use on a per-hour or per-minute basis. SaaS and PaaS may also offer this pricing model, but it is less common.

Question 126: **Skipped**

What is a community cloud, and what are some use cases for it?

- **A community cloud is a cloud computing model where infrastructure is shared by a specific group of organizations**
- **(Correct)**
- **Community clouds are less reliable than public clouds**
- **Use cases for community clouds include collaborations between government agencies, research institutions, and healthcare organizations**
- **Community clouds are only used by small businesses**

Explanation

A community cloud is a cloud computing model where infrastructure is shared by a specific group of organizations. Use cases for community clouds include collaborations between government agencies, research institutions, and healthcare organizations.

Question 127: **Skipped**

Which of the following is an example of a passive attack?

- **Sending a phishing email to trick a user into revealing their login credentials**
- **Installing malware on a target computer to steal sensitive information**
- **Flooding a website with requests to make it unavailable to users**
- **Sniffing network traffic to capture unencrypted data**
- **(Correct)**

Explanation

Passive attacks involve monitoring or eavesdropping on data without making any changes to it. In this case, sniffing network traffic to capture unencrypted data is an example of a passive attack. By contrast, installing malware on a target computer, flooding a website, and sending a phishing email are all examples of active attacks that seek to modify or disrupt data in some way.

Question 128: **Skipped**

What are some benefits of working with a managed service provider (MSP)?

- **All options**
- **(Correct)**
- **Access to specialized IT expertise and resources**
- **Lower costs and increased efficiency**

- **Improved security and compliance**

Explanation

Working with an MSP can provide a range of benefits, including access to specialized IT expertise and resources, lower costs and increased efficiency, and improved security and compliance. MSPs can offer a variety of services, including IT consulting, network and infrastructure management, security management, and support services. By working with an MSP, organizations can focus on their core business while leaving IT functions to the experts.

Question 129: **Skipped**

Which of the following is a disadvantage of hybrid data centers compared to cloud data centers?

- **Limited scalability**
- **(Correct)**
- **Higher latency**
- **Less flexibility**
- **Lower availability**

Explanation

While hybrid data centers offer better security and control over data, they are generally less scalable than cloud data centers. This is because the on-premises infrastructure can limit the amount of resources that can be allocated to a workload. Higher latency and lower availability can also

be potential disadvantages of hybrid data centers, but they are not as directly related to the hybrid model as limited scalability.

Question 130: **Skipped**

What is the main difference between a private cloud and a public cloud?

- **A private cloud is more expensive than a public cloud**
- **A public cloud is less secure than a private cloud**
- **A public cloud is hosted by a third-party provider, while a private cloud is dedicated to a single organization**
- **(Correct)**
- **A private cloud is only accessible from a single location**

Explanation

A public cloud is hosted by a third-party provider, while a private cloud is dedicated to a single organization. Private clouds are typically more expensive than public clouds due to the additional infrastructure and resources required to maintain them.

Question 131: **Skipped**

Which of the following is an example of a phishing attack?

- **Sending an email that contains a fake job offer, asking the recipient to pay a fee to apply.**

- **Sending an email containing malware that infects the recipient's device when they open an attachment.**
- **Sending an email that appears to be from a legitimate financial institution, asking the recipient to click on a link and enter their login credentials.**
- **(Correct)**
- **Sending an email that appears to be from a friend or colleague, asking the recipient to donate to a charity.**

Explanation

Phishing attacks involve using social engineering techniques to trick victims into divulging sensitive information, such as login credentials or financial information. Sending an email containing malware is an example of a malware attack, while sending fake job offers or donation requests are examples of scams.

Question 132: **Skipped**

Which of the following is an example of a Man-in-the-Middle (MITM) attack?

- **A hacker sends an email pretending to be a legitimate company to steal login credentials**
- **A hacker uses a fake website to steal personal information**
- **A hacker intercepts communication between two parties to steal data**
- **(Correct)**

- **A hacker uses malware to control a victim's computer**

Explanation

In a MITM attack, the attacker intercepts the communication between two parties, often by positioning themselves between the two parties, and can then steal sensitive information such as login credentials or financial information.

Question 133: **Skipped**

Which layer of the OSI model is typically associated with the operation of firewalls?

- **Transport layer.**
- **Network layer.**
- **(Correct)**
- **Application layer.**
- **Physical layer.**

Explanation

Firewalls are typically associated with the network layer of the OSI model, as this is the layer at which network traffic is routed and packets are addressed based on their IP addresses. Firewalls operate by filtering traffic based on rules that are defined at the network layer.

Question 134: **Skipped**

How can a network or server protect against Fragment (Teardrop) attacks?

- **By using intrusion detection systems to monitor network traffic for signs of an attack**
- **By regularly updating the operating system and software with the latest security patches**
- **(Correct)**
- **By using firewalls to block incoming traffic from known malicious sources**
- **By installing antivirus software on all devices**

Explanation

To protect against Fragment (Teardrop) attacks, a network or server can regularly update the operating system and software with the latest security patches. This helps to ensure that any known vulnerabilities that can be exploited by the attack are patched and secure. Additionally, network and server administrators can implement measures such as rate limiting to limit the number of fragmented packets that can be sent to a system, as well as filtering rules to block traffic that is known to contain malformed packets.

Question 135: **Skipped**

A company has implemented multiple layers of security controls, but an attacker was still able to compromise their network. Which of the following is an example of an administrative control that could have been used to prevent this?

- **Restricting access to sensitive information**
- **Implementing security policies and procedures**
- **(Correct)**
- **Implementing strong encryption for sensitive data**
- **Conducting vulnerability assessments and penetration testing**

Explanation

Security policies and procedures are administrative controls that can be used as part of defense in depth to ensure that security controls are in place and are being followed.

Question 136: **Skipped**

What is the function of the Transport layer in the OSI model?

- **To provide a way to manage network routing.**
- **To provide error checking and flow control between the source and destination hosts.**
- **(Correct)**
- **To provide a way to format data for transmission over the network.**
- **To define the rules for connecting to a network.**

Explanation

The function of the Transport layer in the OSI model is to provide error checking and flow control between the source and destination hosts.

Question 137: **Skipped**

How many bits are used for the address in IPv6?

- **32 bits**
- **64 bits**
- **16 bits**
- **128 bits**
- **(Correct)**

Explanation

IPv6 uses 128 bits for its address, which allows for approximately 3.4 x 10^38 unique addresses. This larger address space was introduced to address the growing number of devices and the limitations of IPv4 that uses 32 bits only for its address.

Question 138: **Skipped**

How can nmap/zenmap be used for vulnerability scanning?

- **By identifying hosts and services on a network.**
- **By testing the strength of user passwords on a network.**
- **By scanning for open ports on network devices.**
- **By identifying potential vulnerabilities based on version information of software running on network devices.**
- **(Correct)**

Explanation

Nmap can be used for vulnerability scanning by identifying potential vulnerabilities based on version information of software running on network devices. For example, if nmap detects a specific version of a software that is known to have a vulnerability, security professionals can use this information to assess the potential risk to the network and take appropriate action.

Question 139: **Skipped**

Which of the following is an example of a NAC enforcement mechanism?

- **VLAN tagging**
- **Network traffic analysis**
- **Firewall rules**
- **(Correct)**
- **Intrusion detection systems**

Explanation

Firewall rules are an example of a NAC enforcement mechanism that can be used to restrict access to the network based on the identity and compliance status of the device attempting to access it.

Question 140: **Skipped**

What is the main advantage of using a Platform as a Service (PaaS) cloud service model?

- **Reduced operational overhead and maintenance costs**

- **Improved application development and deployment speed**
- **(Correct)**
- **Access to scalable and flexible computing resources**
- **Improved security and compliance**

Explanation

Platform as a Service (PaaS) is a cloud service model that provides developers with a platform for building, testing, and deploying applications without having to worry about the underlying infrastructure. This can help improve the speed and agility of application development and deployment. While PaaS can also provide benefits such as improved scalability and reduced operational overhead, the primary advantage is its ability to accelerate the software development lifecycle.

Question 141: **Skipped**

Which of the following is a benefit of a hybrid cloud data center?

- **Lower latency**
- **Lower cost**
- **Reduced complexity**
- **Greater control over data**
- **(Correct)**

Explanation

A hybrid cloud data center combines public cloud resources with on-premises infrastructure, allowing for greater control over data. This is because sensitive data can be stored and processed on-premises, while less sensitive data can be processed in the public cloud. Hybrid cloud data centers can also offer lower latency compared to public cloud data centers, but they are generally more complex and can be more expensive to operate.

Question 142: **Skipped**

Which cloud service model provides users with access to a complete software application that is hosted and managed by a third-party provider?

- **Software as a Service (SaaS)**
- **(Correct)**
- **Infrastructure as a Service (IaaS)**
- **Platform as a Service (PaaS)**
- **None.**

Explanation

Software as a Service (SaaS) is a cloud service model that provides users with access to a complete software application that is hosted and managed by a third-party provider. This can include applications for email, collaboration, customer relationship management (CRM), and more. IaaS and PaaS provide different levels of

infrastructure and platform services, but they do not include pre-built software applications.

Question 143: **Skipped**

Which of the following is a characteristic of cloud data centers?

- **Customized hardware configurations**
- **Pay-per-use pricing models**
- **(Correct)**
- **High upfront capital expenditures**
- **Location-dependent resource availability**

Explanation

One of the key characteristics of cloud data centers is their pay-per-use pricing model, which allows users to pay only for the resources they actually use. This is in contrast to on-premises infrastructure, which often requires high upfront capital expenditures. Cloud providers also typically offer standardized hardware configurations rather than customized options, and resource availability is not location-dependent in the same way it is for on-premises infrastructure.

Question 144: **Skipped**

Which of the following is NOT a best practice for network segmentation?

- **Monitoring network activity to detect anomalies or suspicious behavior**

- **Using VLANs to separate different departments or functions**
- **Implementing access control policies to restrict network access**
- **Allowing unrestricted communication between all subnetworks**
- **(Correct)**

Explanation

The purpose of network segmentation is to limit communication between different subnetworks, so allowing unrestricted communication would defeat this purpose. It is best to implement access control policies to restrict network access and monitor network activity to detect anomalies or suspicious behavior.

Question 145: **Skipped**

Which of the following is not an example of a technical control that can be used as part of defense in depth?

- **Intrusion detection systems**
- **Security awareness training for employees**
- **(Correct)**
- **Antivirus software**
- **Firewall rules**

Explanation

Security awareness training is an administrative control that can be used as part of defense in depth to ensure that

employees understand the importance of security and are able to identify and report potential security incidents.

Question 146: **Skipped**

What is the primary advantage of a Cloud Next-Generation Firewall that includes a micro-segmentation component?

- **It can provide granular control over access to cloud resources and data.**
- **(Correct)**
- **It can block known malware and viruses from entering the network.**
- **It can detect and block zero-day threats that have not yet been identified.**
- **It can prioritize and allocate bandwidth to critical applications.**

Explanation

A micro-segmentation component of a Cloud Next-Generation Firewall can help organizations enforce security policies at a granular level, enabling them to control access to cloud resources and data based on factors such as user identity, device type, and application type.

Question 147: **Skipped**

What is the primary benefit of microsegmentation in a cybersecurity strategy?

- **Increased network performance**
- **Enhanced security by isolating individual workloads or applications**
- **(Correct)**
- **Better compliance with regulatory requirements**
- **Improved network visibility**

Explanation

Microsegmentation allows for the isolation of individual workloads or applications, each with their own set of security controls, which helps to prevent lateral movement within the network and contain any breaches. This enhances the security posture of the organization and reduces the risk of data breaches.

Question 148: **Skipped**

An organization discovers that several of its critical servers have been compromised by an Advanced persistent threat (APT). What is the best course of action for the organization to take?

- **Notify law enforcement and wait for their guidance on how to proceed.**
- **Begin monitoring the servers for further activity while developing a response plan.**
- **(Correct)**
- **Immediately disconnect the servers from the network and wipe them clean.**

- **Attempt to identify the source of the attack and block it.**

Explanation

When dealing with an Advanced persistent threat (APT), it is important to take a measured and strategic approach. Simply wiping the servers clean or blocking the source of the attack may not be effective if the attacker has already gained persistent access to the network. Notification of law enforcement is important, but organizations should also take steps to actively monitor the affected servers and develop a response plan.

Question 149: **Skipped**

Which of the following is a common example of an on-path attack that targets Domain Name System (DNS) traffic?

- **Cache poisoning**
- **(Correct)**
- **SQL injection**
- **Ransomware**
- **Packet sniffing**

Explanation

Cache poisoning is a type of on-path attack that involves modifying the DNS cache of a victim's device or a DNS server to redirect DNS requests to a malicious domain. This can be used to intercept sensitive information, such

as login credentials, or to redirect users to fake websites. Packet sniffing is a passive form of on-path attack that involves eavesdropping on network traffic, while SQL injection and ransomware are not specific to on-path attacks.

Question 150: **Skipped**

What is the difference between nmap and zenmap?

- **Zenmap is a graphical user interface for nmap.**
- **(Correct)**
- **Nmap is a passive network scanning tool, while Zenmap is an active network scanning tool.**
- **Nmap is a Windows-based network scanning tool, while Zenmap is a Linux-based network scanning tool.**
- **Zenmap is a command-line interface for nmap.**

Explanation

Zenmap is a graphical user interface (GUI) that runs on top of nmap. It provides a more user-friendly interface for nmap and allows security professionals to visualize the results of network scans. Nmap is a command-line tool that is used to scan networks and identify hosts, services, and open ports.

Question 151: **Skipped**

What is the main difference between signature-based detection and anomaly-based detection in IDS?

- **Anomaly-based detection relies on pre-configured rules, while signature-based detection is based on machine learning.**
- **Signature-based detection looks for known patterns of malicious behavior, while anomaly-based detection looks for abnormal behavior patterns.**
- **(Correct)**
- **Signature-based detection is more accurate than anomaly-based detection.**
- **Signature-based detection is faster than anomaly-based detection.**

Explanation

Signature-based detection relies on pre-configured rules that look for known patterns of malicious behavior, while anomaly-based detection looks for abnormal behavior patterns that deviate from what is considered normal activity. While signature-based detection can be more accurate in identifying known threats, anomaly-based detection can help detect unknown threats that may not have a pre-configured signature.

Question 152: **Skipped**

What is one benefit of IPv6 autoconfiguration?

- **It provides better security than manual configuration.**
- **It reduces the need for DHCP servers.**
- **(Correct)**

- **It requires less network bandwidth.**
- **It improves network latency.**

Explanation

IPv6 supports autoconfiguration, which allows devices to automatically configure their own addresses and other network settings without requiring manual configuration or the use of DHCP servers. This can reduce the need for DHCP servers and simplify network management.

Question 153: **Skipped**

What is a Public IP Address?

- **An IP address that is used by a network router to connect to the internet**
- **An IP address that is assigned by an internet service provider (ISP)**
- **An IP address that is reserved for use in a private network**
- **An IP address that is publicly accessible on the internet**
- **(Correct)**

Explanation

A public IP address is a unique address that is assigned to a device on the internet. It is publicly accessible and can be used to connect to the device from anywhere in the world. Public IP addresses are assigned by an ISP and are used to identify devices on the internet.

Question 154: **Skipped**

Which of the following is an advantage of hybrid data centers compared to cloud data centers?

- **Better security and control over data**
- **(Correct)**
- **Lower latency and higher availability**
- **Greater scalability and cost efficiency**
- **More flexible deployment options**

Explanation

One of the main advantages of hybrid data centers is that they offer greater control and security over data compared to cloud data centers. This is because sensitive data can be stored on-premises, while less sensitive data can be stored in the cloud. Hybrid data centers also allow for more flexibility in deployment options, but they are generally not as scalable or cost-efficient as cloud data centers. Lower latency and higher availability are typically associated with on-premises data centers rather than hybrid data centers.

Question 155: **Skipped**

Which layer of the OSI model is responsible for routing and forwarding data packets between different networks?

- **Network layer**
- **(Correct)**
- **Transport layer**

- **Data Link layer**
- **Application layer**

Explanation

The Network layer of the OSI model is responsible for routing and forwarding data packets between different networks.

Question 156: **Skipped**

Which of the following is a limitation of signature-based detection in an Intrusion Detection Systems (IDS)?

- **It can detect zero-day attacks.**
- **It cannot detect unknown attacks.**
- **(Correct)**
- **It cannot detect attacks that originate from outside the network.**
- **It cannot detect known attacks.**

Explanation

Signature-based detection relies on pre-configured rules that look for specific patterns of malicious behavior or known attacks. As a result, it cannot detect unknown attacks or zero-day attacks that do not have a known signature or pattern of malicious behavior. While signature-based detection can be effective for detecting known threats, it is important to use other detection methods such as behavioral-based detection to help detect unknown threats.

Question 157: **Skipped**

What is the main advantage of using a PaaS cloud service model?

- **Reduced operational overhead and maintenance costs**
- **Improved security and compliance**
- **Improved application development and deployment speed**
- **(Correct)**
- **Access to scalable and flexible computing resources**

Explanation

Platform as a Service (PaaS) is a cloud service model that provides developers with a platform for building, testing, and deploying applications without having to worry about the underlying infrastructure. This can help improve the speed and agility of application development and deployment. While PaaS can also provide benefits such as improved scalability and reduced operational overhead, the primary advantage is its ability to accelerate the software development lifecycle.

Question 158: **Skipped**

An employee at an organization receives a suspicious email with an attachment and clicks on it. The attachment contains malware that is part of an APT. What is the best way for the organization to respond to this incident?

- **Immediately disconnect the employee's computer from the network and wipe it clean.**
- **Conduct a thorough investigation to identify the source and purpose of the attack.**
- **Conduct a full network scan to identify any other potential infections.**
- **(Correct)**
- **Notify all employees of the incident and provide additional training on email security.**

Explanation

Advanced persistent threat (APTs) often involve multiple stages of infiltration, and attackers may have already gained access to other systems on the network. Disconnecting the employee's computer and wiping it clean may not be enough to fully address the threat. Notification of employees and additional training may be useful in preventing future incidents, but in this case, the organization should focus on identifying and addressing any other potential infections.

Question 159: **Skipped**

Which of the following best describes the three-way-handshake?

- **A method for blocking a connection between two devices on a network**

- **A method for establishing a connection between two devices on a network**
- **(Correct)**
- **A security protocol used to protect sensitive data during transmission**
- **A process for resolving network conflicts between multiple devices**

Explanation

The three-way-handshake is a method used to establish a connection between two devices on a network. It involves a series of three messages between the devices to ensure that both sides are ready and willing to communicate.

Question 160: **Skipped**

Which of the following is an important factor to consider when selecting a generator for the on-premises infrastructure?

- **Color**
- **Noise level**
- **(Correct)**
- **Shape**
- **Texture**

Explanation

Noise level is an important factor to consider when selecting a generator for the on-premises infrastructure, as

generators can be noisy and may impact the working environment.

Question 161: **Skipped**

What is the goal of a Fragment (Teardrop) attack?

- **To compromise the security of a network or server**
- **To overload the victim's system with malformed packets**
- **(Correct)**
- **To steal sensitive information from the victim's system**
- **To spread malware or ransomware to the victim's system**

Explanation

The goal of a Fragment (Teardrop) attack is to overload the victim's system with malformed packets, causing the system to crash or become unresponsive. The attack relies on sending a large number of fragmented packets to the victim's system, which the system is unable to reassemble due to the malformed nature of the packets.

Question 162: **Skipped**

Which of the following types of antivirus scans checks only files that have been modified since the last scan?

- **Full scan.**
- **Quick scan.**
- **Custom scan.**

- **Incremental scan.**
- **(Correct)**

Explanation

An incremental scan checks only files that have been modified since the last scan, which can help reduce scan time and system resource usage. Full scans check all files on the system, while quick scans check only key system areas. Custom scans allow the user to select specific files or folders to scan.

Question 163: **Skipped**

Which of the following protocols uses port 23?

- **SSH**
- **HTTP**
- **FTP**
- **Telnet**
- **(Correct)**

Explanation

Telnet uses port 23 for communication between the client and server. It is an unencrypted protocol that allows users to remotely access a device's command line interface. Please note that SSH (Secure Shell) that uses port 22 is considered to be more secure for remote access because it encrypts data transmitted between the client and server

Question 164: **Skipped**

Which of the following is a key benefit of using a UPS (Uninterruptible Power Supply) in the on-premises infrastructure?

- **It provides backup power during a power outage**
- **(Correct)**
- **It provides backup storage for the data**
- **It provides physical security for the data center**
- **It provides cooling for the servers**

Explanation

A UPS (Uninterruptible Power Supply) provides battery backup power in the event of a power outage, which helps prevent data loss or server damage due to sudden power loss.

Question 165: **Skipped**

What is the primary function of an intrusion prevention system (IPS) that is integrated with a Next-Generation Firewall?

- **To prevent unauthorized access to the network.**
- **To monitor network traffic and identify suspicious behavior.**
- **To detect and block known and unknown threats in real-time.**
- **(Correct)**
- **To block known malware and viruses from entering the network.**

Explanation

An IPS that is integrated with a Next-Generation Firewall can detect and block both known and unknown threats in real-time. This is accomplished through a combination of signature-based detection, behavioral analysis, and machine learning.

Question 166: **Skipped**

What is a hybrid cloud, and what are some benefits of using one?

- **Benefits of using a hybrid cloud include the ability to balance cost and control, and the flexibility to move workloads between environments**
- **Hybrid clouds are less secure than public clouds**
- **Hybrid clouds are typically used only by large enterprises**
- **A hybrid cloud is a cloud computing model that combines public and private clouds**
- **(Correct)**

Explanation

A hybrid cloud is a cloud computing model that combines public and private clouds. Benefits of using a hybrid cloud include the ability to balance cost and control, and the flexibility to move workloads between environments.

Question 167: **Skipped**

Which cloud service model provides the most flexibility and control over the underlying infrastructure?

- **All options**
- **Infrastructure as a Service (IaaS)**
- **(Correct)**
- **Platform as a Service (PaaS)**
- **Software as a Service (SaaS)**

Explanation

Infrastructure as a Service (IaaS) provides the most flexibility and control over the underlying infrastructure, as users have direct access to virtualized computing resources such as servers, storage, and networking. SaaS and PaaS provide higher-level abstractions that can make it easier to develop and deploy applications, but they do not offer the same level of control over the underlying infrastructure.

Question 168: **Skipped**

Which of the following is the primary difference between Host-based Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS)?

- **HIDS is designed to detect intrusions at the network level, while NIDS is designed to detect intrusions at the host level.**

- **HIDS is installed on individual devices, while NIDS is installed on network devices such as routers and switches.**
- **(Correct)**
- **HIDS is passive and only alerts when an intrusion is detected, while NIDS is active and can take action to prevent an intrusion.**
- **HIDS relies on signature-based detection, while NIDS relies on anomaly-based detection.**

Explanation

Host-based Intrusion Detection Systems (HIDS) is installed on individual devices such as servers, workstations or laptops to monitor system events and detect unauthorized access attempts, while Network Intrusion Detection Systems (NIDS) is installed on network devices like routers or switches to monitor network traffic and detect anomalies in traffic that may indicate an intrusion.

Question 169: **Skipped**

Which of the following is an example of an active attack?

- **Using software to capture encrypted data and crack the encryption key**
- **Running a script that repeatedly tries different login credentials**
- **(Correct)**

- **Sending spam emails to deceive users into revealing sensitive information**
- **Monitoring network traffic to identify patterns of user behavior**

Explanation

An active attack involves a deliberate attempt to modify or disrupt data. In this case, running a script that repeatedly tries different login credentials is an example of an active attack aimed at gaining unauthorized access to a system. The other options describe different types of passive attacks. Monitoring network traffic, sending spam emails, and capturing encrypted data are all forms of passive attack aimed at eavesdropping or observing data without making changes. While these attacks can still be dangerous, they are typically less immediate threats than active attacks since they don't result in direct modifications to data.

Question 170: **Skipped**

Which of the following is a defense strategy against zero-day attacks?

- **Implementing perimeter-based network security controls.**
- **Using strong passwords and multifactor authentication.**
- **Disabling all unnecessary services and ports.**

- **Regularly updating software and systems.**
- **(Correct)**

Explanation

Regularly updating software and systems can help mitigate the risk of zero-day attacks by ensuring that known vulnerabilities are patched and new security features are implemented. While using strong passwords, disabling unnecessary services and ports, and implementing perimeter-based security controls can also help enhance security, they do not necessarily protect against zero-day attacks.

Question 171: **Skipped**

Which of the following is NOT typically included in an SLA?

- **The level of service availability guaranteed by the provider.**
- **The response time for support requests.**
- **The procedures for reporting and resolving service issues.**
- **The price of the service.**
- **(Correct)**

Explanation

While the price of the service may be discussed and negotiated as part of the SLA negotiation process, it is not typically included in the SLA itself, which focuses on the

quality and scope of the service, as well as the responsibilities and expectations of both parties.

Question 172: **Skipped**

A media company needs to store large amounts of video and image data and make it accessible to its global workforce. The company has no dedicated IT staff and needs a cost-effective solution. Which cloud model would be the best fit for this scenario?

- **Community cloud**
- **Hybrid cloud**
- **Private cloud**
- **Public cloud**
- **(Correct)**

Explanation

The best cloud model for this scenario would be a public cloud, as it is cost-effective and provides easy access to cloud resources without requiring the company to manage its own IT infrastructure. Public clouds also have global availability, making them ideal for a globally distributed workforce.

Question 173: **Skipped**

What is the difference between a packet filtering firewall and a stateful firewall?

- **Packet filtering firewalls do not maintain state information, while stateful firewalls maintain state information.**
- **(Correct)**
- **Packet filtering firewalls filter traffic based on application layer protocols, while stateful firewalls filter traffic based on network layer protocols.**
- **Packet filtering firewalls filter traffic based on network layer protocols, while stateful firewalls filter traffic based on application layer protocols.**
- **Packet filtering firewalls use deep packet inspection to filter traffic, while stateful firewalls use basic packet filtering.**

Explanation

Packet filtering firewalls filter traffic based on rules that are applied to individual packets, without maintaining state information about the connection. Stateful firewalls, on the other hand, maintain state information about connections and can use this information to filter traffic more effectively. By maintaining state information, stateful firewalls can also provide additional security features, such as intrusion prevention and application layer filtering.

Question 174: **Skipped**

How can rootkits be detected?

- **Through a network intrusion detection system**

- **Rootkits are designed to evade detection**
- **(Correct)**
- **Through traditional antivirus software**
- **Through a firewall**

Explanation

Rootkits are designed to evade detection by traditional antivirus software and other security tools, which makes them difficult to detect and remove.

Question 175: **Skipped**

What is the primary advantage of a Next-Generation Firewall that includes a sandboxing component?

- **It can detect and block zero-day threats that have not yet been identified.**
- **(Correct)**
- **It can prioritize and allocate bandwidth to critical applications.**
- **It can provide visibility into application usage and performance.**
- **It can block known malware and viruses from entering the network.**

Explanation

A sandboxing component of a Next-Generation Firewall can analyze suspicious files and URLs in a safe, isolated environment to determine if they are malicious. This

allows the firewall to detect and block previously unknown threats that may evade traditional detection methods.

Question 176: **Skipped**

What is the primary benefit of a Cloud Next-Generation Firewall?

- **It provides better protection against spam and other unwanted traffic.**
- **It is faster and more scalable than traditional firewalls.**
- **It is simpler and easier to manage than traditional firewalls.**
- **It provides greater visibility and control over cloud-based applications and services.**
- **(Correct)**

Explanation

A Cloud Next-Generation Firewall provides advanced security capabilities for cloud-based applications and services, enabling organizations to monitor and control access to cloud resources and data.

Question 177: **Skipped**

A company recently implemented a zero trust security model and an employee is attempting to access a sensitive database from their personal laptop at home. What action should the company take?

- **Require the employee to come into the office to access the database**
- **Allow access as the employee is authorized to access the database**
- **Deny access as the employee is not accessing from a company device**
- **Request the employee to use a VPN to access the database**
- **(Correct)**

Explanation

Zero trust security model assumes that no user or device can be trusted automatically, regardless of their location or authorization level. The employee's personal laptop is not a trusted device, and allowing access can lead to potential security risks. Therefore, the best practice is to request the employee to use a VPN, which can establish a secure connection between the laptop and the company's network, and ensure the employee is authenticated before accessing the database.

Question 178: **Skipped**

Which of the following is NOT a common characteristic of spam emails?

- **They often contain unsolicited advertisements or promotions.**

- **They are always automatically identified and filtered out by email spam filters.**
- **(Correct)**
- **They often use deceptive or misleading subject lines to entice recipients to open them.**
- **They are usually sent to a large number of recipients at once.**

Explanation

While spam filters are designed to identify and filter out spam emails, they are not 100% effective and some spam emails may still get through. Spam emails often use deceptive subject lines, are sent to a large number of recipients, and contain unsolicited advertisements or promotions.

Question 179: **Skipped**

Which layer of the OSI model do circuit-level firewalls operate at?

- **Application layer.**
- **Transport layer.**
- **(Correct)**
- **Data link layer.**
- **Physical layer.**

Explanation

Circuit-level firewalls operate at the transport layer of the OSI model and can inspect traffic at this layer. They do not

inspect traffic at the application layer and are less effective at filtering traffic based on application-level protocols. Instead, they focus on filtering traffic based on transport-layer protocols, such as TCP and UDP.

Question 180: **Skipped**

What does the term "Wi-Fi" stand for?

- **Wireless Fiber**
- **Wireless Fidelity**
- **(Correct)**
- **Wireless Fire**
- **Wireless Framework**

Explanation

The term "Wi-Fi" was originally created as a play on the term "Hi-Fi" (High Fidelity) used in the music industry, and stands for "Wireless Fidelity."

Question 181: **Skipped**

Which of the following is a common example of a side-channel attack?

- **Timing attack**
- **(Correct)**
- **Phishing attack**
- **Distributed Denial of Service (DDoS) attack**
- **Brute force attack**

Explanation

A Timing Attack is a type of side-channel attack that involves measuring the time it takes for a system to perform a specific operation, such as comparing passwords or decrypting data. By measuring these times, an attacker can infer information about the system's encryption key or other sensitive data.

Question 182: **Skipped**

What is the purpose of nmap?

- **To test the strength of passwords on user accounts.**
- **To monitor network traffic and analyze bandwidth usage.**
- **o detect vulnerabilities on web servers.**
- **To scan networks and identify hosts, services, and open ports.**
- **(Correct)**

Explanation

Nmap is a popular network scanning tool that is used to scan networks and identify hosts, services, and open ports. It is often used by security professionals to identify potential vulnerabilities and to map out network architecture.

Question 183: **Skipped**

Which of the following is an example of a physical security control used to protect employees in a building?

- **CCTV surveillance**

- **Biometric authentication**
- **Emergency evacuation plan**
- **(Correct)**
- **Encryption**

Explanation

An emergency evacuation plan is an example of a physical security control used to protect employees in a building by ensuring their safe and efficient evacuation in the event of an emergency.

Question 184: **Skipped**

Which of the following is a potential security risk associated with Virtual Local Area Networks (VLANs)?

- **Unauthorized access to confidential data**
- **(Correct)**
- **Increased network latency**
- **Lack of visibility into network traffic**
- **Interference between different logical networks**

Explanation

Virtual Local Area Networks (VLANs) can be a potential security risk if they are not properly configured, as attackers may be able to use them to gain access to confidential data that is not intended for their use. This risk can be mitigated through proper configuration and monitoring of the VLANs.

Question 185: **Skipped**

Which of the following is NOT an effective countermeasure against side-channel attacks?

- **Implementing secure boot protocols**
- **Implementing hardware-based encryption**
- **Disabling all logging and debugging functionality**
- **(Correct)**
- **Using randomized delay techniques**

Explanation

Logging and debugging functionality can be helpful in identifying and mitigating side-channel attacks, and disabling these functions can make it more difficult to detect and respond to attacks. Implementing hardware-based encryption, using randomized delay techniques, and implementing secure boot protocols are all effective countermeasures against side-channel attacks.

Question 186: **Skipped**

What is the difference between phishing and spear phishing?

- **Phishing targets a large number of victims, while spear phishing targets only a small group or individual.**
- **(Correct)**

- **Phishing requires the use of advanced hacking techniques, while spear phishing relies on simple social engineering tactics.**
- **Phishing involves impersonating a well-known company or institution, while spear phishing involves impersonating a specific individual or organization.**
- **Phishing is always carried out through email, while spear phishing can involve other communication methods, such as social media or instant messaging.**

Explanation

Phishing attacks involve targeting a large number of victims with a generic message, while spear phishing attacks are targeted at a specific individual or group and often involve personalized messages or information. Both types of attacks can involve impersonating well-known companies or institutions and can be carried out through various communication methods.

Question 187: **Skipped**

What is the primary benefit of using a Software as a Service (SaaS) cloud service model?

- **Reduced operational overhead and maintenance costs**
- **(Correct)**
- **Access to scalable and flexible computing resources**

- **Improved application development and deployment speed**
- **Reduced software licensing costs**

Explanation

Software as a Service (SaaS) is a cloud service model that provides users with access to a complete software application that is hosted and managed by a third-party provider. This can help reduce operational overhead and maintenance costs for the user, as they do not have to manage the underlying infrastructure or perform software upgrades themselves. While SaaS can also provide benefits such as improved scalability and reduced licensing costs, the primary advantage is its ability to simplify software management.

Question 188: **Skipped**

What is a LAN?

- **A network that connects devices using cellular data**
- **A Local Area Network that connects devices in a small geographical area**
- **(Correct)**
- **A network that connects devices using satellite technology**
- **A Wide Area Network that connects devices over a large geographical area**

Explanation

A Local Area Network (LAN) is a network that connects devices in a local area such as a home, office, or building. It is typically used for sharing resources such as printers, files, and internet access.

Question 189: **Skipped**

Which of the following is a key benefit of using motion detection technology with CCTV (Closed Circuit Television) cameras in the on-premises infrastructure?

- **It reduces the number of cameras needed**
- **It increases storage capacity**
- **It reduces the cost of the CCTV system**
- **It reduces false alarms**
- **(Correct)**

Explanation

Motion detection technology can help reduce false alarms in the CCTV (Closed Circuit Television) system, which can improve the efficiency and effectiveness of the system.

Question 190: **Skipped**

What type of firewall is typically used to protect an entire network?

- **Network layer firewall.**
- **(Correct)**
- **Packet filtering firewall.**
- **Application layer firewall.**
- **Stateful firewall.**

Explanation

Network layer firewalls are designed to protect an entire network by filtering traffic at the network layer (Layer 3) of the OSI model. This allows the firewall to filter traffic based on IP addresses and other network-level information. By filtering network traffic at the network layer, these firewalls can provide a high level of protection for networks.

Question 191: **Skipped**

Which of the following best describes an SLA?

- **A binding agreement between a service provider and a client that outlines the quantity of services provided.**
- **A non-binding agreement between a service provider and a client that outlines the quality and scope of the services provided.**
- **An informal agreement between a service provider and a client that outlines the quality and scope of the services provided.**
- **A legal contract between a service provider and a client that outlines the quality and scope of the services provided.**
- **(Correct)**

Explanation

An SLA (Service Level Agreement) is a formal, legally-binding contract between a service provider and a client that outlines the quality and scope of the services provided, as well as the responsibilities and expectations of both parties.

Question 192: **Skipped**

What is the primary disadvantage of a packet filtering firewall?

- **They are unable to block traffic based on IP addresses.**
- **They are unable to filter traffic based on application layer protocols.**
- **(Correct)**
- **They are unable to maintain state information about connections.**
- **They are vulnerable to attacks that exploit network-layer protocols.**

Explanation

Packet filtering firewalls are designed to filter traffic based on network layer information, such as IP addresses and port numbers. This makes them less effective at filtering traffic that uses application layer protocols, such as HTTP or FTP. As a result, packet filtering firewalls are often used in combination with other security technologies, such as

intrusion detection systems (IDS) or application layer firewalls.

Question 193: **Skipped**

Which cloud service model provides users with access to virtualized computing resources over the internet?

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**
- **(Correct)**
- **All options**

Explanation

Infrastructure as a Service (IaaS) is a cloud service model that provides users with access to virtualized computing resources over the internet, such as servers, storage, and networking. SaaS and PaaS are different cloud service models that focus on delivering software applications and development platforms, respectively.

Question 194: **Skipped**

Which of the following fire suppression systems uses water as the extinguishing agent?

- **Wet chemical**
- **Sprinkler**
- **(Correct)**
- **Halon**
- **Dry chemical**

Explanation

Sprinkler systems use water as the extinguishing agent to suppress fires. The water is discharged when a heat-sensitive element in the system is activated.

Question 195: **Skipped**

What is the difference between the OSI model and the TCP/IP model?

- **The OSI model is a theoretical model, while the TCP/IP model is a practical implementation.**
- **The TCP/IP model has more layers than the OSI model.**
- **The OSI model has more layers than the TCP/IP model.**
- **(Correct)**
- **The OSI model and the TCP/IP model are essentially the same.**

Explanation

The OSI model has seven layers, while the TCP/IP model has four layers. TCP/IP Model is a communication protocols suite using which network devices can be connected to the Internet. On the other hand, the OSI Model is a conceptual framework using which the functioning of a network can be described.

Question 196: **Skipped**

What is the purpose of the OSI model?

- **To provide a way to manage network security.**
- **To provide a standard for the development of network protocols.**
- **(Correct)**
- **To provide a way to classify different types of networks.**
- **To provide a way for different types of networks to communicate with each other.**

Explanation

The purpose of the OSI model is to provide a standard for the development of network protocols. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.

Question 197: **Skipped**

Which of the following is NOT a benefit of network segmentation?

- **Improved network security**
- **Better compliance with regulatory requirements**

- **Easier network management**
- **(Correct)**
- **Increased network performance**

Explanation

Network segmentation can make network management more complex, as there are more subnetworks to manage. However, the benefits of improved security, compliance, and performance usually outweigh this added complexity.

Question 198: **Skipped**

Which protocol is used for real-time communication between two or more clients?

- **HTTP**
- **SMTP**
- **SIP**
- **(Correct)**
- **FTP**

Explanation

SIP (Session Initiation Protocol) is the protocol used for real-time communication between two or more clients. It is commonly used for voice and video calls over the internet.

Question 199: **Skipped**

Which protocol operates at the Network layer and provides routing of IP packets?

- **ICMP**

- **(Correct)**
- **HTTP**
- **FTP**
- **SMTP**

Explanation

ICMP (Internet Control Message Protocol) operates at the Network layer and provides routing of IP packets. ICMP is used by routers to communicate with each other and to diagnose network problems. It is responsible for sending error messages and control messages, such as ping and traceroute, to other devices on the network.

Question 200: **Skipped**

Which of the following protocols is used for secure email communication?

- **POP3**
- **(Correct)**
- **SMTP**
- **HTTPS**
- **IMAP**

Explanation

POP3 (Post Office Protocol version 3) is used for receiving email messages from a server. When used with SSL/TLS encryption, it can provide secure email communication. SMTP (Simple Mail Transfer Protocol) is used for sending

email messages, and can also be used with SSL/TLS encryption.

Question 201: **Skipped**

What is an availability zone in cloud computing, and can it include multiple data centers?

- **An availability zone is a single data center within a region, and it cannot include multiple data centers.**
- **An availability zone is a set of tools for managing cloud resources, and it does not involve physical data centers.**
- **An availability zone is a group of data centers within a region that share resources and provide high availability.**
- **An availability zone is a single data center within a region, but it can include multiple data centers for additional redundancy and fault tolerance.**
- **(Correct)**

Explanation

While the primary definition of an availability zone is a single, physically isolated data center within a region, some cloud providers may choose to have multiple data centers within an availability zone to further improve fault tolerance and high availability. Regardless of the specific implementation, the key concept is that an availability

zone is designed to provide additional resilience and minimize the impact of potential outages or disasters.

Question 202: **Skipped**

Which of the following statements accurately describes the difference between hybrid data centers and cloud data centers?

- **Hybrid data centers typically have higher availability and lower latency than cloud data centers.**
- **Cloud data centers are designed to support a specific application or workload, while hybrid data centers are more flexible in their capabilities.**
- **Cloud data centers offer better scalability and cost efficiency than hybrid data centers.**
- **Hybrid data centers use a mix of on-premises and cloud infrastructure, while cloud data centers rely entirely on remote servers.**
- **(Correct)**

Explanation

The key difference between hybrid data centers and cloud data centers is the infrastructure they rely on. Hybrid data centers use a mix of on-premises and cloud infrastructure to support their workloads, while cloud data centers rely entirely on remote servers. The other options in the question are not accurate descriptions of the difference between the two types of data centers.

Question 203: **Skipped**

Which of the following is an effective defense against phishing and spear phishing attacks?

- **Disabling all email attachments and links.**
- **Using a simple and easy-to-guess password for all accounts.**
- **Sharing sensitive information freely and openly with all contacts.**
- **Enabling multi-factor authentication (MFA) for all online accounts.**
- **(Correct)**

Explanation

Multi-factor authentication (MFA) is an effective defense against phishing and spear phishing attacks because it requires an additional layer of authentication beyond just a username and password, such as a one-time code sent to a mobile device. Disabling all email attachments and links is not practical or effective, and using a simple password or sharing sensitive information freely and openly can increase the risk of a successful attack.

Question 204: **Skipped**

Which of the following protocols is faster but less reliable?

- **UDP**
- **(Correct)**

- **HTTP**
- **FTP**
- **TCP**

Explanation

UDP is a faster but less reliable protocol. It does not establish a connection before transmitting data and does not provide error checking or recovery mechanisms. This makes it suitable for applications that require speed over reliability, such as video or audio streaming.

Question 205: **Skipped**

What types of businesses or organizations are most likely to benefit from working with a managed service provider (MSP)?

- **Small businesses with limited IT resources**
- **All options**
- **(Correct)**
- **Large organizations with complex IT needs**
- **Businesses with highly specialized IT requirements**

Explanation

MSPs can provide benefits to a wide range of businesses and organizations, including small businesses with limited IT resources, large organizations with complex IT needs, and businesses with highly specialized IT requirements. By working with an MSP, organizations can access specialized expertise and resources that they may not

have in-house, while also reducing costs and improving efficiency.

Question 206: **Skipped**

Which of the following ports is typically used for secure communication?

- **Port 80**
- **Port 25**
- **Port 443**
- **(Correct)**
- **Port 110**

Explanation

Port 443 is typically used for secure communication using the HTTPS protocol. HTTPS is a combination of HTTP and SSL/TLS encryption, which ensures that data transmitted between the client and server is encrypted and secure.

Question 207: **Skipped**

How does a Cloud Next-Generation Firewall differ from a traditional Next-Generation Firewall?

- **A Cloud Next-Generation Firewall is easier to manage than a traditional Next-Generation Firewall.**
- **A Cloud Next-Generation Firewall provides more advanced security features than a traditional Next-Generation Firewall.**

- **A Cloud Next-Generation Firewall is designed specifically for cloud-based applications and services.**
- **(Correct)**
- **A Cloud Next-Generation Firewall is slower and less scalable than a traditional Next-Generation Firewall.**

Explanation

While both types of firewalls provide advanced security capabilities, a Cloud Next-Generation Firewall is designed specifically to address the unique security challenges associated with cloud-based applications and services.

Question 208: **Skipped**

Which of the following is an example of a segmentation technique for IoT devices?

- **VLAN tagging**
- **(Correct)**
- **MAC address filtering**
- **Password authentication**
- **Intrusion detection systems**

Explanation

VLAN tagging is a common segmentation technique that can be used to separate IoT devices from other network resources. By isolating IoT devices on a separate network segment, security policies can be implemented that are specific to the devices and their functions. Other

segmentation techniques, such as MAC address filtering, can also be effective, but VLAN tagging is a more comprehensive approach.

(Domain 5) - Security Operations - Results

Question 1: **Skipped**
Which of the following best describes the purpose of a data handling policy?

- **To delegate responsibility for data handling to a third-party provider.**
- **To establish guidelines for the proper handling of data.**
- **(Correct)**
- **To prevent any access to data by employees.**
- **To ensure that data is accessible to all employees.**

Explanation
The purpose of a data handling policy is to establish guidelines for the proper handling of data within an organization. This includes guidelines for data access, storage, transmission, and disposal, as well as guidelines for ensuring the confidentiality, integrity, and availability of data. By establishing clear guidelines for data handling,

organizations can reduce the risk of data breaches, ensure compliance with regulations, and protect their reputation.

Question 2: **Skipped**

Which of the following is a key step in the change evaluation and planning process?

- **Assigning a project manager to oversee the change**
- **Identifying potential risks and impacts of the change**
- **(Correct)**
- **Determining the budget for the change**
- **Communicating the change to end-users**

Explanation

A key step in the change evaluation and planning process is to identify potential risks and impacts of the change, including potential downtime, security risks, and impacts on end-users and business operations.

Question 3: **Skipped**

What is a baseline in configuration management?

- **A backup of the system or application configuration**
- **A record of the current state of a system or application**
- **A comparison of the current state of a system or application to a predefined standard**
- **(Correct)**
- **A method of automating software updates and patches**

Explanation

A baseline is a snapshot of the configuration of a system or application at a specific point in time. It is used as a reference point for future comparisons to determine if any changes have been made to the system or application. A baseline can be compared to a predefined standard to identify any deviations from the standard, which can be addressed through change management processes.

Question 4: **Skipped**

What is the purpose of a security information and event management (SIEM) system?

- **To block all incoming network traffic**
- **To collect, correlate, and analyze logs and events from multiple sources**
- **(Correct)**
- **To delete logs and events that are no longer needed**
- **To provide a backup of all system and network data**

Explanation

A SIEM system is a type of security software that is designed to collect, correlate, and analyze logs and events from multiple sources in order to detect and respond to security incidents. By aggregating and analyzing data from different sources, a SIEM system can provide a comprehensive view of an organization's security posture and identify potential security threats.

Question 5: **Skipped**

A company's HR department creates a new employee record in their HR system. Which phase of the data lifecycle does this represent?

- **Data sharing**
- **Data modification**
- **Data use**
- **Data creation**
- **(Correct)**

Explanation

Data creation is the first phase of the data lifecycle, where data is generated or collected for the first time. In this scenario, the HR department is creating a new employee record in their system, which is the beginning of the data lifecycle for that record.

Question 6: **Skipped**

What is the difference between data classification and data labeling?

- **Data classification is the process of attaching metadata to data, while data labeling is the practice of categorizing data based on its sensitivity or importance.**
- **Data classification is the process of categorizing data based on its sensitivity or importance, while**

data labeling is the practice of attaching metadata to data.

- **(Correct)**
- **Neither data classification nor data labeling is important for data security.**
- **Data classification and data labeling are the same thing.**

Explanation

Data classification is the process of categorizing data based on its sensitivity or importance, while data labeling is the practice of attaching metadata to data. Data classification and labeling are different processes, with data classification helping organizations identify which data is sensitive and requires more stringent access controls, while data labeling provides a way to easily identify and track data based on its classification or other attributes.

Question 7: **Skipped**

What are the key topics covered in security awareness training?

- **Customer service, software tools, data analysis, financial management, marketing strategies**
- **Physical security, workplace safety, first aid, emergency response procedures**

- **Employee benefits, HR policies, supply chain management, workplace culture**
- **Phishing, password management, data protection, mobile device security, social engineering**
- **(Correct)**

Explanation

The key topics covered in security awareness training typically include phishing, password management, data protection, mobile device security, and social engineering, as these are some of the most common security threats faced by organizations.

Question 8: **Skipped**

Which type of encryption uses the same key for both encryption and decryption?

- **Asymmetric encryption**
- **All options**
- **Hash encryption**
- **Symmetric encryption**
- **(Correct)**

Explanation

In symmetric encryption, the same key is used for both encryption and decryption. Asymmetric encryption uses two keys, one for encryption and one for decryption, while hash encryption is a one-way process that cannot be reversed.

Question 9: **Skipped**

Which of the following is a property of a good hash function?

- **Reversibility**
- **Collision resistance**
- **(Correct)**
- **Length variability**
- **Randomness**

Explanation

A good hash function should be resistant to collision attacks, which means it should be difficult to find two different inputs that produce the same output (hash value). Reversibility is not a desirable property of a hash function, as it would compromise its one-way nature. Randomness and length variability are not necessary properties of a hash function.

Question 10: **Skipped**

Which of the following best describes the purpose of change management in cybersecurity?

- **To delegate responsibility for changes to a third-party provider.**
- **To ensure that changes are implemented in a way that minimizes risk and disruption.**
- **(Correct)**

- **To prevent any changes from being made to security measures.**
- **To ensure that changes are implemented quickly and without review.**

Explanation

The purpose of change management in cybersecurity is to ensure that any changes made to security measures are implemented in a way that minimizes risk and disruption. This involves careful planning, review, and testing to ensure that changes are effective and don't cause unintended consequences. By implementing changes in a thoughtful and deliberate way, organizations can ensure that their cybersecurity measures remain effective and their operations remain uninterrupted.

Question 11: **Skipped**

Which of the following is an example of an information asset registry?

- **A list of all the suppliers and vendors used by an organization**
- **A list of all the employees in an organization and their roles**
- **A database of all the financial transactions of an organization**
- **A list of all the hardware and software assets in an organization**

- **(Correct)**

Explanation

An information asset registry is a centralized database or repository that contains information about an organization's hardware, software, and other technology assets. It is used to manage and maintain the assets and ensure that they are secure and compliant with regulations and standards.

Question 12: **Skipped**

What is the difference between a log and an event?

- **A log is a record of security-related events, while an event is a record of all types of events**
- **A log is a specific occurrence, while an event is a record of events**
- **A log is a record of events, while an event is a specific occurrence**
- **(Correct)**
- **A log and an event are the same thing**

Explanation

A log is a record of events that occur on a system or network, while an event is a specific occurrence that is captured in a log. For example, a login attempt is an event, while the record of all login attempts is a log. Option (b) is incorrect because it incorrectly defines a log as a specific occurrence.

Question 13: **Skipped**

What is the most significant challenge associated with implementing changes in cybersecurity?

- **Lack of skilled personnel**
- **(Correct)**
- **Lack of executive buy-in**
- **Lack of awareness about the importance of cybersecurity**
- **Lack of resources**

Explanation

Cybersecurity is a complex and rapidly changing field, and implementing changes requires specialized knowledge and skills. However, there is a significant shortage of skilled personnel in the cybersecurity industry, which can make it difficult for organizations to find and hire qualified professionals. This can lead to delays in implementing changes or even prevent changes from being implemented altogether. Therefore, lack of skilled personnel is the most significant challenge associated with implementing changes in cybersecurity.

Question 14: **Skipped**

What is Egress monitoring?

- **Monitoring incoming network traffic to detect and prevent unauthorized access**

- **Monitoring the behavior of network users to detect and prevent unauthorized access**
- **Monitoring outgoing network traffic to detect and prevent unauthorized access**
- **(Correct)**
- **Monitoring the performance of network devices to detect and prevent unauthorized access**

Explanation

Egress monitoring is the practice of monitoring outgoing network traffic to detect and prevent unauthorized access to an organization's network resources. This can include monitoring for data exfiltration attempts, unauthorized access to sensitive resources, and the use of unauthorized network services.

Question 15: **Skipped**

Which of the following is an example of a digital signature algorithm?

- **AES**
- **HMAC**
- **RSA**
- **(Correct)**
- **SHA-256**

Explanation

RSA (Rivest-Shamir-Adleman), which is a commonly used digital signature algorithm. SHA-256 and HMAC are hash

functions used for message authentication, while AES is a symmetric encryption algorithm used for data confidentiality.

Question 16: **Skipped**

What is the main purpose of an Acceptable Use Policy (AUP)?

- **To allow employees to use company resources as they see fit.**
- **To provide guidelines for appropriate use of company resources.**
- **(Correct)**
- **To delegate responsibility for resource management to a third-party provider.**
- **To restrict access to company resources.**

Explanation

The main purpose of an Acceptable Use Policy (AUP) is to provide guidelines for appropriate use of company resources, such as computer systems, networks, and internet access. This policy outlines what is and isn't allowed, and defines the consequences of policy violations. It helps to protect company resources from abuse, minimize legal and security risks, and establish expectations for employee behavior.

Question 17: **Skipped**

Which of the following best describes a digital signature?

- **A code that encrypts a message**
- **A mathematical scheme that verifies the authenticity and integrity of a digital message or document**
- **(Correct)**
- **An electronic image of a handwritten signature**
- **A password used to access a digital account**

Explanation

A digital signature is a type of electronic signature that uses encryption and a digital certificate to verify the authenticity of a message or document and ensure that it has not been tampered with.

Question 18: **Skipped**

Which type of encryption is used for secure communication between a web server and a web browser?

- **Symmetric encryption**
- **Hash encryption**
- **Asymmetric encryption**
- **SSL/TLS**
- **(Correct)**

Explanation

SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a protocol that uses both symmetric and asymmetric encryption to provide secure communication between a web server and a web browser. Hash encryption is not

typically used for secure communication, and while symmetric and asymmetric encryption can be used for secure communication, they are not typically used on their own for this purpose.

Question 19: **Skipped**

Which of the following is an example of a symmetric encryption algorithm?

- **Diffie-Hellman**
- **ECC**
- **AES**
- **(Correct)**
- **RSA**

Explanation

AES (Advanced Encryption Standard), which is a widely-used symmetric encryption algorithm. RSA, Diffie-Hellman, and ECC are all examples of asymmetric encryption algorithms.

Question 20: **Skipped**

Which of the following is a common requirement for privacy policies under data protection laws?

- **Using personal data for any purpose without user consent**
- **Clearly explaining the purposes for which personal data is collected and processed**
- **(Correct)**

- **Sharing personal data with third parties without user consent**
- **Retaining personal data indefinitely without any justification**

Explanation

Many data protection laws require organizations to clearly explain the purposes for which personal data is collected and processed, and to obtain user consent for these purposes. This helps ensure that individuals are aware of how their personal data is being used and can make informed decisions about whether to share their information with the organization.

Question 21: **Skipped**

What is an example of a hands-on security awareness training activity?

- **Phishing simulation exercises**
- **(Correct)**
- **Taking a multiple-choice quiz about cyber threats**
- **Reading an article about data privacy**
- **Watching a video about password security**

Explanation

Phishing simulation exercises are an example of a hands-on security awareness training activity. They involve sending mock phishing emails to employees to test their ability to identify and report suspicious messages.

Question 22: **Skipped**

How can data classification and labeling help with data governance and compliance?

- **By reducing the risk of data breaches and loss of intellectual property.**
- **By demonstrating that the organization is handling data in a responsible and compliant manner.**
- **By providing a way to easily identify and track data based on its regulatory requirements.**
- **All options**
- **(Correct)**

Explanation

Data classification and labeling can help organizations maintain good data governance practices and comply with regulatory requirements by reducing the risk of data breaches and loss of intellectual property, providing a way to easily identify and track data based on its regulatory requirements, and demonstrating that the organization is handling data in a responsible and compliant manner.

Question 23: **Skipped**

What is the purpose of the data archiving phase of the data lifecycle?

- **To create new data from existing data sources.**
- **To modify data to reflect changes or updates.**

- **To use data for specific purposes, such as analysis or decision-making.**
- **To store data for long-term preservation or regulatory compliance purposes.**
- **(Correct)**

Explanation

The purpose of the data archiving phase of the data lifecycle is to store data for long-term preservation or regulatory compliance purposes.

Question 24: **Skipped**

What are some best practices for data destruction?

- **Only deleting data when storage space is needed.**
- **Storing all data indefinitely, regardless of its importance or sensitivity.**
- **None**
- **Developing and implementing a data destruction policy, training employees on data destruction, and regularly auditing data destruction practices.**
- **(Correct)**

Explanation

Best practices for data destruction include developing and implementing a data destruction policy that outlines the organization's data destruction procedures, training employees on data destruction best practices, and regularly auditing data destruction practices to ensure

compliance with policy and legal requirements. Additionally, organizations should consider using multiple methods of data destruction to ensure that the data is properly erased or destroyed.

Question 25: **Skipped**

What is a common challenge associated with implementing a Bring Your Own Device (BYOD) policy?

- **Monitoring employees' personal use of their devices.**
- **Ensuring that all employees have the latest and most secure devices.**
- **Managing the diversity of devices and operating systems used by employees.**
- **(Correct)**
- **Providing technical support for employees' personal devices.**

Explanation

One of the main challenges of a BYOD policy is the variety of devices and operating systems used by employees, which can make it difficult to ensure consistent security measures and support for all devices. With different devices running different versions of operating systems, security patches and updates may not be available for all devices at the same time. Therefore, a BYOD policy should establish guidelines for device compatibility, security, and

support, including software and hardware requirements, and guidelines for handling lost or stolen devices.

Question 26: **Skipped**

Why is it important to regularly review and update an AUP?

- **To keep the policy up-to-date with changing technology and security risks.**
- **(Correct)**
- **To delegate responsibility for policy management to a third-party provider.**
- **To make the policy more restrictive and limit employee access.**
- **To ensure that employees are following the policy.**

Explanation

It is important to regularly review and update an AUP to ensure that it remains relevant and effective in light of changing technology and security risks. As new threats emerge and technologies evolve, policies must be updated to address these changes. Regular reviews also provide an opportunity to assess policy effectiveness and identify areas for improvement.

Question 27: **Skipped**

Which of the following is a key component of a data handling policy?

- **Limiting access to data on a need-to-know basis.**

- **(Correct)**
- **Storing all data in a single location.**
- **Allowing employees to store data on personal devices.**
- **Delegating responsibility for data handling to a third-party provider.**

Explanation

A key component of a data handling policy is limiting access to data on a need-to-know basis. This helps to ensure that data is only accessed by those who have a legitimate business need for it, reducing the risk of unauthorized access or misuse. Allowing employees to store data on personal devices can increase the risk of data breaches or loss, while storing all data in a single location can increase the impact of a data breach or loss. Delegating responsibility for data handling to a third-party provider can also increase the risk of data breaches or loss, as it can reduce the organization's control over data security.

Question 28: **Skipped**

Which of the following is a potential use case for hash functions?

- **Data encryption**
- **Digital signature verification**
- **Password storage**

- **(Correct)**
- **Data compression**

Explanation

Hash functions can be used to store passwords securely by creating a one-way hash of the password and storing it instead of the actual password. This way, if an attacker gains access to the password database, they cannot easily retrieve the original passwords. Hash functions can also be used for data integrity checking, digital signature verification, and other security applications.

Question 29: **Skipped**

Which of the following is an important consideration when implementing system hardening measures?

- **All security measures should be disabled when performing software updates.**
- **System hardening measures should be tested and evaluated to ensure that they are effective.**
- **(Correct)**
- **Password policies should be relaxed to make it easier for users to access the system.**
- **System performance should always be prioritized over security.**

Explanation

Implementing system hardening measures without testing and evaluating their effectiveness can lead to unexpected

consequences, such as system downtime, user access issues, or increased risk of attacks. System performance should not be prioritized over security, and security measures should not be disabled during software updates. Password policies should not be relaxed as this can weaken the security of the system.

Question 30: **Skipped**

What is the purpose of system hardening?

- **To make a system more resilient against attacks and intrusions.**
- **(Correct)**
- **To ensure that a system is compatible with all software and hardware.**
- **To increase the performance of a system.**
- **To ensure that a system is always available and accessible.**

Explanation

System hardening involves implementing security measures to reduce the attack surface and increase the security of a system. This includes disabling unnecessary services, applying security patches and updates, configuring firewalls and access controls, and enforcing password policies, among other measures. The goal is to make it more difficult for attackers to gain access to the system and its data.

Question 31: **Skipped**

Why is security awareness training important for organizations?

- **It helps employees understand financial policies and procedures of an organization**
- **It helps employees understand the importance of protecting sensitive information and prevent data breaches**
- **(Correct)**
- **It helps employees improve their customer service skills and increase customer satisfaction**
- **It helps employees improve their technical skills and productivity**

Explanation

Security awareness training helps employees understand the importance of protecting sensitive information and prevent data breaches, which can result in significant financial losses and damage to an organization's reputation.

Question 32: **Skipped**

What is a cryptanalyst?

- **A person who manages cryptographic keys**
- **A person who encrypts data**
- **A person who designs cryptographic algorithms**

- **A person who analyzes and breaks cryptographic codes**
- **(Correct)**

Explanation

A person who analyzes and breaks cryptographic codes. Cryptanalysts are experts in breaking codes and ciphers to reveal hidden information. They use various techniques and methods, including mathematical analysis, statistical analysis, and brute-force attacks, to decipher encrypted messages.

Question 33: **Skipped**

What is the role of communication in change management in cybersecurity?

- **To increase the complexity of security measures.**
- **To inform employees about changes to security measures.**
- **(Correct)**
- **To delegate responsibility for changes to a third-party provider.**
- **To keep changes confidential to prevent leaks.**

Explanation

Communication is a critical component of change management in cybersecurity. It is important to inform employees about changes to security measures, both to ensure that they are aware of any new risks and to ensure

that they are prepared for any changes that may impact their work. Communication can also help to build trust and support for changes among employees, increasing the likelihood of their success. Keeping changes confidential is generally not necessary or advisable, as it can hinder communication and limit the effectiveness of change management efforts.

Question 34: **Skipped**

Which of the following is a key component of effective change management in cybersecurity?

- **Rapid implementation of changes to security measures.**
- **Delegation of responsibility for changes to a third-party provider.**
- **Ignoring potential risks associated with changes.**
- **Careful planning, review, and testing of changes.**
- **(Correct)**

Explanation

Effective change management in cybersecurity requires careful planning, review, and testing of changes. This helps to identify potential risks and ensure that changes are effective and don't cause unintended consequences. Rapid implementation of changes without review and testing can lead to disruptions or even security breaches. Similarly, delegation of responsibility for changes to a

third-party provider can lead to a loss of control and increased risk. Therefore, careful planning, review, and testing are essential components of effective change management in cybersecurity.

Question 35: **Skipped**

What is the difference between data backup and data archiving?

- **There is no difference between data backup and data archiving.**
- **Data backup is for storing multiple versions of data, while data archiving is for storing only one version of data.**
- **Data backup is for short-term storage of data, while data archiving is for long-term storage of data.**
- **(Correct)**
- **Data backup is for disaster recovery purposes, while data archiving is for regulatory compliance purposes.**

Explanation

Data backup is for short-term storage of data to protect against data loss in the event of a disaster or system failure. Data archiving is for long-term storage of data for regulatory compliance or historical preservation purposes.

Question 36: **Skipped**

Which of the following is not a component of change management?

- **Change evaluation and planning**
- **Change request management**
- **Service desk management**
- **(Correct)**
- **Change advisory board**

Explanation

Service desk management is not a component of change management. It is a separate process that involves providing support and assistance to end-users for IT-related issues.

Question 37: **Skipped**

What are some common elements of an Acceptable Use Policy (AUP)?

- **Guidelines for social media usage.**
- **All options**
- **(Correct)**
- **Guidelines for using company email accounts.**
- **Rules for accessing company data.**

Explanation

An Acceptable Use Policy (AUP) can include guidelines for a variety of company resources, including email accounts, data access, and social media usage. It can also cover other topics such as computer and network usage, software installation, and remote access. The specific

elements of an AUP will vary depending on the organization's needs and priorities.

Question 38: **Skipped**

Which of the following is an advantage of using symmetric encryption algorithms?

- **They can be used for digital signatures and key exchange**
- **They are faster and more efficient than asymmetric encryption algorithms**
- **(Correct)**
- **They are more secure than asymmetric encryption algorithms**
- **They do not require a shared secret key**

Explanation

Symmetric encryption algorithms are generally faster and more efficient than asymmetric encryption algorithms because they do not involve complex mathematical operations or large key sizes. However, symmetric encryption algorithms require a shared secret key, which must be kept secure between the parties involved. Asymmetric encryption algorithms, on the other hand, do not require a shared secret key but are slower and less efficient.

Question 39: **Skipped**

Which of the following is true about hash functions?

- **They are reversible functions that can be decrypted.**
- **They can be used as a replacement for symmetric encryption.**
- **They are used for encryption and decryption of data.**
- **They produce a fixed-size output for any input.**
- **(Correct)**

Explanation

Hash functions are one-way functions that take an input (message or data) of any size and produce a fixed-size output (hash or digest) of a fixed length. The output cannot be used to retrieve the original input, making them useful for data integrity and digital signature verification.

Question 40: **Skipped**

What is Ingress monitoring?

- **Monitoring the performance of network devices to detect and prevent unauthorized access**
- **Monitoring incoming network traffic to detect and prevent unauthorized access**
- **(Correct)**
- **Monitoring the behavior of network users to detect and prevent unauthorized access**
- **Monitoring outgoing network traffic to detect and prevent unauthorized access**

Explanation

Ingress monitoring is the practice of monitoring incoming network traffic to detect and prevent unauthorized access to an organization's network resources. This can include monitoring for known attack signatures, anomalies in network traffic, and attempts to exploit known vulnerabilities.

Question 41: **Skipped**

What is the main difference between education, training, and awareness?

- **Education focuses on creating a security culture, training focuses on practical skills, and awareness focuses on theoretical knowledge**
- **Education focuses on practical skills, training focuses on theoretical knowledge, and awareness focuses on creating a security culture**
- **Education focuses on providing information about policies and procedures, training focuses on theoretical knowledge, and awareness focuses on practical skills**
- **Education focuses on theoretical knowledge, training focuses on practical skills, and awareness focuses on providing information about policies, procedures and cybersecurity risks and threats**
- **(Correct)**

Explanation

The main difference between education, training, and awareness is that education focuses on theoretical knowledge that provides a comprehensive understanding of cybersecurity concepts and principles. Training is focused on developing specific skills and competencies to perform a task or job. In the context of cybersecurity, training involves providing individuals with hands-on experience in using security tools, technologies, and techniques, and Awareness focuses on creating a security culture within an organization and to raise general awareness of cybersecurity risks and threats among individuals.

Question 42: **Skipped**

How can security awareness training be integrated into everyday work activities?

- **By providing ongoing reminders and updates about security best practices through email or messaging systems**
- **(Correct)**
- **By hosting regular in-person seminars or workshops**
- **By providing employees with security-related tasks to complete as part of their job responsibilities**
- **By requiring employees to complete a training course before accessing company resources**

Explanation

Security awareness training can be integrated into everyday work activities by providing ongoing reminders and updates about security best practices through email or messaging systems. This approach can help reinforce key concepts and encourage employees to stay vigilant about security threats.

Question 43: **Skipped**

Which of the following is NOT a component of a digital signature?

- **A digital certificate**
- **A hash function**
- **A message or document**
- **An encryption key**
- **(Correct)**

Explanation

While encryption is often used in the process of creating a digital signature, it is not a specific component of the signature itself. The components of a digital signature include a digital certificate, a hash function, and a message or document to be signed.

Question 44: **Skipped**

An organization has implemented a data classification policy to protect sensitive information. What is the purpose of data classification?

- **To create new data from existing data sources**

- **To modify data to reflect changes or updates**
- **To apply access controls to data based on its sensitivity**
- **(Correct)**
- **To store data in multiple locations for redundancy**

Explanation

The purpose of data classification is to apply access controls to data based on its sensitivity, which helps protect sensitive information from unauthorized access, modification, or disclosure. By classifying data into different categories based on their sensitivity, organizations can identify which data should be restricted to specific users or groups, and which data can be accessed more broadly.

Question 45: **Skipped**

What factors should organizations consider when determining their data retention policies?

- **None**
- **The size of the organization, the type of data being managed, and the cost of storage.**
- **Industry-specific regulations, business needs, and storage capacity.**
- **(Correct)**
- **Data sensitivity, employee preferences, and budget constraints.**

Explanation

Organizations should consider a variety of factors when determining their data retention policies, including the legal and regulatory requirements specific to their industry, their own business needs and objectives, and their storage capacity. By taking these factors into account, organizations can ensure that their data retention policies are both effective and practical.

Question 46: **Skipped**

What are some best practices for data retention?

- **Deleting all data as soon as it is no longer needed, regardless of legal or business requirements.**
- **None**
- **Storing all data indefinitely, regardless of its importance or sensitivity.**
- **Regularly reviewing and updating data retention policies to ensure compliance with changing legal and regulatory requirements.**
- **(Correct)**

Explanation

Best practices for data retention include regularly reviewing and updating data retention policies to ensure that they comply with changing legal and regulatory requirements, as well as with the organization's own business needs and objectives. Additionally, organizations

should consider implementing a secure and reliable backup and archiving system to ensure that important data is not lost or compromised.

Question 47: **Skipped**

What is the purpose of a change advisory board (CAB) in change management?

- **To monitor the progress of changes to IT systems**
- **To approve all changes to IT systems**
- **To oversee the change management process**
- **To make decisions about changes to IT systems**
- **(Correct)**

Explanation

A change advisory board (CAB) is a group of people responsible for reviewing and evaluating proposed changes to IT systems. The CAB is responsible for assessing the impact of the change, evaluating risks, and making recommendations to the change manager. The CAB does not approve all changes to IT systems, but rather makes decisions about changes based on their impact and risk.

Question 48: **Skipped**

What is encryption?

- **The process of hiding information in plain sight**
- **The process of converting plaintext into gibberish**
- **The process of converting plaintext into ciphertext**

- **(Correct)**
- **The process of converting ciphertext into plaintext**

Explanation

Encryption is the process of converting plaintext, which is readable and understandable information, into ciphertext, which is unreadable and unintelligible information. This is done using a mathematical algorithm and a key that makes it possible to decipher the ciphertext back into plaintext.

Question 49: **Skipped**

What is the purpose of a Configuration Management Database (CMDB)?

- **To manage the configuration of network switches and routers**
- **To automate the process of deploying software updates and patches**
- **To provide a secure storage location for sensitive data**
- **To store and manage information about the configuration items (CIs) in an IT environment**
- **(Correct)**

Explanation

A CMDB is a database that contains information about the CIs in an IT environment, including their attributes, relationships, and dependencies. It is used to support IT

service management processes, such as incident management, problem management, and change management. A CMDB can be used to track the status of CIs, manage changes to CIs, and support decision-making related to IT service management.

Question 50: **Skipped**

What is the difference between an information asset inventory and an information asset catalog?

- **An inventory tracks the physical location of each asset, while a catalog tracks the logical location of each asset.**
- **An inventory is a list of all information assets, while a catalog provides detailed information about each asset.**
- **(Correct)**
- **An inventory is used for risk assessment, while a catalog is used for incident response.**
- **There is no difference between an inventory and a catalog.**

Explanation

An information asset inventory is a list of all information assets, while an information asset catalog provides detailed information about each asset, such as the asset's owner, classification, criticality, and sensitivity.

Question 51: **Skipped**

What are some methods of data destruction?

- **Encryption, compression, and backup.**
- **Overwriting, physical destruction, and degaussing.**
- **(Correct)**
- **Patching**
- **Archiving, metadata removal, and compression.**

Explanation

Overwriting involves replacing the data on a storage medium with new data to ensure that the original data cannot be recovered. Physical destruction involves physically destroying the storage medium, such as by shredding a hard drive or melting a CD. Degaussing involves exposing the storage medium to a powerful magnetic field to erase the data. These methods are all effective ways of ensuring that the data is no longer accessible.

Question 52: **Skipped**

Which of the following is NOT a benefit of maintaining an accurate information asset inventory?

- **Improved employee productivity**
- **(Correct)**
- **Improved compliance with regulations and standards**
- **Improved risk management**
- **Improved incident response and recovery**

Explanation

Maintaining an accurate information asset inventory can lead to improved risk management, compliance with regulations and standards, and incident response and recovery. However, it does not necessarily improve employee productivity.

Question 53: **Skipped**

What is the primary objective of change management in cybersecurity?

- **To minimize the impact of changes to security measures.**
- **(Correct)**
- **To delegate responsibility for changes to a third-party provider.**
- **To increase the complexity of security measures.**
- **To eliminate all cybersecurity risks.**

Explanation

The primary objective of change management in cybersecurity is to minimize the impact of changes to security measures. Changes to security measures can introduce new risks or increase existing ones, and can also disrupt an organization's operations if not implemented properly. Change management processes help to identify potential issues and plan for their mitigation, reducing the risk of disruption and ensuring that security measures continue to be effective.

Question 54: **Skipped**

An employee downloads a customer report from the company's sales database to analyze sales trends. Which phase of the data lifecycle does this represent?

- **Data use**
- **(Correct)**
- **Data creation**
- **Data modification**
- **Data sharing**

Explanation

Data use is the phase of the data lifecycle where data is utilized for a specific purpose, such as analysis or decision-making. In this scenario, the employee is downloading the customer report from the company's sales database to analyze sales trends, which represents the data use phase of the data lifecycle.

Question 55: **Skipped**

Which of the following is an example of a key exchange algorithm used in symmetric encryption?

- **Diffie-Hellman**
- **(Correct)**
- **SHA-256**
- **AES**
- **RSA**

Explanation

Diffie-Hellman, which is a key exchange algorithm used to establish a shared secret key between two parties in symmetric encryption. RSA is an example of an asymmetric encryption algorithm, while AES and SHA-256 are examples of symmetric encryption algorithms and hash functions, respectively.

Question 56: **Skipped**

What is the purpose of logging and monitoring security events?

- **To detect and respond to security incidents in real-time**
- **(Correct)**
- **To identify security vulnerabilities in an organization's systems and networks**
- **To provide a record of security events for auditing and forensic purposes**
- **To increase network bandwidth and performance**

Explanation

While logging and monitoring security events can help organizations identify vulnerabilities in their systems and networks and provide a record of security events for auditing and forensic purposes, the primary purpose is to detect and respond to security incidents in real-time. By monitoring security events, organizations can quickly

identify potential threats and take immediate action to mitigate them.

Question 57: **Skipped**

What is the benefit of real-time monitoring of security events?

- **It allows organizations to respond to security incidents more quickly**
- **(Correct)**
- **It increases network bandwidth and performance**
- **It reduces the need for data backups**
- **It allows organizations to identify potential security threats at a later time**

Explanation

Real-time monitoring of security events allows organizations to detect and respond to security incidents as they occur, rather than after the fact. This can be critical for mitigating the impact of security incidents and minimizing damage to an organization's systems and data.

Question 58: **Skipped**

A company uses labels to identify different types of data based on their sensitivity, such as "public," "confidential," and "top secret." What is the purpose of data labeling?

- **To modify data to reflect changes or updates**

- **To apply access controls to data based on its sensitivity**
- **(Correct)**
- **To create new data from existing data sources**
- **To store data in multiple locations for redundancy**

Explanation

The purpose of data labeling is to identify different types of data based on their sensitivity, which helps determine how data should be accessed, used, and protected. By labeling data with different sensitivity levels, organizations can apply access controls that restrict access to sensitive data only to users who need it, while allowing more open access to less sensitive data.

Question 59: **Skipped**

What is data remanence?

- **The process of securely deleting data from a storage device**
- **The ability of data to be recovered from backups**
- **The process of encrypting data to protect it from unauthorized access**
- **The tendency of data to persist after it has been deleted**
- **(Correct)**

Explanation

Data remanence is the residual representation of data that remains even after attempts have been made to remove or erase it. This can be a significant security risk, as sensitive data that is thought to have been deleted can still be recovered by attackers using specialized techniques and tools.

Question 60: **Skipped**

Which of the following is another name for symmetric encryption algorithms?

- **Hash functions**
- **Public key cryptography**
- **Asymmetric encryption algorithms**
- **Shared secret cryptography**
- **(Correct)**

Explanation

Symmetric encryption algorithms use the same key for both encryption and decryption, and this key must be kept secret and shared between the parties involved. Hence, another names for symmetric encryption are shared secret cryptography, Same key Single key, Shared key, Secret key and Session key. Public key cryptography and asymmetric encryption algorithms use different keys for encryption and decryption, while hash functions are one-way functions that do not involve keys.

Question 61: **Skipped**

Which of the following is a best practice for managing software updates and patches in a production environment?

- **Apply all updates and patches as soon as they become available**
- **Apply updates and patches to all systems simultaneously**
- **Delay the installation of updates and patches until a critical issue is discovered**
- **Test updates and patches in a development environment before applying them to production**
- **(Correct)**

Explanation

It is important to test updates and patches in a non-production environment before applying them to production to ensure that they do not cause any unexpected issues. Applying updates and patches as soon as they become available without testing them can lead to system downtime and other issues. It is also not recommended to delay the installation of updates and patches, as this can leave systems vulnerable to security threats. Instead, updates and patches should be applied in a timely manner after they have been tested in a non-production environment.

Question 62: **Skipped**

What is the purpose of Ingress and Egress monitoring?

- **To ensure compliance with industry regulations**
- **To detect and prevent unauthorized access to an organization's network resources**
- **(Correct)**
- **To monitor the behavior of network users to detect insider threats**
- **To monitor the performance of network devices to optimize network performance**

Explanation

The purpose of Ingress and Egress monitoring is to detect and prevent unauthorized access to an organization's network resources by monitoring incoming and outgoing network traffic. This helps to identify potential security threats and prevent them from causing harm to the organization.

Question 63: **Skipped**

What is the purpose of a change request form in change management?

- **To provide a way to track the progress of the change request**
- **All options**
- **(Correct)**
- **To provide documentation of the change request**

- **To provide a way for stakeholders to review and approve the change request**

Explanation

A change request form is a document used to capture the details of a proposed change. It typically includes information such as the reason for the change, the impact of the change, and the risks associated with the change. The change request form is used to provide documentation of the change request, to track the progress of the change request, and to provide a way for stakeholders to review and approve the change request.

Question 64: **Skipped**

What is the difference between a standard change and an emergency change in change management?

- **A standard change is pre-approved while an emergency change is not.**
- **(Correct)**
- **A standard change follows the normal change management process while an emergency change requires a faster approval process.**
- **A standard change is a routine change while an emergency change is a high-risk change.**
- **A standard change is a minor change while an emergency change is a major change.**

Explanation

A standard change is a pre-approved change that is low-risk and has a predictable outcome. It is typically a routine change that follows a defined process and does not require a lot of scrutiny. An emergency change, on the other hand, is a change that is required to address an urgent situation or to avoid a major impact on the business. Emergency changes are not pre-approved and require a faster approval process, often involving higher-level management.

Question 65: **Skipped**

What are some examples of storage devices where data remanence can occur?

- **Solid-state drives**
- **Hard disk drives**
- **All options**
- **(Correct)**
- **USB flash drives**

Explanation

Data remanence can occur on a variety of storage devices, including hard disk drives (HDDs), solid-state drives (SSDs), and USB flash drives. When data is stored on these devices, it can leave traces that persist even after attempts have been made to delete it. This is why it is important to use secure data destruction techniques to

ensure that data is completely erased and cannot be recovered by attackers.

Question 66: **Skipped**

When should a rollback plan be developed in the change management process?

- **During the change request management process**
- **After the change has been implemented in the IT environment**
- **Before the change is implemented in the IT environment**
- **(Correct)**
- **During the change evaluation and planning process**

Explanation

A rollback plan should be developed before the change is implemented in the IT environment, as part of the change evaluation and planning process. This helps ensure that the organization is prepared to respond quickly if the change causes problems or disruptions.

Question 67: **Skipped**

Which of the following is a potential consequence of violating an AUP?

- **Disciplinary action up to and including termination.**
- **(Correct)**
- **A monetary fine.**
- **Public shaming.**

- **A written warning.**

Explanation

The consequences for violating an AUP can vary depending on the severity of the violation and the organization's policies. However, disciplinary action up to and including termination is a common consequence for serious policy violations. This is intended to send a clear message that policy violations will not be tolerated, and to deter employees from engaging in behaviors that could put company resources at risk. Other consequences may include loss of access to company resources, legal action, or criminal prosecution.

Question 68: **Skipped**

Which of the following is an example of system hardening?

- **Disabling unnecessary services and ports on a server.**
- **(Correct)**
- **Enabling all user accounts with administrative privileges.**
- **Allowing all incoming traffic through a firewall.**
- **Allowing users to connect to a network without a password.**

Explanation

System hardening involves removing or disabling any unnecessary or vulnerable components or settings from a system to reduce the attack surface. Enabling all user accounts with administrative privileges or allowing all incoming traffic through a firewall would increase the risk of an attack. Allowing users to connect to a network without a password would also be a significant security risk.

Question 69: **Skipped**

What is security awareness training?

- **A process of teaching employees how to protect the physical security of an organization**
- **A process of teaching employees how to use software and hardware tools to improve productivity**
- **A process of teaching employees how to improve customer service skills**
- **A process of educating employees about the importance of data protection and how to identify and avoid security threats**
- **(Correct)**

Explanation

Security awareness training is a process of educating employees about the importance of data protection, how to identify and avoid security threats, and how to respond to security incidents.

Question 70: **Skipped**

Which of the following is a key component of a strong password policy?

- **Allowing users to reuse previous passwords.**
- **Mandating complex passwords with a mix of characters, symbols, and numbers.**
- **(Correct)**
- **Mandating passwords that are at least 6 characters long.**
- **Allowing employees to share their passwords.**

Explanation

A key component of a strong password policy is mandating complex passwords with a mix of characters, symbols, and numbers. Passwords that include these elements are generally more difficult to guess or crack using automated tools. Allowing users to reuse previous passwords or mandating shorter passwords can increase the risk of a password being compromised. Allowing employees to share their passwords is also a security risk as it increases the likelihood of a password being compromised or misused.

Question 71: **Skipped**

How can data remanence be addressed?

- **By implementing access controls to restrict who can view or modify data**

- **By performing regular backups of important data**
- **By using data encryption to protect sensitive data**
- **By using secure data destruction techniques**
- **(Correct)**

Explanation

The best way to address data remanence is to ensure that sensitive data is securely and completely erased when it is no longer needed. This can be achieved using secure data destruction techniques, such as overwriting the data with random patterns or physically destroying the storage media. While data encryption, regular backups, and access controls can all be important components of a data security strategy, they are not specifically designed to address the issue of data remanence.

Question 72: **Skipped**

What are the four main phases of the data lifecycle?

- **Data creation, data use, data modification, data archiving**
- **(Correct)**
- **Data creation, data use, data sharing, data archiving**
- **Data creation, data storage, data modification, data destruction**
- **Data creation, data storage, data use, data destruction**

Explanation

The four main phases of the data lifecycle are data creation, data use, data modification, and data archiving.

Question 73: **Skipped**

What does "safety first" mean in the workplace?

- **Safety is only important in high-risk industries**
- **Safety is the top priority in all work activities**
- **(Correct)**
- **Safety is important, but productivity is more important**
- **Safety is the responsibility of individual employees, not the organization**

Explanation

"Safety first" means that safety is the top priority in all work activities. This means that no job or task is more important than the safety of employees and others involved in the work.

Question 74: **Skipped**

What is data destruction, and why is it important for organizations?

- **Data destruction is the process of temporarily deleting data, and it is important for organizations because it helps them free up storage space.**
- **Data destruction is the process of permanently erasing or destroying data, and it is important for organizations because it helps them protect**

sensitive or confidential information from unauthorized access or disclosure.

- **(Correct)**
- **Data destruction is the process of encrypting data, and it is important for organizations because it ensures that the data is protected from hackers and other cyber threats.**
- **Data destruction is not important for organizations.**

Explanation

Data destruction is an important aspect of data management because it helps organizations ensure that sensitive or confidential information is not accessible to unauthorized individuals, even after the data is no longer needed. This is especially important for organizations that handle sensitive information, such as financial institutions, healthcare providers, or government agencies.

Question 75: **Skipped**

What is the best approach to managing the risk of change in cybersecurity?

- **Implementing a set of static security measures**
- **Outsourcing cybersecurity to a third-party provider**
- **Developing a dynamic, risk-based approach to cybersecurity**
- **(Correct)**
- **Ignoring the risk and hoping for the best**

Explanation

Cybersecurity threats are constantly evolving, and static security measures are not sufficient to protect against them. A dynamic, risk-based approach to cybersecurity involves continuously assessing and managing risks and implementing appropriate controls to mitigate those risks. This approach enables organizations to respond to changing threats and adapt their security measures accordingly. It also ensures that security measures are aligned with the organization's overall risk management strategy.

Question 76: **Skipped**

Which of the following is an example of an asymmetric encryption algorithm?

- **Blowfish**
- **RSA**
- **(Correct)**
- **RC4**
- **DES**

Explanation

RSA (Rivest-Shamir-Adleman), which is a widely-used asymmetric encryption algorithm. Blowfish, DES, and RC4 are all examples of symmetric encryption algorithms.

Question 77: **Skipped**

What is a rollback in change management?

- **The process of undoing a change that has been implemented in the IT environment**
- **(Correct)**
- **The process of testing a proposed change before it is implemented in the IT environment**
- **The process of communicating a proposed change to end-users before it is implemented in the IT environment**
- **The process of documenting a proposed change before it is implemented in the IT environment**

Explanation

A rollback is the process of undoing a change that has been implemented in the IT environment, either because the change caused unexpected problems or disruptions, or because the change did not have the desired outcome.

Question 78: **Skipped**

What is the primary purpose of a Bring Your Own Device (BYOD) policy?

- **To require employees to purchase company-approved devices.**
- **To ensure that employees use company-provided devices only.**
- **To prohibit the use of personal devices for work-related tasks.**

- **To allow employees to use their personal devices for work-related tasks.**
- **(Correct)**

Explanation

A Bring Your Own Device (BYOD) policy is designed to allow employees to use their personal devices, such as smartphones or tablets, for work-related tasks. This can increase productivity and convenience for employees, as they can work from anywhere, at any time, using the devices they are most comfortable with. However, a BYOD policy should also establish guidelines and requirements for device security, data protection, and acceptable use, to ensure that company data is protected and employees are using their devices appropriately.

Question 79: **Skipped**

What is a common method of delivering security awareness training?

- **Written manuals**
- **One-on-one coaching sessions**
- **Online courses**
- **(Correct)**
- **Physical demonstrations**

Explanation

Online courses are a common method of delivering security awareness training because they are scalable,

cost-effective, and can be easily tailored to meet the specific needs of an organization.

Question 80: **Skipped**

Which of the following is a potential drawback of a password policy?

- **It can make it easier for attackers to guess passwords by limiting the number of characters allowed.**
- **It can lead to employees sharing their passwords with coworkers.**
- **It can reduce the likelihood of a password breach.**
- **It can create a burden for users who must remember multiple complex passwords.**
- **(Correct)**

Explanation

One potential drawback of a password policy is that it can create a burden for users who must remember multiple complex passwords. This can lead to users writing down passwords or reusing passwords across multiple accounts, which can increase the risk of a password breach. However, using a password manager can help to mitigate this issue by allowing users to store and generate strong, unique passwords for each account they have, reducing the burden of password management.

Question 81: **Skipped**

An organization has classified their data into different categories based on their sensitivity, but they are not consistently applying access controls. What is the risk of not consistently applying access controls?

- **Data may be deleted accidentally**
- **Data may be modified without authorization**
- **The organization may run out of storage space**
- **Sensitive data may be exposed to unauthorized users**
- **(Correct)**

Explanation

The risk of not consistently applying access controls is that sensitive data may be exposed to unauthorized users, which can lead to data breaches, loss of intellectual property, or regulatory noncompliance. By not consistently applying access controls, organizations may inadvertently allow sensitive data to be accessed by users who should not have access, which can put the organization and its stakeholders at risk.

Question 82: **Skipped**

Which of the following is a type of cryptanalysis attack?

- **Phishing attack**
- **Brute-force attack**
- **(Correct)**
- **Firewall attack**
- **DDoS attack**

Explanation

A Brute-force attack is a cryptanalysis technique that involves trying all possible keys or passwords to decrypt an encrypted message. It is a time-consuming and resource-intensive attack, but it can be effective against weak encryption algorithms or short keys. Firewall, phishing, and DDoS attacks are types of network attacks and are not related to cryptanalysis.

Question 83: **Skipped**

Which of the following is a method used by cryptanalysts to break encryption?

- **Cryptography hashing**
- **Key generation**
- **Frequency analysis**
- **(Correct)**
- **Key exchange**

Explanation

Cryptanalysts use various methods and techniques to break encryption, including brute-force attacks, mathematical analysis, and statistical analysis. Frequency analysis is a method used to analyze the frequency distribution of letters or symbols in an encrypted message and to deduce the key or plaintext based on the patterns of the distribution. Key generation and key exchange are methods used to generate or exchange cryptographic

keys, while cryptography hashing is a method used to convert data into a fixed-length code.

Question 84: **Skipped**

What is the role of regular audits in a data handling policy?

- **To delegate responsibility for data handling to a third-party provider.**
- **To ensure that all employees have access to all data.**
- **To prevent employees from accessing data.**
- **To ensure that data is being handled in accordance with the guidelines.**
- **(Correct)**

Explanation

Regular audits are a critical component of a data handling policy. By regularly auditing data handling practices, organizations can ensure that data is being handled in accordance with the guidelines, and can identify any areas that need improvement. Audits can also help to identify potential risks or vulnerabilities, and can ensure compliance with regulations. Regular audits are essential for maintaining the effectiveness of a data handling policy over time.

Question 85: **Skipped**

Which of the following is a key element of a rollback plan in change management?

- **Identifying the steps needed to undo the change**
- **(Correct)**
- **Communicating the change to end-users**
- **Identifying the risks and impacts of the change**
- **Assigning a project manager to oversee the change**

Explanation

One of the key elements of a rollback plan is to identify the steps needed to undo the change. This includes identifying the configuration items that were changed, the order in which they need to be rolled back, and any dependencies or impacts of the rollback on other systems or processes. By having a clear plan in place, the organization can respond quickly and effectively to any issues that arise during the change management process.

Question 86: **Skipped**

What is the purpose of encryption?

- **To hide information from unauthorized access**
- **(Correct)**
- **To compress information for storage**
- **To delete information permanently**
- **To modify information to make it more secure**

Explanation

The primary purpose of encryption is to protect sensitive information from unauthorized access by making it unreadable and unintelligible. This helps to ensure the

confidentiality and privacy of the information, especially when it is being transmitted over an unsecured network or stored on an unsecured device.

Question 87: **Skipped**

What is a message digest?

- **A cryptographic key used to encrypt data**
- **A method of exchanging digital certificates**
- **An algorithm used to generate random numbers**
- **A compressed representation of a message or data**
- **(Correct)**

Explanation

A message digest is a fixed-length sequence of bits that represents a message or data. It is generated using a cryptographic hash function that takes the original message as input and produces the message digest as output. The message digest can be used to verify the integrity and authenticity of the original message, as any change to the message will result in a different message digest.

Question 88: **Skipped**

Which of the following is an example of a secure hash function?

- **SHA-256**
- **(Correct)**
- **SHA-1**

- **MD5**
- **SHA-0**

Explanation

SHA-256, which is a secure hash function that produces a 256-bit hash value. SHA-0 and SHA-1 are outdated and have known vulnerabilities, while MD5 is also considered insecure and should not be used for cryptographic purposes.

Question 89: **Skipped**

What are some legal and regulatory requirements related to data destruction?

- **Sarbanes-Oxley Act**
- **GDPR**
- **All options**
- **(Correct)**
- **HIPAA**

Explanation

There are several legal and regulatory requirements related to data destruction that organizations should be aware of. The Health Insurance Portability and Accountability Act (HIPAA) requires that covered entities implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The General Data

Protection Regulation (GDPR) requires organizations to ensure that personal data is processed securely and protected against unauthorized or unlawful processing, accidental loss, destruction, or damage. The Sarbanes-Oxley Act (SOX) requires public companies to establish and maintain internal controls over financial reporting, which includes the proper management and disposal of sensitive financial data. Other regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, also have requirements related to data destruction.

Question 90: **Skipped**

What is the role of employee training in implementing a data handling policy?

- **To prevent employees from accessing data.**
- **To delegate responsibility for data handling to a third-party provider.**
- **To ensure that all employees understand the guidelines for data handling.**
- **(Correct)**
- **To ensure that all employees have access to all data.**

Explanation

Employee training is a critical component of implementing a data handling policy. By ensuring that all employees

understand the guidelines for data handling, organizations can reduce the risk of data breaches and ensure compliance with regulations. Training can also help to increase employee awareness of the importance of data security, which can help to reduce the likelihood of human error or intentional misconduct.

Question 91: **Skipped**

What is data retention, and why is it important for organizations?

- **Data retention is not important for organizations.**
- **Data retention is the process of storing data for a specific period of time, and it is important for organizations because it helps them comply with legal and regulatory requirements.**
- **(Correct)**
- **Data retention is the process of storing data indefinitely, and it is important for organizations because it ensures that all data is kept safe and secure.**
- **Data retention is the process of deleting data as soon as it is no longer needed, and it is important for organizations because it frees up storage space.**

Explanation

Data retention is the process of storing data for a specific period of time, and it is important for organizations

because it helps them comply with legal and regulatory requirements. Data retention is an important aspect of data management because it ensures that data is kept for the required amount of time and is easily accessible if needed. Additionally, data retention policies help organizations avoid potential legal issues, such as fines or legal action, for failing to retain data when required.

Question 92: **Skipped**

What is the purpose of a digital certificate in relation to digital signatures?

- **To provide access control to the message or document**
- **To prevent unauthorized modification of the message or document**
- **To encrypt the message or document**
- **To verify the identity of the signer**
- **(Correct)**

Explanation

A digital certificate is a document that contains information about the identity of the signer and is used to verify the authenticity of the digital signature.

Question 93: **Skipped**

What is a privacy policy?

- **A legal document that outlines an organization's data protection practices and how it handles personal information**
- **(Correct)**
- **A marketing tool used by organizations to promote their products or services**
- **A document that outlines an organization's employee benefits and compensation policies**
- **A document that outlines an organization's financial policies and procedures**

Explanation

A privacy policy is a legal document that outlines how an organization collects, uses, stores, and shares personal information, and how it protects the privacy rights of individuals.

Question 94: **Skipped**

One of the below is uncommon types of security events that should be logged and monitored?

- **Changes to system configurations**
- **Login attempts and failures**
- **Power outages**
- **(Correct)**
- **Malware infections**

Explanation

Login attempts and failures, changes to system configurations, and malware infections are all common types of security events that should be logged and monitored. By monitoring these events, organizations can identify potential security threats and take appropriate action to mitigate them. Power outages is incorrect because it is not related to security events.

Question 95: **Skipped**

What is the purpose of software updates and patches in configuration management?

- **To optimize the performance of hardware devices**
- **To upgrade the operating system of a server**
- **To fix security vulnerabilities and bugs in software applications**
- **(Correct)**
- **To add new features to software applications**

Explanation

Software updates and patches are released by software vendors to address security vulnerabilities and bugs in their products. They are important for maintaining the security and reliability of IT systems and applications. While new features may be added in some software updates, the primary purpose is to address security vulnerabilities and bugs.

Question 96: **Skipped**

Which of the following is a benefit of security awareness training for organizations?

- **Increased employee turnover and absenteeism**
- **Reduced risk of data breaches and security incidents**
- **(Correct)**
- **Increased operating costs and reduced profitability**
- **Reduced customer satisfaction and brand reputation**

Explanation

Security awareness training can help reduce the risk of data breaches and security incidents by educating employees about how to identify and avoid security threats, how to use secure passwords and authentication methods, and how to report security incidents. This can help protect an organization's sensitive data and prevent financial losses and damage to its reputation.