Top of Form

Question 1:

Which of these is the PRIMARY objective of a Disaster Recovery Plan?

* **Communicate to the responsible entities the damage caused to operations in the event of a disaster**
* **Restore company operation to the last-known reliable operation state**

* **Maintain crucial company operations in the event of a disaster**
* **Outline a safe escape procedure for the organization's personnel**

**Explanation**

A Disaster Recovery Plan (DRP) is a plan for processing and restoring operations in the event of a significant hardware or software failure, or of the destruction of the organization's facilities. The primary goal of a DRP is to restore the business to the last-known reliable state of operations (see Chapter 2 ISC2 Study Guide, module 4, under The Goal of Disaster Recovery). Maintaining crucial operations is the goal of the Business Continuity Plan (BCP). The remaining options may be included in a DRP, but are not its primary objective.

Bottom of Form

Top of Form

Question 2: **Correct**

Which of the following is NOT a possible model for an Incident Response Team (IRT)?

* **Leveraged**
* **Hybrid**
* **Pre-existing**
* **Dedicated**

**Explanation**

The three possible models for incident response are Leveraged, Dedicated, and Hybrid (see the ISC2 Study Guide, Chapter 2, Module 1, under Chapter Takeaways). The term 'Pre-existing' is not a valid model for an IRT.

Bottom of Form

Top of Form

Question 3:

Which port is used to secure communication over the web (HTTPS)?

* **69**
* **443**
* **80**
* **25**

**Explanation**

All options show examples of logical communication ports. Port 80 is reserved for plain HTTP connections, port 69 for TFTP protocol; and port 25 for SMTP protocol. Port 443 is the one reserved for HTTPS connections.

Bottom of Form

Top of Form

Question 4:

What is an effective way of hardening a system?

* **Run a vulnerability scan**
* **Have an IDS in place**
* **Create a DMZ for web application services**
* **Patch the system**

**Explanation**

According to NIST SP 800-152, hardening is defined as the process of eliminating the means of an attack by simultaneously patching vulnerabilities and turning off nonessential services. The ISC2 Study Guide, chapter 5, module 2, under Configuration Management Overview, reads "One of the best ways to achieve a hardened system is to have updates, patches, and service packs installed automatically". Vulnerability scans and IDS do not eliminate the means of an attack. The DMZ does not eliminate vulnerabilities in a system.

Bottom of Form

Top of Form

Question 5:

Which type of attack attempts to trick the user into revealing personal information by sending a fraudulent message?

* **Phishing**
* **Trojans**
* **Denials of Service**
* **Cross-Site Scripting**

**Explanation**

A phishing attack emails a fraudulent message to trick the recipient into disclosing sensitive information to the attacker. A Cross-Site Scripting attack tries to execute code on another website. Trojans are software that appear legitimate, but that have hidden malicious functions. Trojans may be sent in a message, but are not the message themselves. A denial of service attack (DoS) consists in compromising the availability of a system or service through a malicious overload of requests, which causes the activation of safety mechanisms that delay or limit the availability of that system or service.

Bottom of Form

Top of Form

Question 6:

A best practice of patch management is to:

* **Apply patches every Wednesday**
* **Test patches before applying them**

* **Apply all patches as quickly as possible**
* **Apply patches according to the vendor's reputation**

**Explanation**

Patches sometimes disrupt a system's configurations and stability. One of the main challenges for security professionals is to ensure that patches are deployed as quickly as possible, while simultaneously ensuring the stability of running systems. To prevent flawed patches from negatively affecting running systems, it is good practice to test patches in a designated qualification environment before applying them to production systems (see ISC2 Study Guide, chapter 5, module 2 under Configuration Management Overview). Applying patches as quickly as possible is not a good practice. The vendor's reputation can be useful to know, but is not in itself sufficient to qualify the patch. Applying patches on fixed days also does not guarantee the stability of functioning systems after the patch is applied.

Bottom of Form

Top of Form

Question 7:

Which type of attack has the PRIMARY objective of encrypting devices and their data, and then demanding a ransom payment for the decryption key?

* **Ransomware**

* **Trojan**
* **Phishing**
* **Cross-Site Scripting**

**Explanation**

Ransomware is malware designed to deny a user or organization access to files on their computer, by encrypting them and demanding a ransom payment for the decryption key. Trojans and phishing can be used to install ransomware on a system or device, but are not themselves the ransomware attack.

Bottom of Form

Top of Form

Question 8:

Security posters are an element PRIMARILY employed in: (★)

* **Incident Response Plans**
* **Security Awareness**

* **Business Continuity Plans**
* **Physical Security Controls**

**Explanation**

Security posters are used to raise the awareness of employees regarding security threats, and thus are primarily employed in Security Awareness (see ISC2 Study Guide, chapter 5, module 4).

Bottom of Form

Top of Form

Question 9:

Which of these tools is commonly used to crack passwords? (★)

* **John the Ripper**

* **Burp Suite**
* **Wireshark**
* **Nslookup**

**Explanation**

John the Ripper is a famous Open Source password security auditing and password recovery tool. Burp Suite is a well-known set of tools for vulnerability scanning, penetration testing, and web app security (not for cracking passwords). The remaining options are both network analysis tools. Wireshark is the most used network protocol analyzer in the world. Nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between the domain name, IP address, or other DNS records.

Bottom of Form

Top of Form

Question 10:

Which type of key can be used to both encrypt and decrypt the same message?

* **A private key**
* **A symmetric key**

* **An asymmetric key**
* **A public key**

**Explanation**

Symmetric-key algorithms are a class of cryptographic algorithms that use a single key for both encrypting and decrypting of data. Asymmetric cryptography uses pairs of related keys: the public and the corresponding private keys. A message encrypted with the public key can only be decrypted by its corresponding private key, and vice versa. The term 'asymmetric key' is not applicable here.

Bottom of Form

Top of Form

Question 11:

In Change Management, which component addresses the procedures needed to undo changes?

* **Rollback**

* **Request for Change**
* **Request for Approval**
* **Disaster and Recover**

**Explanation**

In Change Management, the Request For Change (RFC) is the first stage of the request: it formalizes the change from the stakeholders' point of view. The next phase is the Approval phase, where each stakeholder reviews the change, identifies and allocates the corresponding resources, and eventually either approves or rejects the change (appropriately documenting the approval or rejection). Finally, the Rollback phase addresses the actions to take when the monitoring change suggests a failure or inadequate performance.

Bottom of Form

Top of Form

Question 12:

If there is no time constraint, which protocol should be employed to establish a reliable connection between two devices?

* **SNMP**
* **TCP**

* **UDP**
* **DHCP**

**Explanation**

TCP is used for connection-oriented communication, verifies data delivery, and is known to favor reliability. In a congested network, TCP delays data transmission, and thus cannot guarantee delivery under time constraints. UDP favors speed and efficiency over reliability, and thus cannot ensure a reliable connection. DHCP and SNMP are (respectively) a device configuration and a device management protocol, which means that neither aims to establish connections between devices.

Bottom of Form

Top of Form

Question 13:

Governments can impose financial penalties as a consequence of breaking a:

* **Standard**
* **Policy**
* **Procedure**
* **Regulation**

**Explanation**

Standards are created by governing or professional bodies (not by governments themselves). Policies and procedures are created by organizations, and are therefore not subject to financial penalties (see ISC2 Study Guide Chapter 1, Module 4)

Bottom of Form

Top of Form

Question 14:

Which of these types of user is LESS likely to have a privileged account?

* **Help Desk**
* **Security Analyst**
* **System Administrator**
* **External Worker**

**Explanation**

Typically, external workers should not have access to privileged accounts, due to the possibility of misuse. The Help Desk (or IT Support Staff) may have to view or manipulate endpoints, servers and applications platforms using privileged or restricted operations. Security analysts may require fast access to the IT infrastructure, systems, endpoints and data environment. By definition, systems administrators require privileged accounts, since they are responsible for operating systems, deploying applications, and managing performance.

Bottom of Form

Top of Form

Question 15:

Which protocol uses a three-way handshake to establish a reliable connection?

* **SMTP**
* **UDP**
* **TCP**

* **SNMP**

**Explanation**

TCP uses a three-way handshake to establish a reliable connection by exchanging three packets with theSYN, SYN/ACK, and ACK flags. SMTP uses a two-way handshake. Neither UDP nor SNMP require a handshake phase.

Bottom of Form

Top of Form

Question 16:

Which of the following attacks take advantage of poor input validation in websites?

* **Phishing**
* **Trojans**
* **Cross-Site Scripting**

* **Rootkits**

**Explanation**

Cross-Site Scripting (XSS) is a type of attack where malicious executable scripts are injected into the code of an otherwise benign website (or web application). Websites are vulnerable to XSS when they display data originating from requests or forms without validating it (and further sanitizing it, so that it is not executable). Trojans and phishing are attacks where software applications and messages try to appear legitimate but have hidden malicious functions, not necessarily relying on poor input validations. Finally, input validation does not even apply to a rootkit attack.

Bottom of Form

Top of Form

Question 17:

Sensitivity is a measure of the …:

* **… pertinence assigned to information by its owner, or the purpose of representing its need for urgency**
* **… urgency and protection assigned to information by its owner**
* **… importance assigned to information by its owner, or the purpose of representing its need for protection**

* **… protection and timeliness assigned to information by its owner, or the purpose of representing its need for urgency**

**Explanation**

Sensitivity is also defined as the measure of the importance assigned to information by its owner, or the purpose of representing its need for protection (see the ISC2 Study Guide, module 1, under CIA Deep Dive).

For example, a government document classified "Top Secret" is highly sensitive because its unauthorized disclosure could cause exceptionally grave damage to national security. The owner of the document, in this case the government, has determined its importance and the need to protect it accordingly.

Bottom of Form

Top of Form

Question 18:

Which of the following types of devices inspect packet header information to either allow or deny network traffic?

* **Switches**
* **Hubs**
* **Firewalls**

* **Routers**

**Explanation**

Standard firewalls examine IP packet headers and flags in order to block or allow traffic from predefined rules. More recently, firewalls with Intrusion Detection Capability (IDC) also analyze each individual packet, looking for specific patterns known to be malicious, and then blocking traffic whenever such patterns are found. Routers, Switches, and Hubs have limited packet filtering capabilities, or none at all. A Router is a device that acts as a gateway between two or more networks by relaying and directing data packets between them. Hubs broadcast (i.e. copy) packets between ports so that all segments of a LAN can see all packets. A Switch is "smarter" than a Hub and can forward packets between network segments instead of copying them.

Bottom of Form

Top of Form

Question 19:

Which concept describes an information security strategy that integrates people, technology and operations in order to establish security controls across multiple layers of the organization?

* **Privileged Accounts**
* **Separation of Duties**
* **Defense in Depth**

* **Least Privilege**

**Explanation**

Defense in depth describes a cybersecurity approach that uses multiple layers of security for holistic protection (see ISC2 Study Guide Chapter 1, Module 3). According to the principle of Separation of Duties, no user should ever be given enough privileges to misuse the system on their own. The principle of Least Privilege dictates that users should be given only those privileges required to complete their specific tasks. Privileged Accounts are a class of accounts that have permissions exceeding those of regular users, such as manager and administrator accounts.

Bottom of Form

Top of Form

Question 20:

The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction, or loss of information, is known as the:

* **Likelihood**
* **Threat**
* **Impact**

* **Vulnerability**

**Explanation**

The sentence matches the definition of the concept of impact (see NIST SP 800-60 Vol. 1 Rev. 1 under Impact). Furthermore, the ISC2 Study Guide, chapter 1, defines likelihood as the probability that a potential vulnerability may be exploited. A threat is defined as a circumstance or event that can adversely impact organizational operations. A vulnerability is a weakness that a threat can exploit.

Bottom of Form

Top of Form

Question 21:

The process of verifying or proving the user's identification is known as:

* **Integrity**
* **Confidentiality**
* **Authentication**

* **Authorization**

**Explanation**

Authentication is the verification of the identity of a user, process or device, as a prerequisite to allowing access to the resources in a given system (see the ISC2 Study Guide, module 1, under Authentication).

For example, when a user tries to log into their email account, they are typically prompted for a username and password. The system then checks these credentials against its database. If the credentials match, the user is authenticated and granted access.

In contrast, authorization refers to the permission granted to users, processes or devices to access specific assets. Confidentiality refers to ensuring that information is not disclosed to unauthorized individuals or systems, which is different from verifying identity. Integrity ensures that information is accurate and unaltered, which also does not involve verifying a user's identity.

Bottom of Form

Top of Form

Question 22:

Which of these has the PRIMARY objective of identifying and prioritizing critical business processes?

* **Business Continuity Plan**
* **Business Impact Plan**
* **Disaster Recovery Plan**
* **Business Impact Analysis**

**Explanation**

The term 'Business Impact Plan' does not exist. A Business Impact Analysis (BIA) is a technique for analyzing how disruptions can affect an organization, and determines the criticality of all business activities and associated resources. A Business Continuity Plan (BCP) is a pre-determined set of instructions describing how the mission/business processes of an organization will be sustained during and after a significant disruption. A Disaster Recovery Plan is a written plan for recovering information systems in response to a major failure or disaster.

Bottom of Form

Top of Form

Question 23:

Which of the following is NOT a type of learning activity used in Security Awareness?

* **Tutorial**

* **Awareness**
* **Training**
* **Education**

**Explanation**

The three learning activities that organizations use in training for security awareness are Education, Training and Awareness (see ISC2 Study Guide, chapter 5, module 4). A tutorial is a form of training, but is not on the list of types of learning activities.

Bottom of Form

Top of Form

Question 24:

Which security principle states that a user should only have the necessary permission to execute a task?

* **Least Privilege**

* **Defense in Depth**
* **Separation of Duties**
* **Privileged Accounts**

**Explanation**

The principle of Defense in Depth refers to using multiple layers of security. The principle of Least Privilege states that subjects should be given only those privileges required to complete their specific tasks (ISC2 Study Guide Chapter 1, Module 3). Separation of Duties states that no user should ever be given enough privileges to misuse the system. Finally, Privileged Accounts are accounts with permissions beyond those of regular users, such as manager and administrator accounts.

Bottom of Form

Top of Form

Question 25:

How many data labels are considered manageable?

* **1**
* **> 4**
* **2 – 3**

* **1 – 2**

**Explanation**

According to data handling and labeling best practices, two or three classifications for data are typically considered manageable for most organizations. In fact, in the ISC2 Study Guide, Chapter 5, Module 1, under Data Handling Practices in Labeling, we read that "two or three classifications are manageable, but more than four tend to be challenging to manage. These classifications could be labels such as Public, Confidential, and Restricted, each representing a different level of data sensitivity.

For example, in a healthcare organization, patient health information might be labeled "Confidential," while general health advice published on the organization's Web site might be labeled "Public. This labeling system allows the organization to easily identify and manage data based on its sensitivity level, ensuring that appropriate security measures are in place for each classification.

The principle is that labeling data based on its sensitivity level should be based on a limited, unambiguous set of labels that correspond to different levels of data sensitivity. The key is to have a system that differentiates data sensitivity levels without being overly complex to implement and maintain. Some organizations need more granularity in their data classification, while others are fine with a simpler system. However, having more than four labels (">4") can make the system overly complex and difficult to manage, increasing the risk of misclassification and potential data breaches.

Bottom of Form

Top of Form

Question 26:

Which physical access control would be MOST effective against tailgating?

* **Fences**
* **Turnstiles**

* **Barriers**
* **Locks**

**Explanation**

Turnstiles are designed to allow only one person through at a time, making them the most effective physical access control against tailgating. Tailgating occurs when an unauthorized person follows an authorized person into a secured area.

For example, consider a secure corporate office that uses a turnstile at the main entrance. Each employee has a unique badge. When the card is swiped, the turnstile allows one person through. If another person tries to follow (or bypass) without swiping the card, the turnstile remains locked, effectively preventing unauthorized access.

The other options are not as effective against tailgating. Fences and barriers are wrong because while they can restrict access to an area, they do not prevent tailgating once an authorized person opens a gate or barrier. Locks are also incorrect because, like fences and barriers, they can secure an area but do not prevent tailgating. Once an authorized person unlocks a door, an unauthorized person can easily follow them inside.

Bottom of Form

Top of Form

Question 27:

In which of the following phases of an Incident Recovery Plan are incident responses prioritized?

* **Contentment, Eradication, and Recovery**
* **Detection and Analysis**

* **Post-incident Activity**
* **Preparation**

**Explanation**

Incident responses are prioritized in the Detection and Analysis phase (see the ISC2 Study Guide, Chapter 2, Module 1, under Components of Incident Response).

Bottom of Form

Top of Form

Question 28:

What does SIEM mean?

* **Security Information and Event Manager**

* **Security Information and Enterprise Manager**
* **System Information and Enterprise Manager**
* **System Information and Event Manager**

**Explanation**

Security Information and Event Management (SIEM) is software for aggregating logs and events from applications, servers, network equipment, and specialized security equipment such as firewalls or Intrusion Prevention systems (IPS). SIEM offers a unified view of security-related data, and is capable of identifying deviations to the regular operation of systems that are often symptoms of attacks. The remaining options do not refer to any common term in Cybersecurity.

Bottom of Form

Top of Form

Question 29:

According to the canon "Provide diligent and competent service to principals", (ISC)² professionals are to:

* **Take care not to tarnish the reputation of other professionals through malice or indifference**
* **Treat all members fairly and,when resolving conflicts, consider public safety and duties to principals, individuals and the profession, in that order**
* **Promote the understanding and acceptance of prudent information security measures**
* **Avoid apparent or actual conflicts of interest**

**Explanation**

The direction for applying the ethical principles of ISC2 states that avoiding conflicts of interest or the appearance thereof is a consequence of providing diligent and competent service to principals (see https://resources.infosecinstitute.com/certification/the-isc2-code-of-ethics-a-binding-requirement-for-certification/). The other options are consequences of the remaining three ethical principles.

Bottom of Form

Top of Form

Question 30:

A device found not to comply with the security baseline should be:

* **Disabled or separated into a quarantine area until a virus scan can be run**
* **Placed in a demilitarized zone (DMZ) until it can be reviewed and updated**
* **Marked as potentially vulnerable and placed in a quarantine area**
* **Disabled or isolated into a quarantine area until it can be checked and updated**

**Explanation**

Security baselines are used to guarantee that network devices, software, hardware and endpoints are configured consistently. Baselines ensure that all such devices comply with the security baseline set by the organization. Whenever a device is found not compliant with the security baseline, it may be disabled or isolated into a quarantine area until it can be checked and updated (see ISC2 Study Guide, chapter 5, module 2, under Configuration Management Overview). A DMZ is a protected boundary network between external and internal networks. Systems accessible directly from the Internet are permanently connected in this network, where they are protected by a firewall; however, a DMZ is not a quarantine area used to temporarily isolate devices.

Bottom of Form

Top of Form

Question 31:

Which of the following areas is connected to PII?

* **Integrity**
* **Non-repudiation**
* **Authentication**
* **Confidentiality**

**Explanation**

Confidentiality is the most distinctive property of personally identifiable information (see ISC2 Study Guide, Module 1, under CIA Deep Dive). The remaining options apply to all types of data. All data requires integrity to be usable. Non-repudiation refers to the inability to deny the production, approval, or transmission of information. Authentication refers to the access to information.

For example, encrypting a customer's personal information in a company's database ensures that even if unauthorized access is gained, the PII remains confidential and indecipherable to the intruder.

Authentication is incorrect because it refers to the process of verifying the identity of a user or device, typically before granting access to resources, but does not directly address the protection of PII itself. Non-repudiation, which ensures that a party to a transaction cannot deny the authenticity of their signature on a document or the sending of a message they created, is more about ensuring the integrity and provenance of data than it is about protecting PII. Integrity, while important for ensuring that PII has not been altered or tampered with, focuses on the accuracy and completeness of data rather than its confidentiality.

Bottom of Form

Top of Form

Question 32:

A web server that accepts requests from external clients should be placed in which network?

* **DMZ**

* **Intranet**
* **Internal Network**
* **VPN**

**Explanation**

In Cybersecurity, a DMZ (demilitarized zone) is a physical or logical subnetwork that contains and exposes external-facing services (such as web services). An Internal Network is an organization-controlled network that is isolated from external access. An Intranet is itself an internal network that supports similar protocols and services to the Internet, but only for the organization's internal use. A Virtual Private Network (VPN) creates a secure tunnel between endpoints (whether between networks, or between networks and devices), allowing traffic to travel through a public network and creating the illusion that endpoints are connected through a dedicated private connection.

Bottom of Form

Top of Form

Question 33:

Which of the following is NOT an example of a physical security control?

* **Firewalls**

* **Biometric access controls**
* **Security cameras**
* **Remote control electronic locks**

**Explanation**

Firewalls are a type of electronic equipment which connects to a network that filters inbound traffic arriving from the Internet, and, thus are a type of technical security controls. Security cameras, biometric access control and electronic locks, though connected to a network, control access to physical facilities, and thus are types of physical security controls. (ISC2 Study Guide, Chapter 1, Module 3)

Bottom of Form

Top of Form

Question 34:

Which access control model specifies access to an object based on the subject's role in the organization?

* **MAC**
* **ABAC**
* **RBAC**

* **DAC**

**Explanation**

The role-based access control (RBAC) model is well known for governing access to objects based on the roles of individual users within the organization. Mandatory access control is based on security classifications. Attribute-based access control is based on complex attribute rules. In discretionary access control, subjects can grant privileges to other subjects and change some of the security attributes of the objects they have access to.

Bottom of Form

Top of Form

Question 35:

After an earthquake disrupting business operations, which document contains the procedures required to return business to normal operation?

* **The Business Continuity Plan**
* **The Business Impact Analysis**
* **The Business Impact Plan**
* **The Disaster Recovery Plan**

**Explanation**

A Disaster Recovery Plan (DRP) is a plan for processing and restoring operations in the event of a significant hardware or software failure, or of the destruction of the organization's facilities. The primary goal of a DRP is to restore the business to the last-known reliable state of operations (see Chapter 2 ISC2 Study Guide, module 4, under The Goal of Disaster Recovery). The term 'Business Impact Plan' does not exist. A Business Continuity Plan (BCP) is a pre-determined set of instructions describing how an organization's mission/business processes will be sustained during and after a significant disruption. A Business Impact Analysis (BIA) is a technique for analyzing how disruptions can affect an organization.

Bottom of Form

Top of Form

Question 36:

Which of the following is NOT an element of System Security Configuration Management?

* **Baselines**
* **Inventory**
* **Updates**
* **Audit logs**

**Explanation**

System Security Configuration Management elements are inventories, baselines, updates and patches. Audit logs can be generated after 'Verification and Audit'. However, 'Verification and Audit' is a configuration management procedure, and not a configuration management element (see ISC2 Study Guide, chapter 5, module 2, under Chapter Resource).

Bottom of Form

Top of Form

Question 37:

According to (ISC)², which are the six phases of data handling?

* **Create →  Use → Store → Share →  Archive → Destroy**
* **Create → Store → Use → Share → Archive → Destroy**

* **Create → Share →  Store → Use → Archive → Destroy**
* **Create → Share → Use → Store → Archive → Destroy**

**Explanation**

According to the data security lifecycle model, the six phases of data security lifecycle model are Create -> Store -> Use -> Share -> Archive -> Destroy (see ISC2 Study Guide, chapter 5, module 1 under data handling).

Bottom of Form

Top of Form

Question 38:

In the event of a disaster, what should be the primary objective? (★)

* **Application of disaster communication**
* **Protection of the production database**
* **Guarantee the continuity of critical systems**
* **Guarantee the safety of people**

**Explanation**

In the event of a disaster, the primary objective should always be to ensure the safety of people (see ISC2 Study Guide, Chapter 2, Module 1). Human life is the most valuable asset, and ensuring the safety of everyone involved should always be the first priority. For example, in the event of a fire in a data center, the first step should be to evacuate all personnel to a safe location before attempting to salvage any equipment or data.

While deploying disaster communications, protecting the production database, and ensuring the continuity of critical systems are important aspects of disaster recovery and business continuity, they are secondary to the safety of people. These tasks focus on minimizing the impact of the disaster on the organization's operations and should be addressed only after the safety of all individuals has been ensured.

Bottom of Form

Top of Form

Question 39:

Which regulations address data protection and privacy in Europe?

* **HIPAA**
* **GDPR**

* **SOX**
* **FISMA**

**Explanation**

The General Data Protection Regulation (GDPR) is the official EU regulation for data protection and privacy. The remaining three options only apply to the United States. The Federal Information Security Management Act (FISMA) contains guidelines and security standards that protect government information and operations in the United States. The Sarbanes–Oxley (SOx) Act of 2002 is a United States federal law that mandates and regulates financial record-keeping and reporting practices for corporations. The Health Insurance Portability and Accountability Act (HIPAA) is a United States federal law that establishes national standards to protect sensitive patient health information from being disclosed without the patient's knowledge and permission.

Bottom of Form

Top of Form

Question 40:

Which of the following documents contains elements that are NOT mandatory?

* **Procedures**
* **Policies**
* **Regulations**
* **Guidelines**

**Explanation**

Only guidelines contain elements that may not be mandatory. Compliance with policies, procedures and regulations is mandatory (see ISC2 Study Guide Chapter 1, Module 4).

Bottom of Form

Top of Form

Question 41:

What is the consequence of a Denial of Service attack?

* **Increase in the availability of resources**
* **Malware Infection**
* **Exhaustion of device resources**

* **Remote control of a device**

**Explanation**

A denial of service attack (DoS) consists in a malicious overload of requests which will eventually lead to the exhaustion of resources, rendering the service unavailable, as well as causing the activation of safety mechanisms that delay or limit the availability of that system or service. This type of attack seeks to compromise service availability, but not to control a device nor to install malware.

Bottom of Form

Top of Form

Question 42:

Which of the following areas is the most distinctive property of PHI?

* **Authentication**
* **Non-repudiation**
* **Confidentiality**

* **Integrity**

**Explanation**

Confidentiality is the most distinctive property of protected health information (see ISC2 Study Guide, Module 1, under CIA Deep Dive). The remaining options apply to all types of data. All data requires integrity to be usable. Non-repudiation refers to the inability to deny the production, approval, or transmission of information. Authentication refers to guaranteeing that systems and information are accessed by persons and systems that are who they claim to be.

For example, a patient's medical records are encrypted and access is tightly controlled to ensure that only authorized healthcare providers who need to know the information for treatment purposes can view it.

Authentication is incorrect because it refers to the process of verifying the identity of a user or device, which is not specific to protecting PHI. Integrity, while important, focuses on ensuring that the information is accurate and has not been tampered with, not on its confidentiality. Non-repudiation ensures that a party cannot deny the authenticity of its actions, which is more relevant to transactional integrity and accountability than to health information privacy.

Bottom of Form

Top of Form

Question 43:

Which access control is more effective at protecting a door against unauthorized access?

* **Fences**
* **Turnstiles**
* **Locks**

* **Barriers**

**Explanation**

A lock is a device that prevents a physical structure (typically a door) from being opened, indicating that only the authorized person (i.e. the person with the key) can open it. A fence or a barrier will prevent ALL access. Turnstiles are physical barriers that can be easily overcome (after all, it is common knowledge that intruders can easily jump over a turnstile when no one is watching).

Bottom of Form

Top of Form

Question 44:

The detailed steps to complete tasks supporting departmental or organizational policies are typically documented in:

* **Standards**
* **Regulations**
* **Policies**
* **Procedures**

**Explanation**

Policies are high-level documents that frame all ongoing activities of an organization to ensure that it complies with industry standards and regulations. Regulations are usually devised by governments. Standards are created by governing or professional bodies to support regulations. Both regulations and standards are created outside of the organization (see ISC2 Study Guide Chapter 1, Module 4).

Bottom of Form

Top of Form

Question 45:

Which of the following principles aims primarily at fraud detection?

* **Separation of Duties**

* **Privileged Accounts**
* **Least Privilege**
* **Defense in Depth**

**Explanation**

According to the principle of Separation of Duties, operations on objects are to be segmented (often referred to as 'transactions'), requiring distinct users and authorizations. The involvement of multiple users guarantees that no single user can perpetrate and conceal errors or fraud in their duties. To the extent that users have to review the work of other users, Separation of Duties can also be considered a mechanism of fraud detection (see ISC2 Study Guide Chapter 1, Module 3). The principle of Least Privilege states that subjects should be given only those privileges required to complete their specific tasks. The principle of Privileged Accounts refers to the existence of accounts with permissions beyond those of regular users. Finally, the principle of Defense in Depth endorses the use of multiple layers of security for holistic protection.

Bottom of Form

Top of Form

Question 46:

In order to find out whether personal tablet devices are allowed in the office, which of the following policies would be helpful to read?

* **AUP**
* **Change Management Policy**
* **BYOD**

* **Privacy Policy**

**Explanation**

The Bring Your Own Device (BYOD) policy establishes rules for using personal devices for work-related activities. The Acceptable Use Policy (AUP) defines the permissions and limitations that users must agree to while accessing the network and using computer systems or any other organizational resources. The Privacy Policy (PP) outlines the data security mechanisms that protect customer data. In the context of Cybersecurity, a Change Management Policy (CMP) establishes the use of standardized methods to enable IT and process change while minimizing the disruption of services, reducing back-out, and ensuring clear communication with all of the stakeholders in the organization.

Bottom of Form

Top of Form

Question 47:

An entity that acts to exploit a target organization’s system vulnerabilities is a:

* **Attacker**
* **Threat Actor**

* **Threat**
* **Threat Vector**

**Explanation**

A Threat Actor is defined as an individual or a group posing a threat (according to NIST SP 800-150 under Threat Actor). A Threat Vector is a means by which a Threat Actor gains access to systems (for example: phishing, trojans, baiting, etc.). An Attacker is always an individual, but a Threat Actor can be either a group or an entity. A Threat is a circumstance or event that can adversely impact organizational operations that a Threat Actor can potentially explore through a Threat Vector.

Bottom of Form

Top of Form

Question 48:

Which of the following cloud models allows access to fundamental computer resources? (★)

* **PaaS**
* **SaaS**
* **FaaS**
* **IaaS**

**Explanation**

Infrastructure as a Service (IaaS) provides the capability to provision processing, storage, networks, and other fundamental computing resources. Platform as a Service (PaaS) enables the provisioning of applications, programming libraries, services, and tools that the provider supports. Unlike IaaS, consumers do not control their underlying cloud infrastructure (including operating systems and storage). Both Software as a Service (SaaS) and Function as a Service (FaaS) models abstract away from underlying computing infrastructure, thereby allowing providers to focus on providing end users with applications, rather than worrying about how their underlying infrastructure functions.

Bottom of Form

Top of Form

Question 49:

Malicious emails that aim to attack company executives are an example of:

* **Whaling**

* **Trojans**
* **Phishing**
* **Rootkits**

**Explanation**

Phishing is a digital social engineering attack that uses authentic-looking (but counterfeit) e-mail messages to request information from users, or to get them to unknowingly execute an action that will make way for the attacker. Whaling attacks are phishing attacks that target high-ranking members of organizations. After gaining root-level access to a host, rootkits are used by an attacker to conceal malicious activities while keeping root-level access. Trojans are a type of software that appears legitimate but has hidden malicious functions that evade security mechanisms.

Bottom of Form

Top of Form

Question 50:

Which of the following is a detection control?

* **Bollards**
* **Firewalls**
* **Turnstiles**
* **Smoke sensors**

**Explanation**

By definition, smoke detectors are fire protection devices employed for the early detection of fire. Firewalls are devices that filter incoming traffic, and are a type of logical preventive control. Bollards and turnstiles are types of physical preventive controls.

Bottom of Form

Top of Form

Question 51:

Which of the following is an example of 2FA?

* **One-Time passwords (OTA)**

* **Badges**
* **Passwords**
* **Keys**

**Explanation**

One-time passwords are typically generated by a device (i.e. "something you have") and are required in addition to the actual main password (i.e. "something you know"). Badges, keys and passwords with no other overlapping authentication controls are considered single-factor (and thus are not 2FA).

Bottom of Form

Top of Form

Question 52:

In which cloud model does the cloud customer have LESS responsibility over the infrastructure? (★)

* **SaaS**

* **FaaS**
* **PaaS**
* **IaaS**

**Explanation**

In Software as a Service (SaaS), consumers may control user-specific application configuration settings, but neither the underlying application logic nor the infrastructure. In the Function as a Service (FaaS) model, cloud customers deploy application-level functionality (typically as microservices) and are charged only when this functionality is executed. In Platform as a Service (PaaS), the cloud customer does not manage or control the underlying cloud infrastructure (wnich includes the network, servers, operating systems, and storage) but has control over the deployed applications and libraries. The Infrastructure as a Service (IaaS) model provides customers with fundamental computing resources (such as processing, storage, or networks) where the consumer is able to deploy and run arbitrary software,and also to choose the operating system.

Bottom of Form

Top of Form

Question 53:

Which of the following canons is found in the (ISC)² code of ethics?

* **Provide diligent and competent service to principals**

* **Protect society, the common good, and the infrastructure**
* **Act honorably, honestly, safely and legally**
* **Advance and promote the profession**

**Explanation**

Only "Provide diligent and competent service to principals" contains the accurate text of the ISC2 code of ethics. Although a security professional should discourage unsafe practices, no direct reference to acting safely exists in the canons. Aside from society, the common good and infrastructure, security professionals are expected to protect public trust and confidence. Finally, they are expected to protect the profession, and not just advance and promote it.

Bottom of Form

Top of Form

Question 54:

In which of the following access control models can the creator of an object delegate permission?

* **MAC**
* **ABAC**
* **DAC**

* **RBAC**

**Explanation**

In a Discretionary Access control model, the permissions associated with each object (file or data) are set by the owner of the object. In this model, the creator of an object implicitly becomes its owner, and therefore can decide who will have permission over the objects. In the remaining models, access specifications are centrally determined.

Bottom of Form

Top of Form

Question 55:

Which of the following properties is NOT guaranteed by Digital Signatures?

* **Authentication**
* **Integrity**
* **Non-repudiation**
* **Confidentiality**

**Explanation**

A digital signature is the result of a cryptographic transformation of data that is useful for providing: authentication of data origin, data integrity, and non-repudiation of the signer. However, digital signatures cannot guarantee confidentiality (i.e., the property that data or information will not be made available or disclosed).

For example, when a document is digitally signed, anyone with the public key can verify the signature, but the content of the document is not encrypted by the digital signature itself. If confidentiality is required, the document must be separately encrypted.

Integrity is incorrect because digital signatures ensure the integrity of a message by allowing the recipient to detect any changes to the content of the message after it has been signed. Non-repudiation, also incorrect, because digital signatures prevent the sender from denying the authenticity of the signed message. Authentication, incorrect because digital signatures authenticate the identity of the sender by linking them to the document or message they signed.

Bottom of Form

Top of Form

Question 56:

Which of these would be the best option if a network administrator needs to control access to a network?

* **IDS**
* **NAC**

* **HIDS**
* **SIEM**

**Explanation**

Network Access Control (NAC) refers to a class of mechanisms that prevent access to a network until a user (or the user's device) either presents the relevant credentials, or passes the results of health checks performed on the client device. Security Information and Event Management (SIEM), Host Intrusion Detection Systems (HIDS), and Intrusion Detection Systems (IDS) are all monitoring systems.

Bottom of Form

Top of Form

Question 57:

An exploitable weakness or flaw in a system or component is a:

* **Risk**
* **Vulnerability**

* **Threat**
* **Bug**

**Explanation**

A Vulnerability is a weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a Threat source (NIST SP 800-30 Rev 1). The Threat is the circumstance or event that can adversely impact operations. A Risk is a possible event that can negatively impact the organization. A Bug is a flaw causing an application to produce an unintended or unexpected result that may be exploitable.

Bottom of Form

Top of Form

Question 58:

Which of the following Cybersecurity concepts guarantees that information is accessible only to those authorized to access it?

* **Non-repudiation**
* **Confidentiality**

* **Authentication**
* **Accessibility**

**Explanation**

Confidentiality, Integrity and Availability are known as the CIA triad, from the model that guides policies for information security. Confidentiality is the property of data or information not being made available or disclosed, which leads to sensitive information being protected from unauthorized access.

For example, in a corporate environment, personal employee information is stored in a secure database. Access controls are implemented to ensure that only authorized HR personnel can access this information, thereby maintaining its confidentiality.

Integrity refers to the preservation of the consistency, accuracy and trustworthiness of data. Availability is the property of data being consistently and readily accessible to the parties authorized to access it. Finally, non-repudiation refers to the inability to deny the production, approval or transmission of information.

Bottom of Form

Top of Form

Question 59:

The last phase in the data security cycle is:

* **Backup**
* **Encryption**
* **Destruction**

* **Archival**

**Explanation**

According to the data security lifecycle model, the last phase is Data Destruction, which aims at guaranteeing that data contained in a given support is erased and destroyed in a way that renders it completely irrecoverable by any means (see ISC2 Study Guide, chapter 5, module 1, under Data Handling). Archival refers to the process whereby an organization creates a long-term data archive for compliance, storage reduction or business intelligence. A Backup is a copy of files and programs created to facilitate recovery. Encryption is the cryptographic transformation of data with the purpose of concealing its original meaning, and is not a phase of the data security lifecycle.

Bottom of Form

Top of Form

Question 60:

Which are the components of an incident response plan?

* **Preparation → Detection and Analysis → Containment, Eradication and Recovery → Post-Incident Activity**

* **Preparation → Detection and Analysis → Eradication → Recovery → Containment → Post-Incident Activity**
* **Preparation → Detection and Analysis → Recovery → Containment → Eradication → Post-Incident Activity**
* **Preparation → Detection and Analysis →  Containment → Eradication → Post-Incident Activity → Recovery**

**Explanation**

The components commonly found in an incident response plan are (in this order): Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-Incident Activity (see the ISC2 Chapter 2, Module 1, under Components of an Incident Response Plan).

Bottom of Form

Top of Form

Question 61:

Which access control model can grant access to a given object based on complex rules?

* **RBAC**
* **ABAC**

* **DAC**
* **MAC**

**Explanation**

ABAC is an access control model that controls access to objects using rules that are evaluated according to the attributes of the subject, relevant objects, and attributes of the environment and action. The RBAC and MAC models are based on more straightforward and relatively less flexible rule systems, which are evaluated according to subject roles and security classifications. The rules that can be specified in a DAC model are even simpler than those of the previous two models

Bottom of Form

Top of Form

Question 62:

With respect to risk management, which of the following options should be prioritized?

* **The expected probability of occurrence is high, and the potential impact is low**
* **The frequency of occurrence is low, and the expected impact value is high**

* **The expected probability of occurrence is low, and the potential impact is low**
* **The frequency of occurrence is high, and the expected impact value is low**

**Explanation**

The highest priority should be given to risks estimated to high impact and low probability over high probability and low impact value (ISC2 Study Guide, Chapter 1, Module 2). In qualitative risk analysis, the 'expected probability of occurrence' and the 'frequency of occurrence' refer to the same thing. The same goes for the concepts of expected impact value (NIST SP 800-30 Rev. 1 under Impact Value) and potential impact (NIST SP 800-60 Vol. 1 Rev. 1 under Potential Impact).

Bottom of Form

Top of Form

Question 63:

Which type of attack will most effectively provide privileged access (root access in Unix/Linux platforms) to a computer while hiding its presence?

* **Phishing**
* **Trojans**
* **Cross-Site Scripting**
* **Rootkits**

**Explanation**

A rootkit tries to maintain root-level access while concealing malicious activity. It typically creates a backdoor and attempts to remain undetected by anti-malware software. A rootkit is active while the system is running. Trojans can also create backdoors but are only active while a specific application is running, and thus are not as effective as a rootkit. Phishing is used to initiate attacks by redirecting the user to fake websites. Cross-Site Scripting is used to attack websites.

Bottom of Form

Top of Form

Question 64:

Which of the following is NOT a protocol of the OSI Level 3?

* **IGMP**
* **IP**
* **ICMP**
* **SNMP**

**Explanation**

Internet Protocol (IP) is known to be a level 3 protocol. Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) are also level 3 protocols. Simple Network Management Protocol (SNMP) is a protocol used to configure and monitor devices attached to networks. It is an application-level protocol (level 7), and therefore the only option that is not from level 3.

Bottom of Form

Top of Form

Question 65:

Logging and monitoring systems are essential to:

* **Identifying efficient performing systems, labeling compromises, and providing a record of how systems are used**
* **Identifying efficient performing systems, detecting compromises, and providing a record of how systems are used**
* **Identifying inefficient performing systems, detecting compromises, and providing a record of how systems are used**

* **Identifying inefficient performing systems, preventing compromises, and providing a record of how systems are used**

**Explanation**

According to the ISC2 Study Guide (chapter 5, module 1, under Data Handling Practices), logging and monitoring systems are characterized as being "Essential to identifying inefficient performing systems, detecting compromises, and providing a record of how systems are used". The remaining options are incorrect variations of this definition.

Bottom of Form

Top of Form

Question 66:

Which tool is commonly used to sniff network traffic? (★)

* **Wireshark**

* **Nslookup**
* **Burp Suite**
* **John the Ripper**

**Explanation**

Wireshark is the world's most widely-used and complete network protocol analyzer that, informally speaking, is the "microscope" of network traffic. John the Ripper is a famous Open Source password security auditing and password recovery tool. Nslookup is a network administration command-line tool for querying the Domain Name System that obtains the mapping between the domain name, IP address, or other DNS records. Finally, Burp Suite is a set of well-known vulnerability scanning, penetration testing, and web app security tools.

Bottom of Form

Top of Form

Question 67:

The cloud deployment model where a company has resources on-premise and in the cloud is known as:

* **Hybrid cloud**

* **Community cloud**
* **Private cloud**
* **Multi-tenant**

**Explanation**

A hybrid cloud is a model that combines (i.e. orchestrates) on-premise infrastructure, private cloud services, and a public cloud to handle storage and service. A community cloud is an infrastructure where multiple organizations share resources and services based on common technological and regulatory necessities. Multi-tenancy refers to a context where several of a cloud vendor's customers share the same computing resources. A private cloud is a cloud computing model where the cloud infrastructure is dedicated to a single organization.

Bottom of Form

Top of Form

Question 68:

Which of these is the most efficient and effective way to test a business continuity plan?

* **Walkthroughs**
* **Discussions**
* **Reviews**
* **Simulations**

**Explanation**

Simulations are full re-enactments of business continuity procedures and can involve most, if not all, of your workforce. They also tend to take place on-site in the relevant business areas. Thus, they are an exceptionally effective way to test your business continuity plan. Walkthroughs verbally carry out specific recovery steps stipulated in the business Continuity plan. Discussion and reviews are static ways of testing the business continuity plan.

Bottom of Form

Top of Form

Question 69:

Risk Management is:

* **The identification, evaluation and prioritization of risks**

* **The creation of an incident response team**
* **The assessment of the potential impact of a threat**
* **The impact and likelihood of a threat**

**Explanation**

Risk Management is the process of identifying, assessing and mitigating risks (ISC2 Study Guide, chapter 1, module 2). "Impact and likelihood of a threat" is a definition of risk. "Creating an incident response team" and "assessing the potential impact of a threat" can be considered Risk Management actions, but are not in themselves Risk Management.

Bottom of Form

Top of Form

Question 70:

When a company hires an insurance company to mitigate risk, which risk management technique is being applied?

* **Risk tolerance**
* **Risk avoidance**
* **Risk transfer**

* **Risk mitigation**

**Explanation**

Risk transfer is a risk management strategy that contractually shifts a pure risk from one party to another (in this case, to an insurance company). Risk avoidance consists in stopping activities and exposures that can negatively affect an organization and its assets. Risk mitigation consists of mechanisms to reduce the risk. Finally, risk tolerance is the degree of risk that an investor is willing to endure.

Bottom of Form

Top of Form

Question 71:

Which of these is NOT a change management component?

* **Governance**

* **Approval**
* **RFC**
* **Rollback**

**Explanation**

All significant change management practices address typical core activities: Request For Change (RFC), Approval, and Rollback (see ISC2 Study Guide, chapter 5, module 3). Governance is not one of these practices.

Bottom of Form

Top of Form

Question 72:

The predetermined set of instructions or procedures to sustain business operations after a disaster is commonly known as:

* **Disaster Recovery Plan**
* **Business Impact Plan**
* **Business Impact Analysis**
* **Business Continuity Plan**

**Explanation**

A Business Continuity Plan (BCP) is a pre-determined set of instructions describing how an organization's mission/business processes will be sustained during and after a significant disruption (see Chapter 2 ISC2 Study Guide, module 4, under Terms and Definitions). A Business Impact Analysis (BIA) is a technique for analyzing how disruptions can affect an organization. A Disaster Recovery Plan is a written plan for recovering information systems in response to a major failure or disaster. The term 'Business Impact Plan' does not exist.

Bottom of Form

Top of Form

Question 73:

The SMTP protocol operates at OSI Level:

* **25**
* **7**

* **23**
* **3**

**Explanation**

Simple Mail Transport Protocol (SNMP) is an application layer protocol that operates at level 7. Level 3 corresponds to the network layer. There are no OSI layers above level 7. The number 25 presumably refers to the TCP/IP port of the SMTP protocol. The number 23, in turn, refers to the TCP/IP port of the Telnet protocol.

Bottom of Form

Top of Form

Question 74:

Which devices would be more effective in detecting an intrusion into a network?

* **HIDS**
* **Firewalls**
* **Routers**
* **NIDS**

**Explanation**

Network intrusion detection systems (NIDS) are network devices that detect malicious traffic on a network. Host intrusion detection systems (HIDS) are applications that monitor computer systems for intrusion. Typically, HIDS are not concerned with network devices. A firewall is a device that filters incoming Internet traffic. Routers receive and forward traffic, but (typically) do not analyze it.

Bottom of Form

Top of Form

Question 75:

Which devices have the PRIMARY objective of collecting and analyzing security events?

* **Hubs**
* **SIEM**

* **Routers**
* **Firewalls**

**Explanation**

A Security Information and Event Management (SIEM) system is an application that gathers security data from information system components and presents actionable information through a unified interface. Routers and Hubs aim to receive and forward traffic. Firewalls filter incoming traffic. Neither of these last three options aims at collecting and analyzing security events.

Bottom of Form

Top of Form

Question 76:

Which of the following is a public IP?

* **10.221.123.1**
* **172.16.123.1**
* **192.168.123.1**
* **13.16.123.1**

**Explanation**

The ranges of IP addresses 10.0.0.0 to 10.255.255.254, 172.16.0.0 to 172.31.255.254, and 192.168.0.0 to 192.168.255.254 are reserved for private use (see ISC2 Study Guide, chapter 4, module 1, under Internet Protocol - IPv4 and IPv6). Therefore, the IP address 13.16.123.1 is the only address in a public range.

Bottom of Form

Top of Form

Question 77:

What type of security control is the biometric reader that grants access to the data center building?

* **Technical Control**
* **Physical Control**

* **Authorization Control**
* **Administrative Control**

**Explanation**

Physical controls have to do with the architectural features of buildings and facilities. Administrative controls are connected to the actions of people within the organization. Technical controls are implemented inside of computer systems. Authorization controls relate to the assets to which a user is granted access inside a particular computer system (see ISC2 Study Guide Chapter 1, Module 3).

Bottom of Form

Top of Form

Question 78:

Which type of attack PRIMARILY aims to make a resource inaccessible to its intended users?

* **Denial of Service**

* **Phishing**
* **Cross-Site Scripting**
* **Trojans**

**Explanation**

A denial of service attack (DoS) consists in compromising the availability of a system or service through a malicious overload of requests, which causes the activation of safety mechanisms that delay or limit the availability of that system or service. Due to this, systems or services are rendered inaccessible to their intended users. Trojans, phishing, and cross-site scripting attacks try to covertly gain access to the system or data, and therefore do not primarily aim at compromising the system's availability.

Bottom of Form

Top of Form

Question 79:

The address 8be2:4382:8d84:7ce2:ec0f:3908:d29a:903a is an:

* **IPv6 address**

* **IPv4 address**
* **Mac address**
* **Web address**

**Explanation**

An IPv6 address is a 128-bit address represented as a sequence of eight groups of 16-bit hexadecimal values. An IPv4 address is a 32-bit address represented as a sequence of four 8-bit integers. A Mac address is a 48-bit address represented as six groups of 8 bits values in hexadecimal. A web address consists of a protocol name, a server address, and a resource path (see ISC2 Study Guide, chapter 4, module 1 - Understand Computer Networking).

Bottom of Form

Top of Form

Question 80:

Which type of attack embeds malicious payload inside a reputable or trusted software?

* **Cross-Site Scripting**
* **Rootkits**
* **Phishing**
* **Trojans**

**Explanation**

Trojans are a type of software that appears legitimate but has hidden malicious functions that evade security mechanisms, typically by exploiting legitimate authorizations of the user that invokes the program. Rootkits try to maintain privilege-level access while concealing malicious activity. They often replace system files, so they are activated when the system is restarted. Trojans often install Rootkits, but Rootkits are not the Trojans themselves). Phishing typically tries to redirect the user to another website. Cross-site scripting attempts to inject malicious executable code into a website.

Bottom of Form

Top of Form

Question 81:

Which of the following is LESS likely to be part of an Incident Response Team (IRT)?

* **Human Resources**

* **Information security professionals**
* **Legal representatives**
* **Representatives of senior management**

**Explanation**

The incident response team carries out the post-incident analysis phase of an incident response plan. They are a cross-functional group of individuals representing the management, technical and functional areas of responsibility most directly impacted by a security incident. In the incident response team, we typically find (i) representatives of senior management, (ii) information security professionals, (iii) legal representatives, (iv) public affairs/communications representatives, (v) engineering representatives (both system and network); however, we don't typically find human resource representatives (see the ISC2 Study Guide Chapter 2, Module 1, under Incident Response Team).

Bottom of Form

Top of Form

Question 82:

Which of the following is NOT a feature of a cryptographic hash function?

* **Reversible**

* **Unique**
* **Useful**
* **Deterministic**

**Explanation**

A cryptographic hash function should be unique, deterministic, useful, tamper-evident (also referred to as 'the avalanche effect' or 'integrity assurance') and non-reversible (also referred to as 'one-way'). Nonreversible means it is impossible to reverse the hash function to derive the original text of a message from its hash output value (see ISC2 Study Guide, chapter 5, module 1, under Encryption Overview). Thus, the 'reversible' feature is not a feature of a hash function.

Bottom of Form

Top of Form

Question 83:

Which of the following are NOT types of security controls?

* **Storage controls**

* **System-specific controls**
* **Common controls**
* **Hybrid controls**

**Explanation**

Storage controls are not a type of security control. Security controls are safeguards or countermeasures that an organization can employ to avoid, counteract or minimize security risks. System-specific controls are security controls that provide security capability for only one specific information system. Common controls are security controls that provide security capability for multiple information systems. Hybrid controls have characteristics of both system-specific and common controls.

Bottom of Form

Top of Form

Question 84:

Which of these is not an attack against an IP network?

* **Oversized Packet Attack**
* **Side-channel Attack**

* **Fragmented Packet Attack**
* **Man-in-the-middle Attack**

**Explanation**

Man-in-the-middle Attacks, Oversized Packet Attacks, and Fragmented Packet Attacks are typical IP network attacks (see ISC2 Study Guide, Chapter 4, Module 1, under Security of the Network). Side Channel Attacks are non-invasive attacks that extract information from devices (typically devices running cryptographic algorithms), and therefore do not aim at IP networks.

Bottom of Form

Top of Form

Question 85:

Which of the following is NOT a social engineering technique? (★)

* **Segregation**

* **Quid pro quo**
* **Baiting**
* **Pretexting**

**Explanation**

In cybersecurity, 'segregation', or 'segregation of duties' (SoD), is a security principle designed to prevent fraud or error by dividing tasks among multiple persons.It is an administrative control that reduces the risk of potential errors or fraud from a single person having control over all aspects of a critical process.

The remaining options are valid social engineering techniques. Baiting is a social engineering attack in which a scammer uses a false promise to lure a victim. Pretexting is a social engineering technique that manipulates victims into revealing information. Quid pro quo is a social engineering attack (technically a combination of baiting and pretexting) that promises users a benefit in exchange for information (that can later be used to gain control of a user's account or sensitive information).

Bottom of Form

Top of Form

Question 86:

Which are the three packets used on the TCP connection handshake? (★)

* **SYN → ACK → FIN**
* **Discover → Offer → Request**
* **SYN → SYN/ACK → ACK**

* **Offer → Request → ACK**

**Explanation**

TCP uses a three-way handshake to establish a reliable connection by exchanging three packets with the SYN, SYN/ACK and ACK flags. Although SYN, ACK and FIN are valid TCP packet flags, the sequence SYN → ACK → FIN is not the TCP handshake. Both the sequences Discover → Offer → Request and Offer → Request → ACK are used in DHCP (but are still incomplete, since DHCP is a four-way handshake).

Bottom of Form

Top of Form

Question 87:

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

* **Acceptable Use Policies**

* **Access Control Lists**
* **No entry signs**
* **Badge Readers**

**Explanation**

Policies are a type of administrative security controls. An access control list is a type of technical security control. A badge reader and a 'No entry' sign are types of physical security controls (see ISC2 Study Guide, Chapter 1, Module 3).

Bottom of Form

Top of Form

Question 88:

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

* **Fences**
* **Turnstiles**
* **Bollards**
* **Access control lists**

**Explanation**

An access control list is a type of technical security control. Bollards, fences and turnstiles control access to physical facilities, and thus are types of physical security controls. (ISC2 Study Guide, Chapter 1, Module 3)

Bottom of Form

Top of Form

Question 89:

Which type of attack attempts to gain information by observing the device's power consumption? (★)

* **Denial of Service**
* **Cross Site Scripting**
* **Side Channels**

* **Trojans**

**Explanation**

A side-channel attack is a passive and non-invasive attack aiming to extract information from a running system, by using special-purpose hardware to perform power monitoring, as well as timing and fault analysis attacks. The remaining are software-based attacks.

Bottom of Form

Top of Form

Question 90:

The Bell and LaPadula access control model is a form of: (★)

* **MAC**

* **DAC**
* **RBAC**
* **ABAC**

**Explanation**

The Bell and LaPadula access control model arranges subjects and objects into security levels and defines access specifications, whereby subjects can only access objects at certain levels based on their security level. Typical access specifications can be things like "Unclassified personnel cannot read data at confidential levels" or "Top-Secret data cannot be written into the files at unclassified levels". Since subjects cannot change access specifications, this model is a form of mandatory access control (MAC). In contrast, Discretionary Access Control (DAC) leaves a certain level of access control to the discretion of the object's owner. The Attribute Based Access Control (ABAC) is based on subject and object attributes (not only classification). Finally, Role Based Access Control (RBAC) is a model for controlling access to objects where permitted actions are identified with roles rather than individual subject identities.

Bottom of Form

Top of Form

Question 91:

Which cloud deployment model is suited to companies with similar needs and concerns?

* **Community cloud**

* **Multi-tenant**
* **Private cloud**
* **Hybrid cloud**

**Explanation**

The correct answer is B. Community cloud deployment models are where several organizations with similar needs and concerns (technological or regulatory) share the infrastructure and resources of a cloud environment. This model is attractive because it is cost-effective while addressing the specific requirements of the participating organizations.

A private cloud is a cloud computing model where the cloud infrastructure is dedicated to a single organization (and never shared with others). A hybrid cloud is a model that combines (i.e. orchestrates) on-premises infrastructure, private cloud services, and a public cloud to handle storage and service. Finally, multitenancy refers to a cloud architecture where multiple cloud tenants (organizations or users) share the same computing resources. Yet, while resources are shared, each tenant's data is isolated and remains invisible to other tenants.

Bottom of Form

Top of Form

Question 92:

Which of the following is a data handling policy procedure?

* **Destroy**

* **Encode**
* **Collect**
* **Transform**

**Explanation**

The data handling procedures are 'Classify', 'Categorize', 'Label', 'Store', 'Encrypt', 'Backup', and 'Destroy' (see ISC2 Study Guide, chapter 5, module 3).

Bottom of Form

Top of Form

Question 93:

How many layers does the OSI model have?

* **4**
* **6**
* **5**
* **7**

**Explanation**

The OSI model organizes communicating systems according to 7 layers: Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer (see Chapter 4 - Module 1 under Open Systems Interconnection).

Bottom of Form

Top of Form

Question 94:

Which of the following is NOT an ethical canon of the (ISC)²?

* **Provide active and qualified service to principal**

* **Protect society, the common good, necessary public trust and confidence, and the infrastructure**
* **Act honorably, honestly, justly, responsibly and legally**
* **Advance and protect the profession**

**Explanation**

In the code of ethics, we read "Provide diligent and competent service to principals", and not "Provide active and qualified service to principals."; all the other options are valid canons of the code of ethics (see ISC2 Study Guide Chapter 1, Module 5).

Bottom of Form

Top of Form

Question 95:

Which device is used to connect a LAN to the Internet?

* **HIDS**
* **Router**

* **SIEM**
* **Firewall**

**Explanation**

A router is a device that acts as a gateway between two or more networks by relaying and directing data packets between them. A firewall is a device that filters traffic coming from the Internet but does not seek to distribute traffic. Neither Security Information and Event Management (SIEM) systems nor Host Intrusion Detection Systems (HIDS) are monitoring devices nor applications that aim at inter-network connectivity.

Bottom of Form

Top of Form

Question 96:

A security safeguard is the same as a:

* **Security control**

* **Privacy control**
* **Safety control**
* **Security principle**

**Explanation**

Security safeguards are approved security measures taken to protect computational resources by eliminating or reducing the risk to a system. These can be measures like hardware and software mechanisms, policies, procedures, and physical controls (see NIST SP 800-28 Version 2, under safeguard). This definition matches the definition of security control as the means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature (see NIST SP 800-160 Vol. 2 Rev. 1 under control).

Bottom of Form

Top of Form

Question 97:

The implementation of Security Controls is a form of:

* **Risk acceptance**
* **Risk transference**
* **Risk avoidance**
* **Risk reduction**

**Explanation**

The implementation of Security Controls involves taking actions to mitigate risk, and thus is a form of risk reduction. Risk acceptance will take no action, risk avoidance will modify operations in order to avoid risk entirely, and risk transference will transfer the risk to another party.

Bottom of Form

Top of Form

Question 98:

Which type of attack has the PRIMARY objective controlling the system from outside?

* **Cross-Site Scripting**
* **Backdoors**

* **Rootkits**
* **Trojans**

**Explanation**

Trojans and Rootkits are often used to install backdoors. A backdoor is a malicious feature that listens for commands on a specific logical port (TCP or UDP) and executes them on the attacked system or device, thereby giving direct control of the system or device to a malicious outside entity (or program). Cross-Site Scripting can execute code with the same permissions as the scripts generated by the target website, compromising the confidentiality and integrity of data transfers between the website and the client.

Bottom of Form

Top of Form

Question 99:

The process that ensures that system changes do not adversely impact business operations is known as:

* **Vulnerability Management**
* **Inventory Management**
* **Configuration Management**
* **Change Management**

**Explanation**

Change Management is the process of implementing necessary changes so that they do not adversely affect business operations (see ISC2 Study Guide, chapter 5, module 3). Vulnerability Management refers to the capacity to identify, track, prioritize and eliminate vulnerabilities in systems and devices. Configuration Management refers to a collection of activities with the purpose of establishing and maintaining the integrity of information systems through their development lifecycle (see NIST SP 1800-16B under Configuration Management). Inventory management refers to the management of keys and/or certificates, so as to monitor their status and owners.

Bottom of Form

Top of Form

Question 100:

In incident terminology, the meaning of Zero Day is:

* **Days without a cybersecurity incident**
* **Days with a cybersecurity incident**
* **A previously unknown system vulnerability**

* **Days to solve a previously unknown system vulnerability**

**Explanation**

A 'Zero Day' is an unknown system vulnerability that can be exploited since it does not yet exist in any vulnerability database. Moreover, these vulnerabilities do not generally fit recognized patterns, signatures or methods (see ISC2 Study Guide Chapter 2, Module 1, under Incident Terminology), making them very hard to detect and prevent.

Bottom of Form