CERTSGURU

ISC2

CC

Certified in Cybersecurity (CC)

QUESTION & ANSWERS

Question: 1

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

A. Web address

B. IPv4 address

C. IPv6 address

D. Mac address

Answer: C

Explanation/Reference:

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).

Question: 2

Which of the following canons is found in the ISC2 code of ethics?

A. Advance and promote the profession

B. Protect society, the common good, and the infrastructure

C. Provide diligent and competent service to principals

D. Act honorably, honestly, safely and legally

Answer: C

Explanation/Reference:

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.

Question: 3

Which of the following is NOT an ethical canon of the ISC2?

A. Advance and protect the profession

B. Protect society, the common good, necessary public trust and confidence, and the infrastructure

C. Act honorably, honestly, justly, responsibly and legally

D. Provide active and qualified service to principal

Answer: D

Explanation/Reference:

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).

Question: 4

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

A. Hybrid cloud

B. Multi-tenant

C. Private cloud

D. Community cloud

Answer: A

Explanation/Reference:

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.

Question: 5

Which of the following is a public IP?

A. 13.16.123.1

B. 192.168.123.1

C. 172.16.123.1

D. 10.221.123.1

Answer: A

Explanation/Reference:

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.

Question: 6

Which of the following is a data handling policy procedure?

A. Transform

B. Collect

C. Encode

D. Destroy

Answer: D

Explanation/Reference:

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

Question: 7

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

A. Routers

B. HIDS

C. Firewalls

D. NIDS

Answer: D

Explanation/Reference:

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.

Question: 8

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?

A. Least Privilege

B. Defense in Depth

C. Separation of Duties

D. Privileged Accounts

Answer: B

Explanation/Reference:

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.

Question: 9

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

A. Fences

B. Turnstiles

C. Barriers

D. Locks

Answer: D

Explanation/Reference:

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).

Question: 10

Which of the following is a detection control?

A. Turnstiles

B. Smoke sensors

C. Bollards

D. Firewalls

Answer: B

Explanation/Reference:

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.

Question: 11

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

A. Backdoors

B. Rootkits

C. Cross-Site Scripting

D. Trojans

Answer: A

Explanation/Reference:

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.

Question: 12

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

A. SNMP

B. ICMP

C. IGMP

D. IP

Answer: A

Explanation/Reference:

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.

Question: 13

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

A. Risk avoidance

B. Risk transfer

C. Risk mitigation

D. Risk tolerance

Answer: B

Explanation/Reference:

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.

Question: 14

The SMTP protocol operates at OSI Level:

A. 7

B. 25

C. 3

D. 23

Answer: A

Explanation/Reference:

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.

Question: 15

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

A. Confidentiality

B. Integrity

C. Authentication

D. Authorization

Answer: C

Explanation/Reference:

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. In contrast, authorization refers to the permission granted to users, processes or devices to access specific assets. Confidentiality and integrity are properties of information and systems, not processes.

Question: 16

If an organization wants to protect itself against tailgating, which of the following types of access control would be most effective?

A. Locks

B. Fences

C. Barriers

D. Turnstiles

Answer: D

Explanation/Reference:

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).

Question: 17

Logging and monitoring systems are essential to:

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

B. Identifying efficient performing systems, labeling compromises, and providing a record of how systems are used

C. Identifying inefficient performing systems, detecting compromises, and providing a record of how systems are used

D. Identifying efficient performing systems, detecting compromises, and providing a record of how systems are used

Answer: C

Explanation/Reference:

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.

Question: 18

In the event of a disaster, which of these should be the PRIMARY objective? (★)

A. Guarantee the safety of people

B. Guarantee the continuity of critical systems

C. Protection of the production database

D. Application of disaster communication

Answer: A

Explanation/Reference:

In the event of a disaster, the clear priority is to guarantee the safety of human life above all. The remaining options, though important from the point of view of disaster recovery and business continuity, are secondary when compared to safety.

Question: 19

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

A. Change Management

B. Vulnerability Management

C. Configuration Management

D. Inventory Management

Answer: A

Explanation/Reference:

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.

Question: 20

The last phase in the data security cycle is:

A. Encryption

B. Backup

C. Archival

D. Destruction

Answer: D

Explanation/Reference:

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.

Question: 21

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

A. RBAC

B. MAC

C. DAC

D. ABAC

Answer: A

Explanation/Reference:

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.

Question: 22

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

A. Firewalls

B. Biometric access controls

C. Remote control electronic locks

D. Security cameras

Answer: A

Explanation/Reference:

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)

Question: 23

Which type of attack will most effectively maintain remote access and control over the victim's computer?

A. Trojans

B. Phishing

C. Cross-Site Scripting

D. Rootkits

Answer: D

Explanation/Reference:

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.

Question: 24

In incident terminology, the meaning of Zero Day is:

A. Days to solve a previously unknown system vulnerability

B. A previously unknown system vulnerability

C. Days without a cybersecurity incident

D. Days with a cybersecurity incident

Answer: B

Explanation/Reference:

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.

Question: 25

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

A. Leveraged

B. Pre-existing

C. Dedicated

D. Hybrid

Answer: B

Explanation/Reference:

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.

Question: 26

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

A. Disabled or separated into a quarantine area until a virus scan can be run

B. Disabled or isolated into a quarantine area until it can be checked and updated.

C. Placed in a demilitarized zone (DMZ) until it can be reviewed and updated

D. Marked as potentially vulnerable and placed in a quarantine area

Answer: B

Explanation/Reference:

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.

Question: 27

A biometric reader that grants access to a computer system in a data center is a:

A. Administrative Control

B. Physical Control

C. Authorization Control

D. Technical Control

Answer: D

Explanation/Reference:

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).

Question: 28

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

A. Denials of Service

B. Phishing

C. Trojans

D. Cross-Site Scripting

Answer: A

Explanation/Reference:

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.

Question: 29

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

A. Trojans

B. Phishing

C. Rootkits

D. Cross-Site Scripting

Answer: A

Explanation/Reference:

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.

Question: 30

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

A. Burp Suite

B. John the Ripper

C. Wireshark

D. Nslookup

Answer: C

Explanation/Reference:

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.

Question: 31

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

A. Side-channel Attack

B. Man-in-the-middle Attack

C. Fragmented Packet Attack

D. Oversized Packet Attack

Answer: A

Explanation/Reference:

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.

Question: 32

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

A. Regulations

B. Standards

C. Policies

D. Procedures

Answer: D

Explanation/Reference:

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).

Question: 33

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

A. SIEM

B. HIDS

C. Router

D. Firewall

Answer: C

Explanation/Reference:

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.

Question: 34

What does SIEM mean?

A. Security Information and Enterprise Manager

B. Security Information and Event Manager

C. System Information and Enterprise Manager

D. System Information and Event Manager

Answer: B

Explanation/Reference:

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.

Question: 35

A Security safeguard is the same as a:

A. Safety control

B. Privacy control

C. Security control

D. Security principle

Answer: C

Explanation/Reference:

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).

Question: 36

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

A. DAC

B. ABAC

C. RBAC

D. MAC

Answer: B

Explanation/Reference:

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

---

Question: 37

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

A. 69

B. 80

C. 25

D. 443

Answer: D

Explanation/Reference:

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.

Question: 38

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

A. Business Impact Plan

B. Business Impact Analysis

C. Disaster Recovery Plan

D. Business Continuity Plan

Answer: B

Explanation/Reference:

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.

Question: 39

Which of the following are NOT types of security controls?

A. Common controls

B. Hybrid controls

C. System-specific controls

D. Storage controls

Answer: D

Explanation/Reference:

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.

Question: 40

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

A. Awareness

B. Training

C. Education

D. Tutorial

Answer: D

Explanation/Reference:

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.

Question: 41

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:

A. Vulnerability

B. Threat

C. Impact

D. Likelihood

Answer: C

Explanation/Reference:

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.

Question: 42

The implementation of Security Controls is a form of:

A. Risk reduction

B. Risk acceptance

C. Risk avoidance

D. Risk transference

Answer: A

Explanation/Reference:

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.

Question: 43

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

A. Trojans

B. Cross-Site Scripting

C. Phishing

D. Rootkits

Answer: B

Explanation/Reference:

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.

Question: 44

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

A. Access Control Lists

B. Acceptable Use Policies

C. Badge Readers

D. No entry signs

Answer: B

Explanation/Reference:

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).

Question: 45

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

A. Request for Approval

B. Request for Change

C. Rollback

D. Disaster and Recover

Answer: C

Explanation/Reference:

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.

Question: 46

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

A. Authentication

B. Confidentiality

C. Non-Repudiation

D. Integrity

Answer: B

Explanation/Reference:

The correct answer is B. A digital signature is the result of a cryptographic transformation of data which is useful for providing: data origin authentication, data integrity, and non-repudiation of the signer (see NIST SP 800-12 Rev. 1 under Digital Signature). However, digital signatures cannot guarantee confidentiality (i.e. the property of data or information not being made available or disclosed).

Question: 47

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

A. Hubs

B. Firewalls

C. Routers

D. SIEM

Answer: D

Explanation/Reference:

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.

Question: 48

What is an effective way of hardening a system?

A. Patch the system

B. Have an IDS in place

C. Run a vulnerability scan

D. Create a DMZ for web application services

Answer: A

Explanation/Reference:

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.

Question: 49

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

A. A public key

B. A private key

C. An asymmetric key

D. A symmetric key

Answer: D

Explanation/Reference:

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.

Question: 50

Which regulations address data protection and privacy in Europe?

A. SOX

B. HIPAA

C. FISMA

D. GDPR

Answer: D

Explanation/Reference:

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.

Question: 51

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

A. Hubs

B. Firewalls

C. Routers

D. Switches

Answer: B

Explanation/Reference:

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 (IDS) 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.

Question: 52

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

A. Intranet

B. DMZ

C. Internal Network

D. VPN

Answer: B

Explanation/Reference:

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.

Question: 53

Sensitivity is a measure of the ...:

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

B. ... urgency and protection assigned to information by its owner.

C. ... importance assigned to information by its owner, or the purpose of representing its need for protection.

D. ... pertinence assigned to information by its owner, or the purpose of representing its need for urgency.

Answer: C

Explanation/Reference:

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).

Question: 54

How many data labels are considered good practice?

A. 2 - 3

B. 1

C. 1-2

D. >4

Answer: A

Explanation/Reference:

According to 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.

Question: 55

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

A. Security Awareness

B. Incident Response Plans

C. Business Continuity Plans

D. Physical Security Controls

Answer: A

Explanation/Reference:

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).

Question: 56

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

A. System Administrator

B. Security Analyst

C. Help Desk

D. External Worker

Answer: D

Explanation/Reference:

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.

Question: 57

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

A. Inventory

B. Baselines

C. Updates

D. Audit logs

Answer: D

Explanation/Reference:

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).

Question: 58

Which are the components of an incident response plan?

A. Preparation -> Detection and Analysis -> Recovery -> Containment -> Eradication -> Post-Incident Activity

B. Preparation -> Detection and Analysis -> Containment -> Eradication -> Post-Incident Activity -> Recovery

C. Preparation -> Detection and Analysis -> Eradication -> Recovery -> Containment -> Post-Incident Activity

D. Preparation -> Detection and Analysis -> Containment, Eradication and Recovery -> Post-Incident Activity

Answer: D

Explanation/Reference:

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).

Question: 59

Which of the following is an example of 2FA?

A. Badges

B. Passwords

C. Keys

D. One-Time passwords (OTA)

Answer: D

Explanation/Reference:

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).

Question: 60

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

A. Business Impact Analysis

B. Disaster Recovery Plan

C. Business Impact Plan

D. Business Continuity Plan

Answer: D

Explanation/Reference:

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.

Question: 61

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

A. Reversible

B. Unique

C. Deterministic

D. Useful

Answer: B

Explanation/Reference:

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.

Question: 62

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

A. Offer → Request → ACK

B. SYN → SYN/ACK → ACK

C. SYN → ACK → FIN

D. Discover → Offer → Request

Answer: B

Explanation/Reference:

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).

Question: 63

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

to normal operation?

A. The Business Impact Plan

B. The Business Impact Analysis

C. The Business Continuity Plan

D. The Disaster Recovery Plan

Answer: D

Explanation/Reference:

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.

Question: 64

What is the consequence of a Denial Of Service attack?

A. Exhaustion of device resources

B. Malware Infection

C. Increase in the availability of resources

D. Remote control of a device

Answer: A

Explanation/Reference:

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.

Question: 65

According to ISC2, which are the six phases of data handling?

A. Create -> Use -> Store -> Share -> Archive -> Destroy

B. Create -> Store -> Use -> Share -> Archive -> Destroy

C. Create -> Share -> Use ->Store -> Archive -> Destroy

D. Create -> Share -> Store -> Use -> Archive -> Destroy

Answer: B

Explanation/Reference:

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).

Question: 66

Which of the following is less likely to be part of an incident response team?

A. Legal representatives

B. Human Resources

C. Representatives of senior management

D. Information security professionals

Answer: B

Explanation/Reference:

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).

Question: 67

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

A. Burp Suite

B. Nslookup

C. John the Ripper

D. Wireshark

Answer: C

Explanation/Reference:

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.

Question: 68

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

A. BYOD

B. Privacy Policy

C. Change Management Policy

D. AUP

Answer: A

Explanation/Reference:

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.

Question: 69

In which cloud deployment model do companies share resources and infrastructure on the cloud?

A. Hybrid cloud

B. Multi-tenant

C. Private cloud

D. Community cloud

Answer: D

Explanation/Reference:

A private cloud is a cloud computing model where the cloud infrastructure is dedicated to a single organization (and never shared with others). Multitenancy means that multiple cloud vendor customers (i.e. tenants) share the same computing resources. A community cloud is an infrastructure where multiple organizations share resources and infrastructure based on common needs (that can be technological or regulatory). Finally, a hybrid cloud refers to a model that combines (i.e. orchestrates) on-premises infrastructure, private cloud services, and a public cloud to handle storage and service.

Question: 70

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

A. Restore company operation to the last-known reliable operation state

B. Outline a safe escape procedure for the organization's personnel

C. Maintain crucial company operations in the event of a disaster

D. Communicate to the responsible entities the damage caused to operations in the event of a disaster

Answer: A

Explanation/Reference:

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.

Question: 71

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

A. Threat Vector

B. Threat Actor

C. Threat

D. Attacker

Answer: B

Explanation/Reference:

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.

Question: 72

A best practice of patch management is to:

A. Apply all patches as quickly as possible

B. Test patches before applying them

C. Apply patches every Wednesday

D. Apply patches according to the vendor's reputation

Answer: B

Explanation/Reference:

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.

Question: 73

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

A. HIDS

B. IDS

C. SIEM

D. NAC

Answer: D

Explanation/Reference:

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.

Question: 74

Which of these is NOT a change management component?

A. Approval

B. RFC

C. Rollback

D. Governance

Answer: D

Explanation/Reference:

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.

Question: 75

Which of the following is NOT a social engineering technique?

A. Pretexting

B. Quid pro quo

C. Double-dealing

D. Baiting

Answer: C

Explanation/Reference:

Baiting is a social engineering attack wherein a scammer uses a false promise to lure a victim. Pretexting is a social engineering technique that manipulates victims into disclosing information. Quid pro quo is a social engineering attack (technically, one that combines 'baiting' with 'pretexting') that promises users a profit in exchange for information that can later be used to gain control of a user's account or sensitive information). Regarding cybersecurity, 'Double-ealing' is not a valid social engineering attack (see ISC2 Study Guide, chapter 5, module 3, under Chapter Resource).

Question: 76

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

A. TCP

B. DHCP

C. SNMP

D. UDP

Answer: A

Explanation/Reference:

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.

Question: 77

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

A. Threat

B. Bug

C. Vulnerability

D. Risk

Answer: C

Explanation/Reference:

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.

Question: 78

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

A. IaaS

B. FaaS

C. PaaS

D. SaaS

Answer: D

Explanation/Reference:

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.

Question: 79

Risk Management is:

A. The assessment of the potential impact of a threat.

B. The creation of an incident response team.

C. The impact and likelihood of a threat.

D. The identification, evaluation and prioritization of risks.

Answer: D

Explanation/Reference:

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.

Question: 80

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

A. Policies

B. Guidelines

C. Regulations

D. Procedures

Answer: B

Explanation/Reference:

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).

Question: 81

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

A. Post-incident Activity

B. Detection and Analysis

C. Preparation

D. Contentment, Eradication, and Recovery

Answer: B

Explanation/Reference:

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

Question: 82

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

A. Privileged Accounts

B. Separation of Duties

C. Least Privilege

D. Defense in Depth

Answer: C

Explanation/Reference:

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.

Question: 83

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

A. ABAC

B. RBAC

C. MAC

D. DAC

Answer: C

Explanation/Reference:

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.

Question: 84

In risk management, the highest priority is given to a risk where:

A. The frequency of occurrence is low, and the expected impact value is high

B. The expected probability of occurrence is low, and the potential impact is low

C. The expected probability of occurrence is high, and the potential impact is low

D. The frequency of occurrence is high, and the expected impact value is low

Answer: A

Explanation/Reference:

The highest priority is given to risks estimated to have 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).

Question: 85

Which of the following areas is connected to PII?

A. Non-Repudiation

B. Authentication

C. Integrity

D. Confidentiality

Answer: D

Explanation/Reference:

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.

Question: 86

According to the canon "Provide diligent and competent service to principals", ISC2 professionals are to:

A. Take care not to tarnish the reputation of other professionals through malice or indifference.

B. Treat all members fairly and,when resolving conflicts, consider public safety and duties to principals, individuals and the profession, in that order.

C. Avoid apparent or actual conflicts of interest.

D. Promote the understanding and acceptance of prudent information security measures.

Answer: C

Explanation/Reference:

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.

Question: 87

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

A. Trojans

B. Whaling

C. Phishing

D. Rootkits

Answer: B

Explanation/Reference:

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.

Question: 88

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

A. Regulation

B. Standard

C. Policy

D. Procedure

Answer: A

Explanation/Reference:

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)

Question: 89

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

A. Phishing

B. Cross-Site Scripting

C. Denials of Service

D. Trojans

Answer: A

Explanation/Reference:

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.

Question: 90

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

A. ABAC

B. MAC

C. RBAC

D. DAC

Answer: D

Explanation/Reference:

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.

Question: 91

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

A. Ransomware

B. Trojan

C. Cross-Site Scripting

D. Phishing

Answer: A

Explanation/Reference:

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.

Question: 92

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

A. SaaS

B. FaaS

C. PaaS

D. IaaS

Answer: D

Explanation/Reference:

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.

Question: 93

How many layers does the OSI model have?

A. 7

B. 4

C. 6

D. 5

Answer: A

Explanation/Reference:

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).

Question: 94

Which of the following principles aims primarily at fraud detection?

A. Privileged Accounts

B. Defense in Depth

C. Least Privilege

D. Separation of Duties

Answer: D

Explanation/Reference:

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.

Question: 95

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

A. TCP

B. SMTP

C. UDP

D. SNMP

Answer: A

Explanation/Reference:

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.

Question: 96

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

A. Access control lists

B. Turnstiles

C. Fences

D. Bollards

Answer: A

Explanation/Reference:

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)

Question: 97

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

A. Side Channels

B. Trojans

C. Cross Site Scripting

D. Denials of Service

Answer: A

Explanation/Reference:

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.

Question: 98

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

A. Integrity

B. Confidentiality

C. Non-Repudiation

D. Authentication

Answer: B

Explanation/Reference:

The correct answer is B. 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.

Question: 99

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

A. Simulations

B. Walkthroughs

C. Reviews

D. Discussions

Answer: A

Explanation/Reference:

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.

Question: 100

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

A. Confidentiality

B. Non-repudiation

C. Authentication

D. Accessibility

Answer: A

Explanation/Reference:

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. 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.

Question: 101

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

A. Apply disaster communication

B. Protect the production database

C. Guarantee the safety of people

D. Guarantee the continuity of critical systems

Answer: C

Explanation/Reference:

In the event of a disaster, the number one priority is to guarantee the safety of human life above all else. The remaining options, though important as concerns business continuity, are never as important as the safety of human beings.

Question: 102

A security professional should report violations of a company's security policy to:

A. The ISC Ethics Committee

B. Company management

C. National authorities

D. A court of law

Answer: B

Explanation/Reference:

The code of ethics requires security professionals to be honest, but not necessarily "law enforcers". A violation of a company's security policy should be reported and handled within the company itself (usually involving the human resources, legal, or management departments). Only individuals can be reported to the ISC2 ethics committee (i.e. not companies). National authorities only deal with violations of laws and regulations.

Question: 103

Which department in a company is NOT regularly involved in a DRP?

A. Executives

B. IT

C. Public Relations

D. Financial

Answer: D

Explanation/Reference:

Executives and Public Relations (PR) need to be aware of the company DRP to handle the expectation of the public and of company stakeholders. IT personnel should be involved in helping businesses get back to normal operations. A company's financial department is rarely involved in a disaster recovery plan. An exception would be if the issue at hand is connected to their area of expertise (see Chapter 2 ISC2 Study Guide, module 4, under Components of a Disaster Recovery Plan).

Question: 104

Which of the following is included in an SLA document?

A. A plan to prepare the organization for the continuation of critical business functions

B. A plan to keep business operations going while recovering from a significant disruption

C. Instructions to detect, respond to, and limit the consequences of a cyber-attack

D. Instructions on data ownership and destruction

Answer: D

Explanation/Reference:

A set of instructions or procedures to detect, respond and limit the consequences of a cyber-attack is an Incident Response Plan (see ISC2 Study Guide Chapter 2, module 1, under The Goal of Incident Response). A plan to sustain business operations while recovering from a significant disruption is a Business Continuity Plan (see ISC2 Study Guide Chapter 2, module 2, under The Importance of Business Continuity). A plan to prepare the organization for the continuation of critical business functions is called a Disaster Recovery Plan (see ISC2 Study Guide Chapter 2, module 3, under The Goal of Disaster Recovery).

Question: 105

What is the most important difference between MAC and DAC?

A. In MAC, security administrators set the roles for the users; in DAC, roles are set at the object owner’s discretion

B. In MAC, security administrators assign access permissions; in DAC, security administrators set user roles

C. In MAC, security administrators assign access permissions; in DAC, access permissions are set at the object owner’s discretion

D. In MAC, access permissions are set at the object owner’s discretion; in DAC, it is up to security administrators to assign access permissions

Answer: C

Explanation/Reference:

In Mandatory Access Control (MAC), security administrators assign access permissions. In contrast, with Discretionary Access Control (MAC), it is up to the object owner’s discretion to set object permissions (see ISC2 Study Guide chapter 1, module 3, under Understand Logical Access Controls).

Question: 106

Requiring a specific user role to access resources is an example of:

A. MAC

B. ABAC

C. RBAC

D. DAC

Answer: C

Explanation/Reference:

Role-Based Access Control (RBAC) restricts access to the resources of a computer or network, according to the roles of individual users within your organization. Attribute-Based Access Control (ABAC) is based on complex attribute rules. In Discretionary Access Control (DAC), users may grant privileges to other subjects, as well as change the security attributes of the objects they have access to.

Question: 107

Which type of document outlines the procedures ensuring that vital company systems keep running during business-disrupting events?

A. Business Impact Plan

B. Business Impact Analysis

C. Disaster Recovery Plan

D. Business Continuity Plan

Answer: D

Explanation/Reference:

A Business Continuity Plan (BCP) is a pre-determined set of instructions describing how an organization's mission or 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 method of analyzing how disruptions can affect an organization. A Disaster Recovery Plan is used to recover systems after a major failure or disaster. The term 'Business Impact Plan' does not exist in Cybersecurity.

Question: 108

Which of the following is NOT a best practice in access management?

A. Give only the right amount of permission

B. Periodically assess if user permissions still apply

C. Request a justification when upgrading permission

D. Trust but verify

Answer: D

Explanation/Reference:

The “Trust but verify” model is a method of threat protection wherein privileged accounts are trusted (but always verified) and allowed access to the network and other resources . Over time, the “Trust but verify” model has been found to expose organizations to multiple security threats, and is therefore being progressively abandoned in favor of the Zero Trust model. The remaining options are all good practices of access management.

Question: 109

If a company collects PII, which policy is required?

A. Remote Access Policy

B. GDPR

C. Privacy Policy

D. Acceptable Use Policy

Answer: C

Explanation/Reference:

A Privacy Policy (PP) outlines the data security mechanisms which ensure that customer data is protected, namely, how Personal Identifiable Information (PII) is collected, stored and processed. An Acceptable Use Policy (AUP) defines the guidelines and limitations that users must agree on while accessing the an organization's network, computer systems or other related resources. The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for the European Union and the European Economic Area. The Remote Access Policy (RAP) defines acceptable methods of remotely connecting to an organization's internal network.

Question: 110

Which of these is LEAST likely to be installed by an infection?

A. Logic Bomb

B. Keylogger

C. Trojan

D. Backdoor

Answer: A

Explanation/Reference:

A logic bomb is a piece of code intentionally inserted into software that will activate after specific conditions are met (see ISC2 Study Guide, chapter 4, module 2). Logic bombs are typically embedded in legitimate software. Trojans are a type of malware used to install keyloggers and backdoors. Keyloggers capture keystrokes and user input, but typically require malware to install the keylogger. 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).

Question: 111

(★) The best defense method to stop a 'Replay Attack' is to:

A. Use an IPSec VPN

B. Use a Firewall

C. Use password authentication

D. Use message digesting

Answer: A

Explanation/Reference:

A replay attack is when an attacker captures and resends (i.e. "replays") authenticated messages (see ISC2 Study Guide, chapter 4, module 2). An IPSec VPN can prevent a replay attack because it tracks packet sequencing and includes the sender's signature on all packets; therefore preventing forged packages. Message digesting is ineffective in preventing resends (and thus also replay attacks), since it doesn't matter whether the attacker can read or decipher the original message and key (all they would have to do would be to resend the message and key together). One-time passwords can be used as a temporary session key known both to the sender and to the receiver that cannot be reused; although related, the concept 'password authentication' refers to a means to identify a user to a given system, and this is different from a one-time password. Firewalls are equipment that filters inbound Internet traffic, and are ineffective against replay attacks inside a network.

Question: 112

Which of these devices has the PRIMARILY objective of determining the most efficient path for the traffic to flow across the networks?

A. Hubs

B. Firewalls

C. Routers

D. Switches

Answer: C

Explanation/Reference:

A router is a networking device whose primary objective is to determine the most efficient path for traffic to flow across a network. Routers connect two or more networks and forward data packets between them according to their destination address (see ISC2 Study Guide, chapter 4, module 1). When a router receives a data packet, it checks the destination address and determines the best route on which to forward the packet, based on its routing table. The routing table is a

set of rules that the router uses to determine the next hop for a given data packet.
Hubs connect multiple devices on a network and broadcast incoming data packets to all connected devices. Hubs cannot route data based on destination address; as a result, all connected devices receive all incoming data packets. Switches connect multiple devices on a network and forward data packets between them based on the MAC address of the destination device. Switches use MAC addresses to create a forwarding table that efficiently routes data to the correct destination.
Firewalls are network devices or software designed to protect a network from external threats (like hacking and malware). Firewalls can block or allow traffic based on various criteria, such as the source or destination of the traffic, as well as the type of data.

Question: 113

Which of these types of malware self-replicates without the need for human intervention?

A. Worm

B. Trojan

C. Virus

D. Rootkits

Answer: A

Explanation/Reference:

A worm is a type of malware designed to replicate itself and spread to other computers without human intervention. Worms exploit operating systems, network servers and other software vulnerabilities in order to propagate themselves. They can cause various damaging effects, including disrupting network performance, consuming bandwidth, and stealing sensitive information (see ISC2 Study Guide, chapter 4, module 2). Some worms can also perform directly malicious actions, such as installing rootkits, backdoors or other malicious software on the systems they infect. Viruses, like worms, replicate themselves and exploit vulnerabilities in systems or software to propagate themselves. However, viruses typically require human intervention (like being activated from an e-mail or downloaded from the internet to be run on a system). On the other hand, Trojans do not replicate themselves, and typically rely on human intervention to be delivered and installed. Finally, rootkits are malware that conceals the presence of other malicious software (such as viruses or Trojans) on a system, namely by hiding their files, processes, and other system artifacts.

Question: 114

As an (ISC)² member, you are expected to perform with due care. What does 'due care' specifically mean?

A. Do what is right in each situation you encounter on the job

B. Give continuity to the legacy of security practices of your company

C. Apply patches annually

D. Researching and acquiring the knowledge to do your job right

Answer: A

Explanation/Reference:

The concept of 'due Care' (also known as 'the prudent person rule') refers to what a prudent person would do in a given situation. In cybersecurity, 'due care' means taking reasonable steps to secure and protect the organization's assets, reputation and finances. The concept is holistic and includes, among other things: implementing the appropriate security standards, policies and procedures; ensuring proper cybersecurity awareness training; and promoting the continuous improvement of monitoring controls. Applying patches, continuing security practices and acquiring knowledge for the job are specific tasks included in 'due care', but are not good overall definitions of the concept (see ISC2 Study Guide, chapter 1, module 5).

Question: 115

(★) Which of these is NOT a best practice in access management?

A. Periodically assessing whether user permissions still apply

B. Requesting a justification when upgrading permission

C. Giving only the right amount of permission

D. Trust but verify

Answer: D

Explanation/Reference:

The "Trust but verify" model is a method of threat protection that involves granting privileged accounts access to the network and other resources, while at the same time verifying their actions and activities. However, over time, this model was found to have limitations that expose organizations to a wide array of security threats. Therefore, "Trust but verify" is being progressively abandoned in favor of the Zero Trust model. The remaining options are all best practices of access management.

Question: 116

During the investigation of an incident, which security policies are more likely to cause difficulties?

A. Configuration standards

B. Incident response policies

C. Communication policies

D. Retention policies

Answer: D

Explanation/Reference:

For many organizations, retention policies entail keeping data only for a limited time. Because of the high costs of data storage capacity, organizations maintain specific logs only for a short period of time (a few hours to several days), and keep other data records for more extended periods (months to years). Because of this, not all data regarding an incident may be available. Communication and incident response policies can provide valuable help to an incident investigation. Finally, configuration standards are not considered policies (see ISC2 Study Guide, chapter 1, module 4).

Question: 117

In an Access Control List (ACL), the element that determines which permissions you have is:

A. The subject

B. The object

C. The firmware

D. The rule

Answer: D

Explanation/Reference:

An Access Control List (ACL) is a list of rules that specifies which users or systems are granted or denied access (i.e., have permission to access) to a particular object or system resource (see ISC2 Study Guide, chapter 3, module 4). The subject is a user or a process run by a user, which inherits the user authorization. The object is the resource or data in the system (or the network) to be accessed. Firmware is a type of software embedded in a hardware system; therefore, the concept of an Access Control List does not directly apply to it.

Question: 118

What does the term 'data remanence' refer?

A. Data in use that can't be encrypted

B. Files saved locally that can't be remoted accessed

C. Data left over after routine removal and deletion

D. All of the data in a system

Answer: C

Explanation/Reference:

Data Remanence refers to data left over after routine removal and deletion of data from a storage device (see ISC2 Study Guide, chapter 4, module 3). When digital data is deleted, instead of being erased from the storage media, it is often only marked deleted, and the corresponding space is then made available to be overwritten later on. Consequently, deleted data can still be present on the storage media, and can be recovered using the proper media analysis and recovery tools. Data remanence is a concern when media storage devices containing sensitive or confidential data need to be disposed of. Specialized techniques and tools can be used to securely erase data and reduce the risk of data remanence, such as degaussing and other specialized data destruction tools. Therefore, the term data remanence is unrelated to any of the other options.

Question: 119

(★) Which type of recovery site has some or most systems in place, but does not have the data needed to take over operations?

A. A hot site

B. A cloud site

C. A warm site

D. A cold site

Answer: C

Explanation/Reference:

A cold site requires space, power, network connectivity, systems and data to be put in place and take over operations. Warm sites have power, connectivity, and systems, but do not have live or current data enabling the immediate takeover of operations (see ISC2 Study Guide, chapter 2, module 3). A hot site can immediately take over operations. A cloud site is not a term that refers to one of the three most common types of recovery sites.

Question: 120

Which of these is NOT a characteristic of an MSP implementation?

A. Manage all in-house company infrastructure

B. Monitor and respond to security incidents

C. Mediate, execute and decide top-level decisions

D. Utilize expertise for the implementation of a product or service

Answer: A

Explanation/Reference:

Manage all-in-house company infrastructure is not a characteristic of an MSP (Managed Service Provider) implementation. MSPs provide an outsourced IT service to manage a company's IT infrastructure and endpoints, rather than managing it all in-house. Some characteristics of an MSP implementation include the following (see ISC2 Study Guide, chapter 4, module 3):
Utilizing expertise for the implementation of a product or service
Monitoring and responding to security incidents
Mediating, executing and deciding top-level decisions
Manage all in-house IT infrastructure
In contrast, managing an all-in-house IT infrastructure refers to the scenario where an organization's internal IT team is responsible for all aspects of its IT systems and infrastructure.

Question: 121

Which of these is NOT a typical component of a comprehensive business continuity plan (BCP)?

A. A cost prediction of the immediate response procedures

B. Immediate response procedures and checklists

C. Notification systems and call trees for alerting personnel

D. A list of the BCP team members

Answer: A

Explanation/Reference:

Cost predictions of response procedures are not typical components of business continuity plans (BCP). A BCP typically includes the following elements:
A list of BCP team members, who will be responsible for implementing the BCP and coordinating the response to an incident;
Immediate response procedures and checklists, with step-by-step instructions for responding to an incident and restoring operations;
Notification systems and call trees for alerting personnel, the purpose of which is to effectively communicate with personnel and coordinate incident response;
Procedures for backup and restoration of critical systems and data, including steps for backing up and restoring essential systems and data, in the event of an incident;
Procedures for maintaining business operations, detailing the steps for maintaining business operations during and after an incident;
BCP testing and maintenance procedures for regularly testing and maintaining the BCP, in order to ensure that it is both effective and up-to-date;
Communications and PR plan, for communicating with stakeholders, customers and the public about a given incident and the actions needed to address it.

Question: 122

Acting ethically is mandatory for (ISC)² members. Which of these is NOT considered unethical?

A. Disrupting the intended use of the internet

B. Seeking to gain unauthorized access to resources on thae internet

C. Compromising the privacy of users

D. Having fake social media profiles and accounts

Answer: D

Explanation/Reference:

Having fake social media profiles and accounts can be socially objectionable, but does not violate the (ISC)² Ethics Canons (see ISC2 Study Guide, chapter 1, module 5). That being said, seeking to gain unauthorized access to resources on the internet, compromising the privacy of users, and disrupting the intended use of the internet are all considered unethical behaviors by (ISC)², as well as by other similar professional organizations. Aside from being violations of professional codes of conduct, such actions may also be in violation of laws and regulations.

Question: 123

In an incident response process, which phase uses indicators of compromise and log analysis as part of a review of events?

A. Preparation

B. Eradication

C. Identification

D. Containment

Answer: C

Explanation/Reference:

According to NIST methodology, an incident response plan has four phases to structure the organization’s incident response, and typically includes short and long-term goals, metrics for measuring success, training, and job requirements for incident response roles. The identification phase focuses on identifying the attack, understanding its severity, and prioritizing it appropriately. Preparation focuses on building tools, processes and procedures to respond to incidents. Eradication involves the removal of artifacts related to the incident, and containment limits both the scope and the impact of the incident. The critical aspect here is that identification uses multiple techniques to analyze attack events and identify potential cascading incidents or variants. Furthermore, substantial effort is devoted to documenting and investigating what happened during the incident, so as to ensure even better preparation, detection and analysis for future incidents (see ISC2 Study Guide, chapter 5, module 3).

Question: 124

Which of these Access Control Systems is commonly used in the military?

A. ABAC

B. DAC

C. RBAC

D. MAC

Answer: D

Explanation/Reference:

Mandatory Access Control (MAC) is a model of access control that is commonly used in the military, because it enables the centralized management of access rights, as well as the enforcement of strict security policies (see ISC2 Study Guide, chapter 3, module 3). In MAC, access to resources is based on the classification level of a given resource, as well as on the clearance level of the user. The use of classification and clearance levels allows for a hierarchical approach to security, whereby access to more sensitive resources is restricted to users with a higher clearance level. This is important in the military, where the risk of unauthorized access or actions can have very serious consequences. Role-Based Access Control (RBAC) restricts access to the resources of a computer or network according to the roles of each individual user in the organization. Attribute-Based Access Control (ABAC) is based on complex attribute rules. In Discretionary Access Control (DAC), users can grant privileges to other subjects, as well as change the security attributes of objects they have access to.

Question: 125

Which of these is NOT a security principle?

A. Security in Depth (SID)

B. Zero Trust model

C. Least Privilege

D. Separation of Duties

Answer: A

Explanation/Reference:

Security in Depth (SID) is not a security principle, but a security model that involves implementing multiple layers of security controls, so as to protect against threats and reduce the risk of a successful attack. In Security in Depth, the idea is to create a multi-layered defense system that includes both technical controls (such as firewalls and intrusion detection systems) and administrative controls (such as policies and procedures).

Zero Trust model, Separation of Duties and Least Privilege are all security principles. The Zero Trust model is based on the idea that organizations should not trust any user, device or network (even within the organization's own network) until appropriately verified. Separation of Duties is a principle that involves dividing tasks and responsibilities among different individuals or groups, in order to prevent any single individual or group from having too much control over a given process. This helps reduce the risk of fraud or errors. Least Privilege prescribes limiting privileges and access to resources only to those users and processes that actually need them. This helps reduce the risk of unauthorized access, or of misuse of resources.

Question: 126

Which of these is not a common goal of a cybersecurity attacker?

A. Allocation

B. Alteration

C. Disclosure

D. Denial

Answer: A

Explanation/Reference:

The three most common goals of cybersecurity attackers are disclosure, alteration, and denial (DAD), which correspond directly to to the cybersecurity triad: confidentiality, integrity, and availability (CIA) (see ISC2 Study Guide, chapter 1, module 1). Allocation means assigning controls to specific system elements responsible for providing a security or privacy capability (e.g., access control systems, routers, servers, etc.), and therefore is not a common goal of a cybersecurity attacker.

Question: 127

Which of these types of layers is NOT part of the TCP/IP model?

A. Application

B. Physical

C. Internet

D. Transport

Answer: B

Explanation/Reference:

The physical layer exists in the OSI model, but not in the TCP/IP model. The TCP/IP Protocol Architecture Layers are: [1] Application (Determines the protocols for the Transport layer); [2] Transport (Allows for data to move among devices); [3] Internet (Creates and inserts packets); [4] Network Interface (Governs how data will move through the network) (for more on this, see ISC2 Study Guide, Chapter 4, Module 1).

Question: 128

On a BYOD model, which of these technologies is best suited to keep corporate data and applications separate from personal?

A. Biometrics

B. Full-device encryption

C. Context-aware authentication

D. Containerization

Answer: D

Explanation/Reference:

Containerization allows users to run corporate applications and access corporate data in a secure environment that applications outside the container cannot access. Containerization solutions for mobile devices typically use encryption and other isolation techniques to ensure that data and applications do not cross over. Full-device encryption helps reduce the risk of theft or loss of a device, thereby reducing the risk of a data breach. Biometrics and context-aware authentication are helpful in ensuring that the right user is using a device, but do not guarantee this separation themselves (see ISC2 Study Guide, chapter 4, module 3).

Question: 129

In the context of risk management, which information does ALE outline?

A. The expected cost per year of not performing a given risk-mitigating action

B. The business impact of a risk

C. The percentage of Asset Lost Efficiency

D. The probability of a risk coming to pass in a given year

Answer: A

Explanation/Reference:

The Annualized Loss Expectancy (ALE) is a standard metric of risk exposure that refers to the expected cost per year of a given risk if it is not mitigated. The business impact of a risk is technically considered a loss, and is better captured by a metric called Single Loss Expectancy (see ISC2 Study Guide, chapter 1, module 2). The probability of a risk coming to pass in a given year is best captured by a metric called Annualized Rate of Occurrence (ARO). Asset Lost Efficiency is a misleading term that is not directly related to risk management.

Question: 130

Which of these techniques is PRIMARILY used to ensure data integrity?

A. Message Digest

B. Content Encryption

C. Backups

D. Hashing

Answer: A

Explanation/Reference:

Data integrity means that a message has not been tampered with or altered. A Message Digest ensures the integrity of any message data that is transmitted over an insecure channel (since a channel that may alter the message's content) (see ISC2 Study Guide, chapter 1, module 1). Cryptographic hash functions (like MD5 or SHA-256) create a fixed-length digital fingerprint of the message data called the Message Digest. If the Message Digest does not match, then the message's integrity has been compromised.
In itself, hashing doesn't guarantee integrity, since integrity follows from the protocol whereby the sender and the receiver both digest the message. Content encryption guarantees the property of confidentiality whereby the contents of a message can only be accessed from the original data with the knowledge of a key. Backups are copies of data stored in a separate location that can be used to restore data in the event of data loss or corruption. They can ensure data integrity by providing a way to verify its authenticity and accuracy. However, backups do not actively prevent data corruption or tampering, and may not even be able to detect changes in the data unless a comparison with the original data is made.

Question: 131

Which of these is an example of a privacy breach?

A. Any observable occurrence in a network or system

B. Being exposed to the possibility of attack

C. Unavailability of critical systems

D. Access of private information by an unauthorized person

Answer: D

Explanation/Reference:

A privacy breach is a compromise of confidentiality (see ISC2 Study Guide, chapter 2, module 1). The NIST defines privacy breach as "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses (or potentially accesses) personally identifiable information, or uses it for anything other than its authorized purpose". The unavailability of a critical system is a compromise of availability (not of confidentiality). Finally, not every occurrence in a network is an instance of a security breach, and virtually every system and organization is exposed to the possibility of being attacked

Question: 132

Which of these terms refers to a collection of fixes?

A. Downgrade

B. Patch

C. Service Pack

D. Hotfix

Answer: C

Explanation/Reference:

A service pack comprises a collection of updates, fixes or enhancements to a software program delivered as a single installable package. A hotfix (or quick-fix) engineering update is a cumulative package which includes information that will be used to address a problem in a software product. A software patch is a quick-repair job for a piece of programming, and is designed to resolve functionality issues, improve security and/or add new features.

Question: 133

While performing background checks on new employees, which of these can NEVER be an attribute for discrimination?

A. Employment history, references, criminal records

B. Credit history, employment history, references

C. Criminal Records, credit history, references

D. References, education, political affiliation, employment history

Answer: D

Explanation/Reference:

The correct answer is A. A best practice when hiring new staff is to perform a background check, so as to minimize risks. A company can use discriminatory factors such as references, academic degrees, and employment, criminal, or credit history (although this is not very common). However, it is illegal to inquire about potential or current employees' political preferences (see ISC2 Study Guide, chapter 5, module 4).

Question: 134

When looking for cybersecurity insurance, which of these is the MOST IMPORTANT objective?

A. Risk acceptance

B. Risk transference

C. Risk avoidance

D. Risk spreading

Answer: B

Explanation/Reference:

The purpose of any insurance is to transfer risk from one party to another. The insurer is obligated to indemnify the insured for a loss caused by an unexpected event, over the course of a definite and mutually-agreed period of time. Risk avoidance consists in avoiding or eliminating the actions and conditions that give rise to the risk. Risk spreading consists in spreading a significant amount of risk over a larger part of the organization or activity, namely by manipulating the sequence or size of related events or activities. Finally, risk acceptance means that the possibility of loss is assumed in that risk, and that no positive action is taken to avoid, reduce or transfer the risk (see ISC2 Study Guide, chapter 1, module 2).

Question: 135

Which of these documents is MORE directly related to what can be done with a system or with its information?

A. SLA

B. MOA

C. MOU

D. ROE

Answer: C

Explanation/Reference:

A Memorandum of Understanding (MOU) outlines the terms and conditions for collaboration, including eventual restrictions on the use of information (see ISC2 Study Guide, chapter 4, module 3). A Memorandum of Agreement (MOA) is similar to an MOU, but is both more formal and legally binding. A Service Level Agreement (SLA) is a contract between a service provider and a customer which specifies service-related guarantees or warranties. In Cybersecurity, Rules of Engagement (ROE) are guidelines and principles outlining the conditions under which a cybersecurity team or organization can act to defend against cyber threats. ROE may include the types of actions that are authorized, the circumstances under which such actions can be taken, and the procedures for obtaining approval or authorization to take such actions. ROEs are important, since they ensure that an organization does not become vulnerable to further attacks while defending itself from an ongoing attack.

Question: 136

Which kind of document outlines the procedures ensuring that vital company systems keep running during business-disrupting events?

A. Business Impact Analysis

B. Business Impact Plan

C. Business Continuity Plan

D. Disaster Recovery Plan

Answer: C

Explanation/Reference:

A Business Continuity Plan (BCP) is a predetermined set of instructions describing how an organization's 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 method of analyzing how such disruptions can affect an organization. A Disaster Recovery Plan is used to recover systems after a major failure or disaster. The term 'Business Impact Plan' does not actually exist in Cybersecurity.

Question: 137

Which of these social engineering attacks sends emails that target specific individuals?

A. Pharming

B. Whaling

C. Vishing

D. Spear phishing

Answer: D

Explanation/Reference:

Spear phishing is a highly targeted phishing attack (and not just random spam) which aims to get specific individuals to reveal confidential information. The particularity of spear phishing is that these attacks are sent with prior knowledge about the target (person or company), so as to increase its chance of success. Whaling is a phishing attack targeted at a group (typically an organization's executives) (see ISC2 Study Guide, chapter 4, module 3). A pharming attack corrupts an infrastructure service such as DNS (Domain Name System), which causes traffic to be misdirected to a forged site, thereby getting users to reveal sensitive information or download malware. Therefore, pharming is not directed at a specific individual. Vishing is an attack carried out by voice where the attacker calls the victim (for example, claiming they are from their bank).

Question: 138

(★) Which of these properties is NOT guaranteed by a Message Authentication Code (MAC)?

A. Authenticity

B. Anonymity

C. Integrity

D. Non-repudiation

Answer: B

Explanation/Reference:

A Message Authentication Code (MAC) does not guarantee anonymity. MAC is a cryptographic function that guarantees a message's integrity, authenticity, and non-repudiation. In particular:
Integrity is the ability of the MAC to detect any changes that may have occurred to a message during either transmission or storage. A MAC provides this by generating a unique code for the message based on its contents, as well as a secret key that is shared between the sender and the receiver. If any changes are made to the message, the MAC code will not match the original code, thus indicating that the message has been tampered with.
Authenticity is the ability to verify the identity of a message's sender. A MAC provides this by sharing a secret key between the sender and receiver. Only the sender knows the key, meaning that only the sender can generate a valid MAC code for the message (which may only have come from the sender.)
Non-repudiation is the ability to prevent the sender from denying that they sent a given message. A MAC provides this by sharing a secret key between the sender and receiver. If the sender sends a message with a valid MAC code, then they cannot later deny that they sent the message, because they must necessarily have known the secret key to generate the valid MAC code.
On the other hand, anonymity is not a property guaranteed by a MAC. Anonymity is the ability to hide the identity of the sender of a given message. A MAC does not provide anonymity, since it uses a secret key that is shared between the sender and the receiver, and the sender must then use this key to generate a valid MAC code for the message. This means that the receiver can accurately determine the identity of the sender.

Question: 139

What is the PRIMARY objective of a degaussing?

A. Preventing magnetic side-channel attacks

B. Reducing noisy data on a disk

C. Erasing the data on a disk

D. Retaining the data on a disk

Answer: C

Explanation/Reference:

Degaussing is a technique used to erase data from a magnetic storage device, such as a hard disk drive (HDD) or magnetic tape. In degaussing, devices are exposed to strong magnetic fields that neutralize the magnetic records of the data stored on the device. This effectively erases the data, making it difficult or impossible to recover. Degaussing is often used to securely erase data from storage devices before disposing or repurposing them, thereby ensuring that unauthorized parties cannot access sensitive or confidential information. Conceivably, a magnetic side-channel attack could target the magnetic fields emitted by a disk, in order to extract information from it. Therefore, strictly speaking, degaussing the disk would prevent the side channel attack by rendering it unusable. However, this is not the primary goal of degaussing (see ISC2 Study Guide, chapter 5, module 1).

Question: 140

Which of these is part of the canons $(ISC)^2$ code of ethics?

A. Provide diligent and competent services to stakeholders

B. Advance and protect the profession

C. Prevent and detect unauthorized use of digital assets in a society

D. Act always in the best interest of your client

Answer: B

Explanation/Reference:

The four canons of ISC2 are (see ISC2 Study Guide, chapter 1, module 5):
Advance and protect the profession;
Act honorably, honestly, justly, responsibly and legally;
Provide diligent and competent service to principals;
Protect society, the common good, necessary public trust and confidence and the infrastructure.
Although some options seem right, only 'Advance and protect the profession' is correct.

Question: 141

Which of these is NOT one of the (ISC)² ethics canons?

A. Act honorably, honestly, justly, responsibly, and legally

B. Consider the social consequences of the systems you are designing

C. Protect society, the common good, necessary public trust and confidence, and the infrastructure

D. Provide diligent and competent service to principals

Answer: B

Explanation/Reference:

Considering the social consequences of the systems you are designing is a valid concern, since the professional must abide by the canon of their protecting society, the common good, necessary public trust and confidence, and the infrastructure. However, this is not in itself a canon. The four canons of (ISC)² are: Protect society, the common good, necessary public trust and confidence, and the infrastructure; Act honorably, honestly, justly, responsibly, and legally; Provide diligent and competent service to principals; Advance and protect the profession (see ISC2 Study Guide, chapter 1, module 5).

Question: 142

(★) Which of these is the PRIMARY objective of the PCI-DSS standard?

A. Personally Identifiable Information (PII)

B. Change Management

C. Secure Credit Cards Payments

D. Protected Health Information (PHI)

Answer: C

Explanation/Reference:

PCI-DSS (Payment Card Industry Data Security Standard) is a standard used in the payment card industry. Protected Health Information (PHI) is any individually identifiable health information that is created, used or disclosed while providing healthcare services. The Health Insurance Portability and Accountability Act (HIPAA) is a United States law aimed at protecting PHI. Personally Identifiable Information (PII) is any information that is capable of identifying an individual. PII is protected by regulations, such as GDPR (in the EU) and HIPAA and PCI-DSS (in the US). Finally, Change management is the process of planning, implementing and controlling changes to a company's information systems.

Question: 143

Which of these is an attack that encrypts the organization's information, and then demands payment for the decryption code?

A. Phishing

B. DDoS

C. Spoofing

D. Ransomware

Answer: D

Explanation/Reference:

Ransomware is an attack that encrypts an organization's information (thereby rendering it inaccessible or unusable) and then demands payment in exchange for the decryption code (see ISC2 Study Guide, chapter 4, module 2). A distributed denial-of-service (DDoS) attack is a type of attack in which a large amount of malicious traffic is directed at a specific target (such as a website or server), so as to overwhelm it, thus making it unavailable to users. Phishing is an attack in which attackers send fake emails or text messages that seem to come from legitimate sources, so as to trick the recipient into revealing sensitive information or clicking on a malicious link. Finally, spoofing is an attack in which an attacker impersonates another person or device to gain unauthorized access to a system, or to steal sensitive information.

Question: 144

The PRIMARY objective of a business continuity plan is:

A. To regularly verify whether the organization complies with applicable regulations

B. To sustain business operations while recovering from a disruption

C. To assess the impact of disruption to the business

D. To restore the business to the full last-known reliable state of operations

Answer: B

Explanation/Reference:

A Business Continuity Plan (BCP) is a predetermined set of instructions describing how the mission and business processes of an organization will be sustained during and after a significant disruption (see Chapter 2 ISC2 Study Guide, module 4, under Terms and Definitions). Restoring a business to its last-known reliable state of operations is the goal of a Disaster Recovery Plan (see Chapter 2 ISC2 Study Guide, module 4, under The Goal of Disaster Recovery). Assessing the

impact of a disruption is the goal of Risk Analysis. Finally, an organization's regulatory compliance is verified via auditing.

Question: 145

Which of these is an attack whose PRIMARY goal is to gain access to a target system through falsified identity?

A. Ransomware

B. Amplification

C. Spoofing

D. DDoS

Answer: C

Explanation/Reference:

Spoofing is an attack whose primary goal is to gain access to a target system through a falsified identity. In a spoofing attack, the attacker creates or manipulates a digital identity or communication, so as to deceive the target into believing that the attacker is someone or something else. There are many different types of spoofing attacks, including email spoofing, IP spoofing, and URL spoofing. Such attacks are used to gain unauthorized access to systems or networks, steal sensitive information, or spread malware (see ISC2 Study Guide, chapter 4, module 2).
The other types of attacks listed above have different primary goals. DDoS (Distributed Denial of Service) attacks aim at overwhelming a target system with traffic to disrupt its operation; amplification attacks involve using a third-party system to amplify the strength of an attack; and ransomware attacks typically encrypt a target system's data, and then demand a ransom in exchange for the decryption code

Question: 146

When an incident occurs, which of these is not a PRIMARY responsibility of an organization's response team?

A. Determining the scope of the damage caused by the incident

B. Implementing the recovery procedures necessary to restore security and recover from any incident-related damage

C. Determining whether any confidential information has been compromised over the course of the entire incident

D. Communicating with top management regarding the circumstances of the cybersecurity event

Answer: D

Explanation/Reference:

While communicating with top management about the circumstances of the cybersecurity event is always important, it is not a primary responsibility of the response team. Indeed, the primary responsibility of the response team is to address

the immediate impact of the incident, and to restore security as quickly as possible. When an incident occurs, the primary duties of a response team include the following:
Determining the scope of the damage caused by the incident, and ascertaining the resources that will be needed to recover from it;
Determining whether any confidential information has been compromised over the course of the entire incident;
Implementing the recovery procedures necessary to restore security and recover from incident-related damage (including restoring systems, recovering data, and implementing any required security controls);
Communicating with relevant parties (such as users, customers and other stakeholders) about the incident itself, and about the steps needed to address it.

Question: 147

What is the PRIMARY objective of a rollback in the context of the change management process?

A. Identify the required changes needed

B. Validate the system change process

C. Restore the system to its last state before the change was made

D. Establish a minimum understood and acceptable level of security requirements

Answer: C

Explanation/Reference:

In the context of the change management process, the primary objective of a rollback is to restore the system to its last state before the change was made. By rolling back the change, the system can be returned to its previous state, which may help to resolve issues and restore regular operation. Rollbacks can be either triggered automatically in response to a failure or error, or initiated manually during the change management process (see ISC2 Study Guide, chapter 5, module 2).
Establishing a minimum understood and acceptable level of security requirements refers to the definition of the minimum acceptable level of security for a system or network. In turn, identifying the required changes refers to identifying any weaknesses or vulnerabilities that need to be addressed in a system or network, as well as to determining the best course of action to address them. Finally, validating the system change process refers to verifying that the process used to implement change to a system is working as intended. This validation involves testing changes to ensure they do not cause unintended consequences or disruptions.

Question: 148

Which of these entities is responsible for signing an organization's policies?

A. Human Resources

B. Security engineer

C. Financial Department

D. Senior management

Answer: D

Explanation/Reference:

Senior management is typically responsible for setting the organization's overall direction and strategy, and for ensuring that policies and procedures are in place to support that strategy. Therefore, it is the senior management's responsibility to sign the organization's policies. Although other departments and stakeholders may be called in to develop and draft policies, it is ultimately the responsibility of senior management to sign off on the policies, indicating their approval and support.

Question: 149

Which of these terms refers to threats with unusually high technical and operational sophistication, spanning months or even years?

A. Rootkit

B. APT

C. Side-channel

D. Ping of death

Answer: B

Explanation/Reference:

An Advanced Persistent Threat is a threat with unusually high technical and operational sophistication. APTs can be difficult to detect and defend against, as the attackers often use sophisticated techniques to evade detection, and to remain stealthy for extended periods of time. APTs are typically carried out by highly skilled and well-funded attackers (such as nation-state actors or well-organized criminal groups), and often target specific organizations or individuals with the goal of stealing sensitive information or disrupting operations (see ISC2 Study Guide, chapter 4, module 2).
The other options listed above are all related to different types of cyber threats, but are not typically associated with APTs. Rootkits are a type of malware designed to conceal the presence of other malicious software on a system, while a ping of death is a type of denial of service (DoS) attack which involves sending a maliciously large ping packet to a target system, in an attempt to overwhelm it. Side-channel attacks exploit information leaked through non-traditional channels (such as power consumption, electromagnetic emissions, or physical timing), in order to gain access to sensitive information or perform other malicious actions.

Question: 150

The PRIMARY objective of a security baseline is to establish ...

A. . a minimum understood and a good level of security requirements

B. ... a minimum understood and acceptable level of security requirements

C. ... security and configuration requirements

D. ... a maximum understood and an acceptable level of security requirements

Answer: B

Explanation/Reference:

A security baseline is a set of security standards, guidelines and procedures used to ensure that a system or network meets a minimum level of security. Security baselines are typically based on industry best practices, regulatory requirements, and an organization's specific security needs. The primary objective of a security baseline is to establish a minimum understood and acceptable level of security requirements. While it is true that a security baseline specifies security and configuration requirements that must be met to ensure that the system or network is adequately protected, that is actually not its primary goal (see ISC2 Study Guide, chapter 5, module 2). The other options do not apply, since they do not align the definition of a security baseline. Moreover, enforcing a maximum number of security requirements is not necessarily a good practice, since practically no organization could bear such a cost.

Question: 151

Which of these attacks take advantage of inadequate input validation in websites?

A. Phishing

B. Trojans

C. Cross-Site Scripting

D. Rootkits

Answer: C

Explanation/Reference:

Cross-Site Scripting (XSS) is an attack where malicious executable scripts are injected into an otherwise benign website (or web application) code. 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) (see ISC2 Study Guide, chapter 4, module 2). Trojans and phishing are attacks where software applications and messages try to appear legitimate, but have hidden malicious functions. They do not necessarily rely on poor input validations. Finally, input validation does not even apply to a rootkit attack.

Question: 152

An organization needs a network security tool that detects and acts in the event of malicious activity. Which of these tools will BEST meet their needs?

A. Router

B. IPS

C. IDS

D. Firewall

Answer: B

Explanation/Reference:

An intrusion prevention system (IPS) is designed to monitor network traffic in real-time, identifying patterns or behaviors that may indicate an attempted intrusion or other malicious activity. Whenever an IPS detects suspicious activity, it can also act to protect the network (such as by blocking suspicious traffic, alerting the network administrator, or initiating a response to contain the threat) (see ISC2 Study Guide, chapter 4, module 2).
Another type of network security tool is an intrusion detection system (IDS), which is similar to an IPS, except that it focuses on detecting rather than preventing attacks. Firewalls are network security equipment or software that controls the incoming and outgoing network traffic according to predetermined security rules. They are indeed valuable in network security, but do not typically have the detection capabilities of IDS or IPS. Finally, a router is a networking device that forwards data packets between computer networks, but does not have the same security features as an IPS, IDS or firewall.

Question: 153

In a DAC policy scenario, which of these tasks can only be performed by a subject granted access to information?

A. Changing security attributes

B. Reading the information

C. Executing the information

D. Modifying the information

Answer: A

Explanation/Reference:

As a principle, users can perform Read, Write and Execute actions with every Access Control policy. However, in discretionary access control policies, the permissions associated with each object (files or system resources) are set by the object's owner. In this model, the creator of an object implicitly becomes its owner, and therefore can decide who will have permission to the objects (see ISC2 Study Guide, chapter 3, module 3). A major weakness of DAC is that it gives users complete control to set security level settings for other users, which can result in users having more privileges than they are supposed to.

Question: 154

In the event of non-compliance, which of these can have considerable financial consequences for an organization?

A. Policies

B. Regulations

C. Guidelines

D. Standards

Answer: B

Explanation/Reference:

Regulations are created by governments or national authorities, and often lead to financial fines for infringement. For example, the EU's GDPR prescribes penalties of up to 2% of annual revenue. Standards are created by governing or professional bodies (not by governments), and thus are not legally enforceable. Regulations are mandatory, while standards are voluntary. Policies and guidelines are internal to organizations, and are therefore not subject to financial penalties (see ISC2 Study Guide Chapter 1, Module 4).

Question: 155

What does the term LAN refer to?

A. A tool to manage and control network traffic, as well as to protect a network.

B. A network on a building or limited geographical area

C. A device that connects multiple other devices in a network

D. A long-distance connection between geographically-distant networks

Answer: B

Explanation/Reference:

A local area network (LAN) typically covers a single floor or building. Long-distance connections between geographically-distant networks form something called a wide area network (WAN). Multiple devices in a network are connected through hubs or switches. The management and control of network traffic and protection is achieved by specialized equipment, such as firewalls and intrusion prevention systems (ISC2 Study Guide, Chapter 4, Module 1)

Question: 156

Which of these is a type of corrective security control?

A. Patches

B. Intrusion detection systems

C. Guidelines

D. Encryption

Answer: A

Explanation/Reference:

Patches are a type of corrective security control, since they repair damage and restore resources and capabilities to a secure and previously-updated state (see ISC2 Study Guide, chapter 5, module 2). Encryption is a preventive security control that ensures data confidentiality. Intrusion detection systems are detective controls, since they monitor a given system for unwanted activity. Intrusion detection systems (IDS) alert administrators to potential security breaches or attacks. Although they help prevent or mitigate their impact, they are not in themselves corrective controls. Guidelines provide recommendations or suggestions for achieving a particular goal or objective, and are often used to guide best practices or recommended approaches; furthermore, they are not typically considered corrective security controls.

Question: 157

Which of these enables point-to-point online communication over an untrusted network?

A. VLAN

B. Firewall

C. Router

D. VPN

Answer: D

Explanation/Reference:

A VPN is a type of network technology that creates a secure encrypted connection between a device and a network. This connection allows users to communicate with each other and access network resources as if they were on the same local network, even if they are in different locations (see ISC2 Study Guide, chapter 4, module 3). A VLAN (Virtual Local Area Network) is a network segmentation technology that allows devices on a network to be logically grouped, even if they are in different locations. Firewalls are network security systems that control incoming and outgoing network traffic according to predetermined security rules. Finally, a router is a networking device that forwards data packets between computer networks, but does not provide the same level of security as a VPN.

Question: 158

At which of the OSI layers do TCP and UDP work?

A. Transport Layer

B. Session Layer

C. Application Layer

D. Physical Layer

Answer: A

Explanation/Reference:

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both transport layer protocols, which operate at the fourth layer of the OSI (Open Systems Interconnection) model (see ISC2 Study Guide, chapter 4, module 1). The transport layer (also known as "Layer 4") ensures that data is delivered reliably and efficiently between different devices on a network. TCP is a connection-oriented protocol which establishes a dedicated end-to-end connection. UDP is a connectionless protocol, and therefore does not establish a reliable connection before transmitting data. The choice between using TCP or UDP is typically based on tradeoffs between requirements of reliability and speed.
The physical layer ("Layer 1") is responsible for transmitting raw data over a physical medium, such as a copper wire or fiber optic cable. The session layer ("Layer 5") is responsible for establishing, maintaining and terminating connections between different devices on a network. The application layer ("Layer 7") is the highest layer of the OSI model, and is responsible for enabling communication between applications, as well as for providing services to the user.

Question: 159

(★) Which is the PRIMARY focus of the ISO 27002 standard?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Information Security Management System (ISMS)

C. Risk Management

D. Application Security

Answer: B

Explanation/Reference:

ISO 27002 is a supplementary standard aimed at guiding implementation controls in order to maintain security controls for Information Security Management Systems (ISMS), as defined in ISO 27001. Among many other aspects, these security controls comprise application security. Risk management is an activity that is touched on in this standard, but is not its primary focus (it is the focus of the ISO 31000 standard). HIPAA is the United States law that governs the privacy

of healthcare information.

Question: 160

(★) Which of these different sub-masks will allow 30 hosts?

A. /26

B. /30

C. /27

D. /29

Answer: C

Explanation/Reference:

A subnet mask is a number that distinguishes between the network address and the host address. Subnetting divides a network into two or more subnets (see ISC2 Study Guide, chapter 4, module 1). To allow 30 hosts + 2 addresses for broadcast and network addresses. Thus, we are looking for the mask 255.255.255.224, or /27 using CIDR (Classless Inter-Domain Routing) notation. For 32 addresses, we need 5 bits and the mask /32 - log2(32) = /32 - 5 = /27. As for the remaining masks, /26 would result in 64 hosts, /29 in 8 hosts, and /30 in 4 hosts.

Question: 161

(★) Which of these statements about the security implications of IPv6 is NOT true?

A. Rules based on static IPv6 addresses may not work

B. IPv6's NAT implementation is insecure

C. IPv6 traffic may bypass existing security controls

D. IPv6 reputation services may not be mature and useful

Answer: B

Explanation/Reference:

IPv6 does not include network address translation (NAT), since many IP addresses are available. As a result, there is no NAT implementation, and so IPv6 can't actually have an insecure version. Rules based on static IPv6 addresses may not work, since IPv6 addresses are often dynamically assigned. Thus, certain security controls that rely on static address rules (such as firewalls or access controls) may not work in all cases. Reputation services are still relatively rare, and also somewhat less useful for IPv6 traffic. Finally, an organization needs to configure its security controls to handle IPv6 traffic adequately; otherwise, IPv6 traffic may bypass many existing IPv4 security tools (see ISC2 Study Guide, chapter 4,

module 3).

Question: 162

Which of these is a type of detective access control?

A. Bollards

B. Movement Sensors

C. Turnstiles

D. Firewalls

Answer: B

Explanation/Reference:

Detective controls alert us to security problems by constantly monitoring activity and recording information, so as to take immediate action in the event of a security control failure (such as bollards or turnstiles). Therefore, a movement sensor is considered a detective control, and is complementary to physical controls. Firewalls are network devices used to filter network traffic, and are thus considered technical controls. Logging and monitoring tools, such as Security Information and Event Management (SIEM), are detective access controls (see ISC2 Study Guide, chapter 1, module 3).

Question: 163

The name, age, location and job title of a person are all examples of:

A. Biometric factors

B. Attributes

C. Account permissions

D. Identity factors

Answer: B

Explanation/Reference:

Attributes such as a person's name, age, location, job title, and even characteristics such as height or hair color, may all be associated with their identity. None of these describe biometric factors used for authentication. Identity factors are something you know, are or have. Account permissions determine what an authenticated person (a user) can do, and not attributes related to the user's identity.

Question: 164

Which cloud service model provides the most suitable environment for customers who want to install their custom operating system?

A. SaaS

B. SLA

C. IaaS

D. PaaS

Answer: C

Explanation/Reference:

Infrastructure as a Service (IaaS) is a cloud service model that allows the customer to manage the computing resources (including the operating systems). Software as a Service (SaaS) is a model that provides customers with access to software applications (typically on a subscription-based or pay-per-use model) but does not allow them to access the underlying infrastructure. Platform as a Service (PaaS) is a service model that provides a platform for building, deploying and managing applications; however, like SaaS, it does not offer the ability to access the underlying infrastructure (including the operating system). An SLA is simply a service-level agreement (and not a cloud service deployment model) (see ISC2 Study Guide, chapter 4, module 3).

Question: 165

(★) Which of these statements is TRUE about cybersquatting?

A. Its an unethical practice but everyone does it

B. It is partially illegal practice

C. It is an illegal practice

D. It is s a legal practice

Answer: C

Explanation/Reference:

Cybersquatting (also known as domain squatting) is the practice of speculatively registering and then selling (typically at a high price) a domain name, with the intent of profiting from someone else's trademark. An example would be someone registering the domain name "mycompany.com" and then offering to sell it to the owner of the trademark "MyCompany" for a high price. Cybersquatting can cause confusion and damage to the trademark owner's brand, which is generally considered unethical and deceptive. Indeed, cybersquatting is an illegal practice under the United States'

Anticybersquatting Consumer Protection Act (ACPA), as well as under similar laws in other countries.

Question: 166

Which of these addresses is commonly reserved specifically for broadcasting?

A. 192.299.121.254

B. 192.299.121.0

C. 192.299.121.14

D. 192.299.121.255

Answer: D

Explanation/Reference:

IPv4 addresses are 32-bits represented as a sequence of four 8-bit integers separated by a dot. Addresses ending with 0 are reserved to specifically signify the network itself (and not a specific device on that network). In contrast, addresses ending in 255 are generally reserved for broadcasting to all devices on that network (see ISC2 Study Guide, chapter 4, module 1).

Question: 167

Which department in a company is NOT typically involved in a Disaster Recovery Plan (DRP)?

A. Executive

B. Financial

C. Public Relations

D. IT

Answer: B

Explanation/Reference:

Executives and Public Relations staff need to be aware of the company's Disaster Recovery Plan (DRP) to properly handle the expectations of the public, as well as of company stakeholders. IT personnel should be focused on helping businesses return to normal operations. A company's financial department is rarely involved in a disaster recovery plan, except when the issue at hand is directly connected to company finances (see Chapter 2 ISC2 Study Guide, module 3, under Components of a Disaster Recovery Plan).

Question: 168

Which of these pairs does NOT constitute Multi-Factor Authentication (MFA)?

A. Fingerprint and password.

B. Username and retina scan.

C. Password and username.

D. PIN and credit card.

Answer: C

Explanation/Reference:

Multi-Factor Authentication uses authentication from more than one factor. Passwords and usernames are not multifactor, since they are both 'something you know' (see ISC2 Study Guide, chapter 3, module 1).

Question: 169

Which method is COMMONLY used to map live hosts in the network?

A. Geolocation

B. Traceroute

C. Ping sweep

D. Wireshark

Answer: C

Explanation/Reference:

A ping sweep is a commonly used method to map live hosts in a network. A ping sweep involves sending a series of ping messages (ICMP Echo Request packets) to a range of IP addresses on a network so as to determine which hosts are currently online. Hosts that are online will respond with a reply message when a ping is sent to them. Collecting the replies makes it possible to map which hosts are currently online on the network (see ISC2 Study Guide, chapter 4, module 3).
The remaining options are not typically used to map live hosts in a network. Geolocation is a process for determining a device or user's physical location, based on information obtained from the device's IP or MAC address. Traceroute is a method to determine the sequence of hops that the packets took to a given IP address, so as to both map a network's topology and diagnose connectivity or routing issues. Finally, Wireshark is a network protocol analyzer tool that can be used to view and analyze packets' contents, including the IP addresses and hostnames.

Question: 170

A poster reminding the best password management practices is an example of which type of learning activity?

A. Awareness

B. Schooling

C. Education

D. Training

Answer: A

Explanation/Reference:

An awareness poster or campaign can be effective in engaging a user's attention and encouraging them to consider their password practices. Specific strategies include highlighting the risks associated with weak or easily guessable passwords (such as the risk of account compromise or data theft) and encouraging users to remember to use a password manager to store and manage their passwords securely. The primary goal of education is to help learners improve both their understanding of concepts and their ability to relate to them. Education about password management may involve learning how to create and manage passwords effectively. Training focuses on building proficiency in a set of skills. Methods such as lectures, workshops, and online courses can be considered training. Schooling is the process of teaching in a school, which may or may not include posters (see ISC2 Study Guide, chapter 5, module 4).

Question: 171

Which part of the CIA Triad will be PRIMARILY jeopardized in a Distributed Denial Of Service (DDOS) attack?

A. Accountability

B. Availability

C. Integrity

D. Confidentiality

Answer: B

Explanation/Reference:

Distributed Denial-of-Service (DDoS) attacks are malicious attempts to block businesses from their traffic by flooding a target server, service or network with malicious coordinated traffic generated by a wide number of systems on the internet. The goal of DDoS attacks is to compromise availability (see ISC2 Study Guide, chapter 1, module 1 and also chapter 4, module 3) . A DDoS attack does not target confidentiality, but it may accidentally compromise integrity. Accountability is the property that actions of an entity can be traced uniquely to that entity (according to NIST SP 800-

12), and is not directly threatened by DDoS attacks.

Question: 172

(★) What technology is MOST LIKELY to conserve the storage space required for video recordings?

A. Motion detection

B. PTZ

C. Facial recognition

D. Infrared cameras

Answer: A

Explanation/Reference:

Motion-detecting cameras record only when motion is detected, and thus help in reducing video storage requirements. A recording will occur more rarely in low-occupancy places (like data centers), thus conserving storage. In more heavily used areas, the impact on total storage space used will be negligible. Infrared cameras, facial recognition, and the ability to pan, tilt, and zoom (PTZ) a camera are important features, but more is needed to conserve storage space.

Question: 173

An organization that uses a layered approach when designing its security architecture is using which of these security approaches?

A. Zero trust

B. Defense in depth

C. Network Layers

D. Network Control Access

Answer: B

Explanation/Reference:

An organization that uses a layered approach when designing its security architecture is using a defense in-depth approach. In a defense in-depth approach, different layers of security controls may be implemented at different levels of the organization, such as at the network, application and user levels (see ISC2 Study Guide, chapter 4, module 3). Network control access refers to the process of controlling access to a network. Network layers refer to the different levels of a computer network, such as the network infrastructure, network applications and network devices. Zero trust is

a security strategy which assumes that all network traffic is potentially malicious and requires verification.

Question: 174

Which of these techniques will ensure the property of 'non-repudiation'?

A. Using a VPN

B. Passwords

C. Encryption

D. Digital signatures

Answer: D

Explanation/Reference:

Non-repudiation means ensuring that the sender cannot later deny having sent the message. Digital signatures provide an undeniable match between sender and digital signature. We can think of a digital signature as a Message Digest encrypted with an asymmetric key: first, the message hash is encrypted using the sender's private key; then, the message (possibly encrypted) previously encrypted message hash; finally, the recipient decrypts the signature with the sender's public key, and transfers the decrypted content to the same cryptographic hash. Non-repudiation is guaranteed because, if the output of the hash matches the decrypted hash, then the recipient knows that the message is not forged, and that no one else but the sender could have created that signature and sent that message (see ISC2 Study Guide, chapter 1, module 1).
A Virtual Private Network (VPN) creates a secure tunnel between endpoints, thereby ensuring confidentiality. However, without a digital signature, an attacker could still send a message over a secure channel and then deny having sent it.
Passwords are a mechanism for authentication, and are not typically used for non-repudiation. Some applications ask the sender to enter a password previously sent by the receiver to sign a message.
Finally, encryption is the cryptographic transformation of data in order to conceal its original meaning. This concept is distinct from non-repudiation. Consider the scenario where we may need to guarantee the non-repudiation of a plain (that is, non-encrypted) message.

Question: 175

(★) A USB pen with data passed around the office is an example of:

A. Data in motion

B. Data at rest

C. Data in transit

D. Data in use

Answer: B

Explanation/Reference:

Data at rest is stored data that resides on hard drives, on tapes, in the cloud, or on other storage media like (in this case) a USB pen. Data in processing (also called data in use) is actively used by a computer system. Data sent over a network is called data in motion. Data in transit is a term that does not usually apply to such a situation.

Question: 176

Suppose that an organization wants to implement measures to strengthen its detective access controls. Which one of these tools should they implement?

A. Patches

B. Encryption

C. IDS

D. Backups

Answer: C

Explanation/Reference:

Detective controls are a crucial component of a cybersecurity program, since they provide visibility into malicious activity, breaches and attacks on an organization's IT environment. An intrusion detection system (IDS) is a device or software application which monitors a network or systems for malicious activity or policy violations (meaning that it's a detective control) (see ISC2 Study Guide, chapter 4, module 1). Patches are corrective controls. Backups are compensating controls, since they provide redundancy for the information in a given system.

Question: 177

(★) Which of these is an example of a MAC address?

A. 00-51-02-1F-58-F6

B. 0051021f58

C. 10.23.19.49

D. 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888

Answer: A

Explanation/Reference:

All network devices have a 48-bit Media Access Control (MAC) address, represented as six groups of 8 bits values in

hexadecimal (see ISC2 Study Guide, chapter 4, module 1 - Understand Computer Networking). An example of a MAC address would be 00-51-02-1F-58-F6. An IPv4 address is a 32-bit address represented as a sequence of four 8-bit integers, an example of which would be 10.23.19.49. An IPv6 address is a 128-bit address represented as a sequence of eight groups of 16-bit hexadecimal values, an example of which would be 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888. The string 0051021f58 is a 40-bit WEP key consisting of 10 hexadecimal digits typically represented as a string of 5 ASCII characters. WEP keys are used to secure wireless networks, and can be either 40 bits or 104 bits in length, depending on the encryption mode that is used.

Question: 178

Which of these types of credentials is NOT used in multi-factor authentication?

A. Something you have

B. Something you know

C. Something you are

D. Something you trust

Answer: D

Explanation/Reference:

Authentication generally requires that users provide identity factors (that others can't not easily provide). Because no single factor is ever foolproof, multi-factor authentication typically uses one or several of the following (see ISC2 Study Guide, chapter 3, module 1):
'Something you know', such as a password or personal identification number (PIN);
'Something you have', such as a smart card or certificate;
'Something you are', which would be based on your physical characteristics, in which biometric reading may be used.
Some of the security literature mentions a fourth method based on 'something you do', such as a sample of handwriting, a gesture, or a voice print; that being said, no identity factor is ever based on 'something you trust'.

Question: 179

On an Incident Response team, which role acts as the team's main link to Senior Management?

A. Information security

B. Communications and public relations

C. Management

D. Technical expert

Answer: C

Explanation/Reference:

On most incident response teams, members of management or organizational leadership act as a primary conduit to senior management (see ISC2 Study Guide, chapter 2, module 1). The management team member also ensures that difficult or urgent decisions can be made without escalating authority. Communications and public relations staff focus on internal and external communications that typically differ from the direct conduit to senior management. Technical and information security experts are primarily concerned with undertaking incident response work.

Question: 180

Which of these is NOT an effective way to protect an organization from cybercriminals?

A. Removing or disabling unneeded services and protocols

B. Using firewalls

C. Using out-dated anti-malware software

D. Using intrusion detection and prevention systems

Answer: C

Explanation/Reference:

Using out-dated anti-malware software is NOT an effective way to protect an organization from cybercriminals. Anti-malware software (such as antivirus programs) are designed to detect and remove malware from computer systems and networks. To be effective, it is vital, instead, to ensure that running software is kept up-to-date with the latest security updates and definitions. Other effective ways to protect an organization from cybercriminals are:
Removing or disabling unneeded services and protocols;
Using intrusion detection and prevention systems;
Using firewalls.

Question: 181

Which of these CANNOT be a corrective security control?

A. Disaster Recovery Plan

B. Backups

C. Patches

D. Bollards

Answer: D

Explanation/Reference:

Corrective security controls are measures used to address security vulnerabilities or weaknesses already identified. Backups, patches, and Disaster Recovery Plans are all corrective security controls (see ISC2 Study Guide, chapter 3, module 2). Backups can help ensure that important information is not lost in the event of an incident. Patches can help fix vulnerabilities and improve security. Disaster Recovery Plans are administrative security controls that establish the corrective measures to be implemented in case of a disaster. Bollards are not typically considered a corrective security control

---

Question: 182

Which of these is included in an SLA document?

A. Instructions on data ownership and destruction

B. Instructions to detect, respond to, and limit the consequences of a cyber-attack

C. A plan to keep business operations going while recovering from a significant disruption

D. A plan to prepare the organization for the continuation of critical business functions

Answer: A

Explanation/Reference:

A Service Level Agreement (SLA) is a contract between a service provider and a customer which defines the level of service that the provider will deliver. It must include instructions on data ownership and destruction in order to ensure that sensitive data is properly protected. A set of instructions or procedures to detect, respond, and limit the consequences of a cyber-attack is called an Incident Response Plan (see ISC2 Study Guide chapter 2, module 1, under The Goal of Incident Response). A plan to sustain business operations while recovering from a significant disruption is called a Business Continuity Plan (see ISC2 Study Guide chapter 2, module 2, under The Importance of Business Continuity). A plan to prepare an organization for the continuation of critical business functions is called a Disaster Recovery Plan (see ISC2 Study Guide chapter 2, module 3, under The Goal of Disaster Recovery).

Question: 183

Which port number corresponds to the Simple Mail Transfer Protocol (SMTP)?

A. 161

B. 69

C. 25

D. 22

Answer: C

Explanation/Reference:

The Simple Mail Transfer Protocol (SMTP) is well-known for accepting connections on port 25, so as to receive unencrypted email messages. The more secure alternative is to use port 587 for SMTP by using Transport Layer Security (TLS), which encrypts the data between the mail client and the server (see ISC2 Study Guide, chapter 4, module 1)

Question: 184

Which type of attack attempts to mislead the user into exposing personal information by sending fraudulent emails?

A. Cross-Site Scripting

B. Denial of Service

C. Trojans

D. Phishing

Answer: D

Explanation/Reference:

A phishing attack emails a fraudulent message with the goal of tricking the recipient into disclosing sensitive information to the attacker (see ISC2 Study Guide, chapter 4, module 2). A Cross-Site Scripting attack tries to execute code on another website. Trojans are software that seem legitimate, but has hidden malicious functions. Trojans may be sent in a message, but are not themselves the message. A denial of service attack (DoS) compromises the availability of a system or service through a malicious overload of requests, thereby activating safety mechanisms that delay or limit the availability of that system or service.

Question: 185

Which of these is NOT a characteristic of the cloud?

A. Zero Customer Responsibility

B. Broad Network Access

C. Measured Service

D. Rapid Elasticity

Answer: A

Explanation/Reference:

The characteristics of the cloud, also known as the "five essential characteristics" of cloud computing, are (see ISC2

Study Guide, chapter 4, module 3):
Broad network access: Cloud resources, such as the internet, can be accessed over a network;
Rapid elasticity: Cloud resources can be scaled up or down quickly and automatically to meet changing demand;
Measured service: Cloud providers track and measure the use of resources, and users are typically charged based on their usage;
Resource pooling: Cloud providers pool resources (such as storage and computing power) and allocate them to users on demand;
On-demand self-service: Cloud users can access computing resources on demand without human intervention.
Finally, the cloud model is typically run under the shared responsibility model, where the provider is responsible for both maintaining the infrastructure and delivering the resources and services to the customer. In contrast, the customer uses the resources and services according to the terms of their agreement with the provider. Therefore, zero customer responsibility is NOT a characteristic of the cloud.

Question: 186

Which of these is a COMMON mistake made when implementing record retention policies?

A. Not categorizing the type of information to be retained

B. Not labeling the type of information to be retained

C. Applying the longest retention periods to the information

D. Applying shorter retention periods to the information

Answer: C

Explanation/Reference:

A common mistake in record retention is applying the longest retention period without taking into account the sensitivity or importance of the corresponding information. Retaining unnecessary data has considerable costs in terms of storage and management. Less important or sensitive information can have shorter retention periods, thereby allowing longer retention periods for more important or sensitive information (see ISC2 Study Guide, chapter 5, module 1).

Question: 187

Which type of security control does NOT include CCTV cameras?

A. Corrective

B. Deterrent

C. Preventive

D. Detective

Answer: A

Explanation/Reference:

CCTV cameras are considered a deterrent to criminal activity. In addition, combined with other sensors, they can detect movement, and thus are considered a detective control. Image recordings provide evidence after the fact. According to the NIST, preventive controls are measures to detect, deter and/or reduce an impact of a system. CCTV cameras are not corrective controls, as they are not deployed to repair detected errors or irregularities (see ISC2 Study Guide, chapter 3, module 2).

Question: 188

A security consultant hired to design the security policies for the PHI within an organization will be primarily handling:

A. Personal Health information

B. Public Health information

C. Procedural Health information

D. Protected Health information

Answer: D

Explanation/Reference:

PHI is an acronym that stands for Protected Health Information (see ISC2 Study Guide, chapter 1, module 1). The remaining options are incorrect.

Question: 189

Which of these cloud deployment models is a combination of public and private cloud storage?

A. Community

B. Private

C. Hybrid

D. Public

Answer: C

Explanation/Reference:

A hybrid cloud deployment model combines public and private cloud storage. For example: an organization might use private cloud storage for sensitive or proprietary data that needs to be kept confidential, while at the same time using

public cloud storage for less sensitive data or workloads, which are more suited to a shared infrastructure. This allows the organization to tailor its cloud storage strategy to meet the specific needs of its workloads, while at the same time taking advantage of the economies of scale and flexibility offered by public cloud storage (see ISC2 Study Guide, chapter 4, module 3).
Other types of cloud deployment models include the public cloud, where the infrastructure is owned and operated by a third-party provider and made available to the public; and the private cloud, where the infrastructure is owned and operated by a single organization and not made available to the public. Finally, a community cloud is a type of cloud infrastructure shared by organizations with similar needs, and is not made available to the public.

Question: 190

What is the primary goal of a Change Management Policy?

A. To standardize the creation of the organization's network and computer systems

B. To guarantee that systems are up to date with the latest security patch

C. To standardize the usage of the organization's network and computer systems

D. To guarantee that system changes are performed without negatively affecting business operations

Answer: D

Explanation/Reference:

The primary goal of a Change Management Policy is to realize the benefits of the system's changes while minimizing disruptions to business operations, namely by ensuring the integrity of the organization's systems and processes (see ISC2 Study Guide, chapter 5, module 3). Guaranteeing that systems have the latest security patches is the goal of a Patch Management Policy. A Networking Policy governs the usage of networks, and an Acceptable Use Policy governs the usage of computer systems. The creation of networks and computer systems in an organization is governed by the following:
Networking standards: cover the protocols, technologies, and practices used to create and operate networks, including local area networks (LANs), wide area networks (WANs) and the internet;
System development standards: guide the design, development and maintenance of both software and computer systems

---

Question: 191

Which of these is NOT a feature of a SIEM (Security Information and Event Management)?

A. Log auditing

B. Log encryption

C. Log consolidation

D. Log retention

Answer: A

Explanation/Reference:

Log auditing is not a feature of a SIEM (Security Information and Event Management). A SIEM typically provides the following features:
Log consolidation, which consists in collecting logs from various sources (like servers, firewalls or IDS/IPS) and then storing them in one central location.
Log retention, which consists in storing logs for a specific period (like 90 days), so as to allow security analysts to keep track of and investigate past events.
Log encryption, which is an optional feature that safeguards the confidentiality of log data.
Log analysis, which involves identifying patterns, trends and anomalies related to security events, in or close to real time.
Though related to log analysis, log auditing specifically refers to ensuring the reliability and trustworthiness of log data for debugging, performance monitoring, security, and compliance purposes. This is usually done on a periodic basis (not in real-time).

Question: 192

Which of these technologies is the LEAST effective means of preventing shared accounts?

A. Requiring a one-time password via an application

B. Requiring one-time passwords via a token

C. Password complexity requirements

D. Requiring biometric authentication

Answer: C

Explanation/Reference:

Password complexity requirements do not prevent the sharing of complex passwords, making it the least effective option from the above list. One-time passwords are hard to share, making it far less convenient to share accounts. Biometric authentication requires the registered user to actually be present when signing in. However, in some cases, such as fingerprint systems, multiple users could each register a valid fingerprint for a single account (see ISC2 Study Guide, chapter 3, module 1).

Question: 193

Which of these is NOT a best practice in access management?

A. Trust but verify

B. Periodically assessing whether user permissions still apply

C. Giving only the right amount of permission

D. Requesting a justification when upgrading permission

Answer: A

Explanation/Reference:

The "Trust but verify" model is a method of threat protection that involves granting privileged accounts access to the network and other resources, while at the same time verifying their actions and activities. However, over time, this model was found to have limitations that expose organizations to a wide array of security threats. Therefore, "Trust but verify" is being progressively abandoned in favor of the Zero Trust model. The remaining options are all best practices of access management.

Question: 194

(★) When analyzing risks, which of these activities is required?

A. Accepting all evaluated risks

B. Identifying risks associated with loss of confidentiality

C. Determining the likelihood of occurrence of a set of risks

D. Selecting the appropriate controls

Answer: C

Explanation/Reference:

Determining the likelihood of occurrence of a set of risks involves estimating the likelihood that the identified risks will occur, along with the potential impact it could have on the organization. Once the likelihood of occurrence has been determined, the next step is to select the appropriate controls to mitigate those risks, such as encryption, access controls, or administrative controls (like policies and procedures). Identifying the risks associated with loss of confidentiality (such as unauthorized access or disclosure of sensitive data) is important but insufficient on its own, as many other risks must also be considered. Finally, accepting all evaluated risks is typically not advisable, as some risks should be mitigated or eliminated. Only risks at a residual level acceptable to the organization should be accepted.

Question: 195

Which of these exercises goes through a sample of an incident step-by-step, validating what each person will do?

A. A simulation exercise

B. A walk-through exercise

C. A tabletop exercise

D. A checklist exercise

Answer: B

Explanation/Reference:

A walk-through exercise reviews each step of the incident, in order to ensure that every team member knows exactly what they should do, and how they should do it. In tabletop exercises, team members are given a scenario and asked how they would respond, as well as what tasks they believe would be relevant. A simulation exercise attempts to recreate an actual incident so as to thoroughly test responses. Checklists are essential in incident response, but aren't actually a specific type of exercise.

Question: 196

(★) Which of these types of documents is usually THE LEAST formal?

A. Standards

B. Guidelines

C. Policies

D. Regulations

Answer: B

Explanation/Reference:

Of the document types listed above, guidelines are generally the least formal. Guidelines provide recommendations or suggestions for achieving a particular goal or objective. They are often less formal than standards and policies, and are used to specify best practices or recommended approaches. Standards are generally more formal than guidelines, and describe the requirements, specifications or characteristics that a product, service or system should possess. Policies are usually more formal than guidelines, and outline the rules or principles that an organization or governing body has established to guide the actions of its members or employees. Regulations are typically created by government agencies or regulatory bodies, and are enforceable by law. They are generally more formal than guidelines.

Question: 197

A backup that captures the changes made since the latest full backup is an example of:

A. A differential backup

B. An incremental backup

C. A backup snapshot

D. A full backup

Answer: A

Explanation/Reference:

A differential backup is a backup that captures the changes made since the latest full backup. Incremental backups capture changes since the latest backup (which can be full or incremental), and snapshots are live copies of a system. Neither incremental backups nor snapshots necessarily capture changes since a full backup (see ISC2 Study Guide, chapter 5, module 1).

Question: 198

A high-level executive of an organization receives a malicious email that tries to trick him. Which attack is the perpetrator using?

A. DDOS

B. Whaling

C. Phishing

D. Spear phishing

Answer: B

Explanation/Reference:

When executives receive malicious emails that try to trick them, the attackers are likely attempting a whaling attack (see ISC2 Study Guide, chapter 4, module 2). Whaling is a type of spear phishing, and, in turn, spear phishing is a type of phishing. Whaling is a spear phishing attack targeted at a group of high-level executives, or at other influential individuals inside the organization. Spear phishing is a targeted attack in which the attacker uses email or other digital communication to trick a specific individual or group into divulging sensitive information. Phishing is an attack in which attackers send fake emails or text messages that seem to come from legitimate sources, so as to trick the recipient into revealing sensitive information or clicking on a malicious link.
Finally, a distributed denial-of-service (DDoS) attack is a type of attack in which a large amount of malicious traffic is directed at a specific target (systems, not individuals), such as a website or server, in an attempt to overwhelm it, thus making it unavailable.

Question: 199

What does redundancy mean in the context of cybersecurity?

A. Designing systems with robust components, so that the organization has more attack resilience

B. Conceiving systems with only the most necessary components, so that the organization has just the necessary risks.

C. Conceiving systems with less attack surface, so that the attacker has less chance of success

D. Conceiving systems with duplicate components so that, if a failure occurs, there will be a backup

Answer: D

Explanation/Reference:

In cybersecurity, redundancy refers to conceiving systems for resilience with duplicate components so that, if a failure occurs, the redundant component will take over and maintain operations, thereby helping to prevent outages or other disruptions (see ISC2 Study Guide, chapter 4, module 3). Examples of this are redundant servers, redundant network links, and redundant power supplies. Redundancy is also effective against attacks, since the attacked nodes can be quarantined and then replaced by the backup

---

Question: 200

When a company collects PII, which policy is required?

A. Remote Access Policy

B. GDPR

C. Privacy Policy

D. Acceptable Use Policy

Answer: C

Explanation/Reference:

A Privacy Policy outlines the data security mechanisms which ensure that customer data is protected; namely, how Personal Identifiable Information (PII) is collected, stored and processed (see ISC2 Study Guide, chapter 5, module 3). The General Data Protection Regulation (GDPR) is a data protection and privacy regulation for the European Union and the European Economic Area (not a policy). An Acceptable Use Policy (AUP) defines the guidelines and limitations that users must agree on while accessing the organization's network, computer systems or other related resources. Finally, the Remote Access Policy (RAP) defines acceptable methods of remotely connecting to an organization's internal network.

Question: 201

Which type of attack PRIMARILY aims to consume all the available resources, thereby making an organization's service inaccessible to its intended users?

A. Trojans

B. Cross-Site Scripting

C. Denial of Service

D. Phishing

Answer: C

Explanation/Reference:

A denial of service attack (DoS) compromises the availability of a system or service through a malicious overload of requests, thereby activating safety mechanisms that delay or limit the availability of that system or service. As a result, systems or services become temporarily inaccessible to their intended users (see ISC2 Study Guide, chapter 4, module 2). Trojans, phishing and cross-site scripting attacks try to gain access to the system or data covertly, and therefore do not primarily aim at compromising the system's availability.

Question: 202

Which one of these tools is MOST likely to detect an XSS vulnerability?

A. Network vulnerability scanner

B. Static application test

C. Intrusion detection system

D. Web application vulnerability scanner

Answer: D

Explanation/Reference:

Intrusion detection systems are designed to detect attacks, not vulnerabilities. The remaining three tools could all possibly discover cross-site scripting (XSS) vulnerabilities. However, a web application vulnerability scanner is the one that's most likely to detect it, since it is specifically designed to test web applications (see ISC2 Study Guide, chapter 4, module 3).

Question: 203

Which kind of physical access control is LESS effective at preventing unauthorized individual access to a data center?

A. Turnstiles

B. Barriers

C. Fences

D. Bollards

Answer: D

Explanation/Reference:

Bollards are short, vertical posts that block vehicles from accessing a data center. They are, however, ineffective at preventing access to individuals. Fences can be placed around the perimeter of the data center, so as to block unauthorized access and deter potential intruders. Barriers such as gates, walls or barricades can be used to block access to the data center. Finally, turnstiles can be used to control access to a data center, namely by allowing entry only to authorized individuals.

Question: 204

Which of these is NOT a type of malware?

A. Trojan

B. Worm

C. Spoofing

D. Rootkit

Answer: C

Explanation/Reference:

Spoofing is not a type of malware. Spoofing is an attack whose primary goal is to gain access to a target system through a falsified identity (see ISC2 Study Guide, chapter 4, module 2). Trojans, rootkits and worms are all different types of malware. A Trojan is a type of malware that disguises itself as a legitimate program or file. A Rootkit is a type of malware that hides itself to go unnoticed in the compromised system, or in the victim's computer. A Worm is a type of malware designed to replicate itself and spread to other computers, often over a network.

Question: 205

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

A. Privileged Accounts

B. Separation of Duties

C. Least Privilege

D. Defense in Depth

Answer: C

Explanation/Reference:

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.
