# ➢Dumpsgate ISC2 CC Dumps

## Question: 1

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

A. Protect society, the common good, necessary public trust and confidence, and the infrastructure
B. Provide active and qualified service to principal
C. Advance and protect the profession
D. Act honorably, honestly, justly, responsibly and legally

**Answer: B**

**Explanation:**
The Code of Ethics states, "Provide diligent and competent service to principals," not "Provide active and qualified service to principals."; all other options are valid canons of the Code of Ethics (see ISC2 Study Guide, Domain 1). "Provide active and qualified service to principals" is not listed among the ISC2 ethical canons, which focus on broader societal, professional and ethical guidelines rather than specific service obligations to principals.

The other options are incorrect because they directly reflect ISC2's ethical canons. "Protect society, the common good, necessary public trust, and infrastructure" emphasizes the responsibility of cybersecurity professionals to protect broader societal interests. "Act honorably, honestly, fairly, responsibly, and legally" outlines the personal integrity and ethical behavior expected of professionals. "Advance and protect the profession" encourages actions that enhance the credibility and standards of the cybersecurity field. Each of these principles is closely aligned with ISC2's commitment to ethics and professional conduct in cybersecurity.

**Domain**
Understand ISC2 Code of Ethics

## Question: 2

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

A. Security cameras
B. Remote control electronic locks
C. Biometric access controls
**D.** Firewalls

**Answer: D**

**Explanation:**
Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules to create a barrier between a trusted internal network and untrusted external networks, such as the Internet, to prevent unauthorized access to the network. Firewalls are not physical controls; they are a type of technical control.

For example, an organization might use a firewall to block incoming connections from certain IP

addresses that are known to be associated with malicious activity. This setup helps protect the network from unauthorized access, viruses, or denial-of-service attacks. The firewall acts as a filter, allowing or blocking traffic based on the network administrator's set of security rules.

On the other hand, security cameras, lighting, and guards are all examples of physical security controls. Security cameras monitor and record physical activity in and around a facility. Lighting enhances visibility and can deter criminal activity by making it difficult for intruders to hide. Guards are personnel employed to protect property and individuals by maintaining a physical presence to prevent and deter illegal or unauthorized activity. Each of these controls directly impacts the physical security of an environment by adding layers of protection against physical threats.

**Domain**

Understand Security Controls

## Question: 3

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

A. Cross-Site Scripting
B. Trojans
C. Phishing
**D.** Denials of Service

**Answer: C**

**Explanation:**

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

**Domain**

Understand Network (Cyber) Threats and Attacks

## Question: 4

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

A. Useful
B. Deterministic
C. Reversible
**D.** Unique

**Answer: C**

**Explanation:**

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

**Domain**
Understand Data Security

## Question: 5

Which physical access control would be MOST effective against tailgating?

A. Turnstiles
B. Barriers
C. Locks
**D.** Fences

**Answer: A**

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

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

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

**Domain**
Understand Physical Access Controls

## Question: 6

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

A. Cross-Site Scripting
B. Phishing
C. Trojans
**D.** Rootkits

**Answer: C**

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

**Domain**
Understand Network (Cyber) Threats and Attacks

## Question: 7

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

A. Threat
B. Vulnerability
C. Bug
**D.** Risk

**Answer: B**

**Explanation:**
A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. This term is used to identify the security gaps or flaws in an organization's infrastructure, software, or processes.

For example, consider a software application that does not properly validate user input. This vulnerability could allow an attacker to inject malicious SQL queries into the system (SQL injection), potentially leading to unauthorized access to sensitive data stored in the database. This scenario illustrates how a specific vulnerability in the system (improper input validation) can be exploited to compromise security.

A threat, on the other hand, is a potential cause of an unwanted incident that could damage a system or an organization. It does not describe the vulnerability, but rather the potential danger of exploiting it. Risk is the potential for loss, damage, or destruction of assets due to a threat that exploits a vulnerability. It involves the assessment of both the likelihood and impact of an incident. Finally, a bug is a term often used to describe an error, flaw, or fault in software that causes it to produce an incorrect or unexpected result, but does not necessarily imply a security risk or vulnerability.

**Domain**
Understand the Risk Management Process

## Question: 8

Which are the components of an incident response plan?

A. Preparation → Detection and Analysis → Containment, Eradication and Recovery → Post-Incident Activity
B. Preparation → Detection and Analysis → Recovery → Containment → Eradication → Post-Incident Activity
C. Preparation → Detection and Analysis → Containment → Eradication → Post-Incident Activity → Recovery
D. Preparation → Detection and Analysis → Eradication → Recovery → Containment → Post-Incident Activity

**Answer: A**

**Explanation:**
The components commonly found in an incident response plan are (in this order): Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-Incident Activity (see ISC2 Study Guide, Domain 2).

• Preparation: Establish policies, tools, and procedures before incidents occur.

• Detection and Analysis: Identify and investigate the nature of the cybersecurity incident.

• Containment: Limit the spread of the incident to minimize damage.

• Eradication: Remove the threat completely from the affected systems.

• Recovery: Restore and validate system functionality for normal operations.

• Post-Incident Activity: Review and improve incident handling processes and defenses.

**Domain**
Understand Incident Response

## Question: 9

Which of the following is an example of 2FA?

A. Keys
B. Passwords
C. Badges
D. One-Time passwords (OTA)

**Answer: D**

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

**Domain**
Understand Physical Access Controls

## Question: 10

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

A. Phishing
B. Rootkits
C. Cross-Site Scripting
**D.** Trojans

**Answer: B**

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

**Domain**
Understand Network (Cyber) Threats and Attacks

## Question: 11

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

A. The Business Impact Analysis
B. The Business Continuity Plan
C. The Business Impact Plan
D. The Disaster Recovery Plan

**Answer: D**

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

**Domain**
Understand Disaster Recovery (DR)

## Question: 12

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

A. Fences
B. Barriers
C. Locks
**D.** Turnstiles

**Answer: C**

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

**Domain**
Understand Physical Access Controls

## Question: 13

Which are the three packets used on the TCP connection handshake?

A. Discover → Offer → Request
B. Offer → Request → ACK
C. SYN → ACK → FIN
D. SYN → SYN/ACK → ACK

**Answer: D**

**Explanation:**
TCP uses a three-way handshake to establish a reliable connection by exchanging three packets with

the SYN, SYN/ACK and ACK flags. Although SYN, ACK and FIN are valid TCP packet flags, the sequence SYN → ACK → FIN is not the TCP handshake. Both the sequences Discover → Offer → Request and Offer → Request → ACK are used in DHCP (but are still incomplete, since DHCP is a four-way handshake).

**Domain**

Understand Computer Networking

## Question: 14

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

A. SNMP
B. TCP
C. UDP
**D.** SMTP

**Answer: B**

**Explanation:**

Transmission Control Protocol, or TCP, uses a three-way handshake mechanism to establish a reliable connection between two devices. The process has three steps: SYN (synchronize), SYN-ACK (synchronize-acknowledge), and ACK (acknowledge). This handshake ensures that both the sender and receiver are ready to send data and that a reliable channel for communication has been established.

For example, when a user accesses a Web site, the user's computer (client) sends a SYN packet to the server to request a connection. The server responds with a SYN-ACK packet to acknowledge the request and simultaneously sends its own SYN. Finally, the client sends an ACK packet back to the server. Once this handshake is complete, data transmission begins, ensuring that both parties are synchronized and ready to communicate.

In contrast, UDP (User Datagram Protocol) is a connectionless protocol that does not use a handshake mechanism, making it faster but less reliable than TCP. UDP sends packets without establishing a reliable channel, which is suitable for applications where speed is more important than reliability. Then, SMTP (Simple Mail Transfer Protocol) is used to send email, not to establish a reliable connection. Finally, SNMP (Simple Network Management Protocol) is used for network management and monitoring, not for establishing a connection.

**Domain**

Understand Computer Networking

## Question: 15

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

A. Risk mitigation
B. Risk transfer
C. Risk tolerance
**D.** Risk avoidance

**Answer: B**

**Explanation:**

Risk transfer is a risk management strategy in which the financial consequences of a risk are shifted to another party, typically through insurance.

For example, a company might purchase cyber liability insurance to cover the costs associated with a data breach, including legal fees, notification costs, and remediation efforts. This strategy allows the company to more effectively manage its risk exposure by transferring the potential financial impact to the insurer.

With respect to the other options, risk avoidance involves eliminating the risk by discontinuing the activity that creates it. For example, a company might decide not to store customer credit card information to avoid a data breach. Risk mitigation involves implementing measures to reduce the likelihood or impact of a risk, such as installing firewalls and encryption. Risk tolerance refers to the level of risk an organization is willing to accept without taking further action. Unlike risk transfer, these options do not involve shifting the financial consequences of a risk to another party.

**Domain**

Understand Security Controls

## Question: 16

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

A. Vulnerability Management
B. Inventory Management
C. Change Management
D. Configuration Management

**Answer: C**

**Explanation:**

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

**Domain**

Understand Security Policy Best Practices

## Question: 17

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

A. Protect society, the common good, and the infrastructure
B. Advance and promote the profession
C. Act honorably, honestly, safely and legally
D. Provide diligent and competent service to principals

**Answer: D**

**Explanation:**

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

**Domain**

Understand ISC2 Code of Ethics

## Question: 18

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

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

**Answer: A**

**Explanation:**

Avoid apparent or actual conflicts of interest. This principle is critical for ISC2 professionals because it ensures that they maintain their professional integrity and trustworthiness by avoiding situations in which their personal interests may conflict with their professional duties or the interests of their clients (see the ISC2 Code of Ethics).

For example, a cybersecurity consultant working for a client should not own a significant amount of stock in a competing company that could benefit from the consultant's decisions or actions.

The other options, while important, do not directly address the principle of avoiding conflicts of interest. Taking care not to harm the reputation of other professionals focuses on maintaining professional relationships and reputations, treating all members fairly relates to equity and justice in professional interactions, and promoting understanding of security measures deals with advocacy and education in cybersecurity practices.

**Domain**

Understand ISC2 Code of Ethics

## Question: 19

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

A. Help Desk
B. System Administrator
C. External Worker
**D.** Security Analyst

**Answer: C**

**Explanation:**

Typically, external workers should not have access to privileged accounts, due to the possibility of misuse. The Help Desk (or IT Support Staff) may have to view or manipulate endpoints, servers and applications platforms using privileged or restricted operations. Security analysts may require fast access

to the IT infrastructure, systems, endpoints and data environment. By definition, systems administrators require privileged accounts, since they are responsible for operating systems, deploying applications, and managing performance.

**Domain**

Understand Access Control Concepts

## Question: 20

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

A. DAC
B. ABAC
C. MAC
**D.** RBAC

**Answer: C**

**Explanation:**

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

**Domain**

Understand Logical Access Controls

## Question: 21

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

A. DHCP
B. UDP
C. TCP
**D.** SNMP

**Answer: C**

**Explanation:**

The Transmission Control Protocol (TCP) is designed to provide reliable, orderly, and error-tested packet delivery between applications running on hosts communicating over an IP network. TCP is preferred when there is no time constraint because it ensures that all data packets are delivered accurately and in the correct order, making it ideal for applications where data integrity is critical.

In contrast, UDP (User Datagram Protocol) is a simpler, message-based protocol that does not guarantee the delivery or order of messages, making it less reliable than TCP for applications that require high reliability and data integrity. DHCP (Dynamic Host Configuration Protocol) is a protocol for

dynamically assigning IP addresses to devices on a network; it does not directly handle data transmission between devices. Finally, SNMP (Simple Network Management Protocol) is used for network management and monitoring, not general data transfer.

**Domain**

Understand Computer Networking

## Question: 22

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

A. Standards
B. Policies
C. Procedures
**D.** Regulations

**Answer: C**

**Explanation:**

Procedures are detailed, step-by-step instructions that explain how to carry out a specific task in accordance with departmental or organizational policies. For example, a procedure might outline the steps for setting up a secure network connection, including the specific settings to use, the order in which to perform the steps, and how to verify that the connection is secure.

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, Domain 1).

**Domain**

Understand Governance Processes

## Question: 23

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

A. Cross Site Scripting
B. Side Channels
C. Trojans
**D.** Denial of Service

**Answer: B**

**Explanation:**

A side-channel attack is a passive and non-invasive attack that aims to extract information from the specific physical implementation of a running system. This attack uses indirect information such as power consumption, electromagnetic leakage, or even sound to extract secret data.

Following the above definition, consider the following example. In a laboratory setting, a cybersecurity researcher could perform a side-channel attack on a cryptographic device by monitoring its power consumption while it processes data. By analyzing the power consumption patterns during encryption, the researcher can infer the encryption key being used without having direct access to the cryptographic data or algorithms.

As for the other options, it is important to distinguish side-channel attacks from other types of threats. Cross-site scripting (XSS) is a vulnerability commonly found in web applications that allows attackers to inject client-side scripts into web pages viewed by other users. Denial of Service (DoS) is an attack designed to disrupt a network or service, making it inaccessible to its intended users. Trojans, on the other hand, are malicious programs that masquerade as legitimate software and allow unauthorized control of a computer. This is different from side-channel attacks, which exploit hardware emissions or power consumption to extract information.

**Domain**

Understand Network (Cyber) Threats and Attacks

## Question: 24

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

A. Inventory
B. Audit logs
C. Baselines
**D.** Updates

**Answer: B**

**Explanation:**

The elements of system security configuration management are inventories, baselines, updates, and patches. While audit logs are critical to security because they provide a record of who has accessed a system and what actions they have taken, they are not a specific element of system security configuration management.

Audit logs can be generated by the Verification and Audit process. However, Verification and Audit is a Configuration Management procedure. It is not an element (see the ISC2 Study Guide, Domain 5).

Configuration Management focuses on managing software and hardware configurations to maintain systems in a desired, secure state. For example, an organization might use configuration management tools to automatically apply software updates as they become available. This ensures that systems are not vulnerable to known vulnerabilities.

Inventorying, baselining, and updating are integral parts of system security configuration management. Inventory involves a detailed record of all hardware and software assets, which is essential to understanding what needs to be secured and managed. In particular:

• Baselines refer to specifications or standards that are considered secure for systems, against which current configurations can be compared to detect deviations or unauthorized changes.

• Updates refer to the application of patches or software updates to ensure that security features are current and vulnerabilities are addressed.

• Inventory Management aims to ensure that all assets are accounted for and properly managed.

**Domain**

Understand Security Awareness Training

## Question: 25

Which of the following are NOT types of security controls?

A. System-specific controls
B. Common controls
C. Storage controls
**D.** Hybrid controls

**Answer: C**

**Explanation:**

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

**Domain**

Understand Security Controls

## Question: 26

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

A. DMZ
B. Internal Network
C. Intranet
**D.** VPN

**Answer: A**

**Explanation:**

In Cybersecurity, a DMZ (demilitarized zone), is an additional layer of security for an organization's local area network (LAN); it is an isolated subnetwork that separates the internal network from the external Internet. This area contains outward-facing services, such as a Web server, and serves as a buffer zone. It prevents external users from having direct access to an organization's internal servers and data.

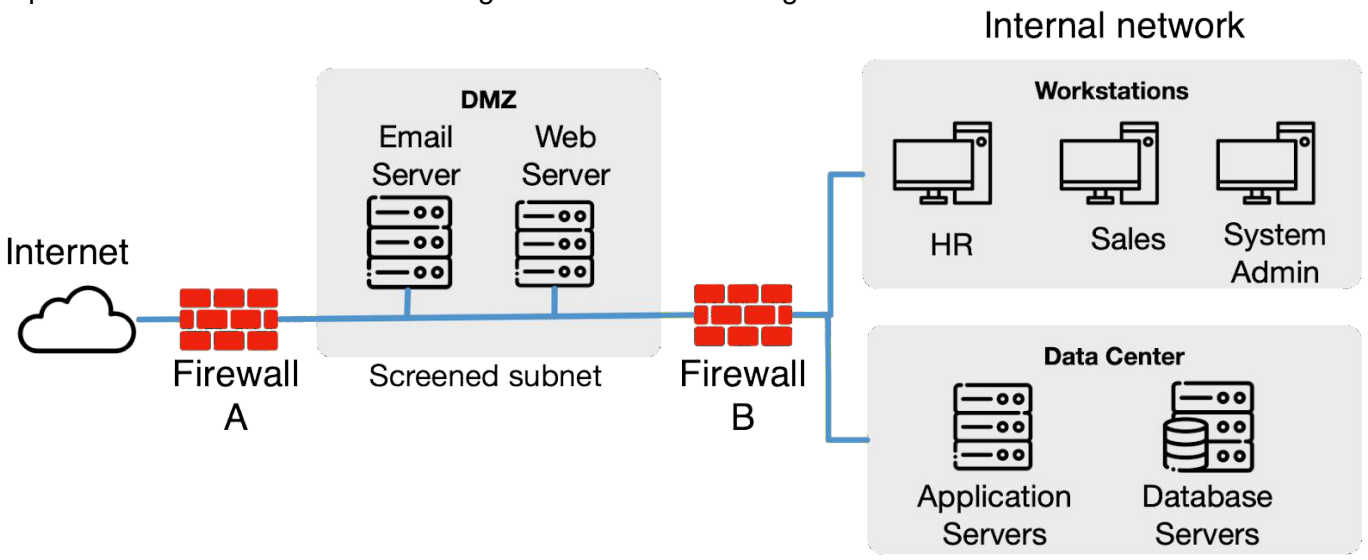



**Illustration of the creation of a network buffer zone, known as a demilitarized zone (DMZ), to enhance security.**

For example, suppose an organization creates a DMZ that hosts publicly accessible servers, such as the e-mail server and Web server, that must be accessible from the Internet, while limiting access to the

internal network. As shown in the figure, traffic from the external network (Internet) is separated from the internal network (intranet and data center). Firewall A (left) controls and filters inbound and outbound traffic to the DMZ from the Internet. Firewall B (right) controls and filters traffic between the DMZ and the internal network (intranet and data center).

As for the remaining options, an internal network is intended for traffic within an organization and is protected from external access, making it inappropriate for hosting services intended for public access. An intranet is a type of internal network designed specifically for use within the organization and hosts information and services that are not intended for external users. Finally, a VPN, or Virtual Private Network, creates a secure connection over the Internet between remote users and the network; it is not a place to host services, but rather a tunnel to securely access them. Therefore, placing a Web server that needs to be accessible from the Internet inside a VPN is not consistent with its intended use.

**Domain**

Understand Network Security Infrastructure

## Question: 27

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

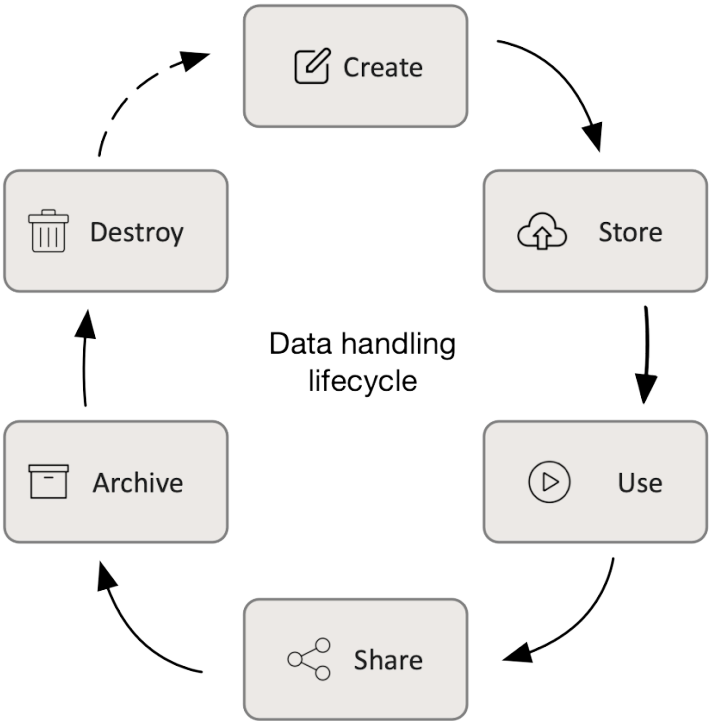
A. Create → Use → Store → Share → Archive → Destroy
B. Create → Share → Store → Use → Archive → Destroy
C. Create → Share → Use → Store → Archive → Destroy
D. Create → Store → Use → Share → Archive → Destroy

**Answer: D**

**Explanation:**

According to ISC2, there are six phases in the data lifecycle (create → store → use → share → archive → destroy). Each phase addresses a specific aspect of data management and ensures that data is managed appropriately from its creation to its eventual destruction.

For example, an organization may create customer data when a new account is opened, store it in a secure database, use it for customer service, share it with authorized personnel, archive it for future reference, and finally destroy it when it is no longer needed.




**The secure data handling lifecycle**
The diagram illustrates of the successive stages that data passes through during its existence. Each stage has specific security requirements to ensure proper data handling and compliance. Specifically, the stages are:
1. Create Stage. Involves generating new data through various means, such as data entry, collecting data from external sources, collecting data from sensors, or creating digital documents and files (examples: writing a report, filling out a form, generating logs from a system, capturing images or video).

2. Storage Stage. Data is securely stored and organized in databases, data warehouses, cloud storage, or physical storage media so that it can be easily accessed and retrieved when needed.

3. Usage Stage. Data is accessed and used for various purposes such as analysis, decision making, operations, or reporting. The integrity and accuracy of the data are critical at this stage (examples: analyzing sales data, using customer information for marketing campaigns, querying a database to generate reports).

4. Share Stage. Data is shared with authorized people or systems. This stage ensures that data is transmitted securely and reaches the intended recipients without unauthorized access or breaches (examples: reports can be emailed, documents can be shared through collaboration tools, and data can be distributed to other systems through APIs).

5. Archive phase. When data is no longer actively used, but needs to be retained for future reference or compliance purposes, it is archived. Archiving involves moving data to a secure, long-term storage solution (examples: moving old financial records to an archive system, storing historical data in a tape backup, keeping inactive customer records in an archive database).

6. Destruction phase. This final phase involves the secure destruction of data to ensure that sensitive information is permanently erased and cannot be recovered or misused (examples include shredding physical documents, securely deleting digital files, degaussing hard drives, and using data wiping

software to erase data from storage devices).
**Domain**
Understand Data Security

## Question: 28

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

A. DAC
B. ABAC
C. RBAC
**D.** MAC
**Answer: C**
**Explanation:**
The RBAC (or Role-Based Access Control) model is well known for managing access to objects based on the roles of individual users within the organization. It assigns permissions to specific roles, and users are then granted access based on their assigned roles. This model simplifies administration and ensures that users only have access to the information they need to do their jobs.

To reinforce the above about the RBAC model, imagine that an RBAC system is used to assign different access rights to roles such as doctors, nurses, and administrative staff in a hospital. A nurse might have access to a patient's medical records but not to financial details, while an accountant might have access to financial records but not to medical information. This model ensures that each employee has access to only the data they need for their role, improving security and privacy.

In contrast, MAC (or Mandatory Access Control) is wrong because it is based on fixed security attributes assigned to both resources and users, and access decisions are made by comparing these attributes. DAC (or Discretionary Access Control) allows the owner of the resource to decide who can access it, which is not necessarily based on the user's role. Finally, ABAC (or Attribute-Based Access Control) uses a variety of attributes (user, resource, environment) to determine access, which is more flexible and context-aware than role-based.
**Domain**
Understand Logical Access Controls

## Question: 29

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

A. Non-repudiation
B. Accessibility
C. Authentication
**D.** Confidentiality
**Answer: D**
**Explanation:**
Confidentiality, Integrity and Availability are known as the CIA triad, from the model that guides policies for information security. Confidentiality is the property of data or information not being made available or

disclosed, which leads to sensitive information being protected from unauthorized access.

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

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

**Domain**

Understand the Security Concepts of Information Assurance

## Question: 30

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

A. Hubs
B. Routers
C. SIEM
**D.** Firewalls

**Answer: C**

**Explanation:**

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

**Domain**

Understand Network (Cyber) Threats and Attacks

## Question: 31

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. Change Management Policy
B. BYOD
C. AUP
**D.** Privacy Policy

**Answer: B**

**Explanation:**

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

**Domain**
Understand Network Security Infrastructure

## Question: 32

Which of these is NOT a change management component?

A. Rollback
B. Governance
C. Approval
**D.** RFC
**Answer: B**
**Explanation:**
All significant change management practices address typical core activities: Request For Change (RFC), Approval, and Rollback (see ISC2 Study Guide, Domain 5). Governance is not one of these practices.

Governance generally refers to the system of rules, practices, and processes by which an organization is guided and controlled.

The remaining options are actually components of Change Management. A Request for Change (RFC) is a formal proposal for a change to a system or service that initiates the change process by outlining the proposed change. Another component is approval by relevant stakeholders or a Change Advisory Board prior to implementation. Rollback is a contingency plan to return to a previous state if the change implementation fails or produces undesirable results (this is critical to ensure system stability when new changes cause problems).
**Domain**
Understand Security Policy Best Practices

## Question: 33

How many layers does the OSI model have?

A. 7
B. 6
C. 4
**D.** 5
**Answer: A**
**Explanation:**
The Open Systems Interconnection (OSI) model has seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer performs a specific function in the process of communicating over a network (see ISC2 Study Guide, Domain 4).


**A side-by-side illustration of the layers of the OSI and TCP/IP network stack models**