ISC2 SSCP - Quiz Questions with Answers

Domain 1: Security Concepts and Practices

1.

Which of the following defines eight privacy principles?

- **OECD**
- GDPR
- PCI DSS
- HIPAA

Correct Answer: OECD

The Organization for Economic Cooperation and Development (OECD) defines eight privacy principles used worldwide. GDPR, PCI DSS, and HIPAA are all privacy-related regulations.

2.

Which of the following is NOT something that is useful to assess or estimate for an information systems asset?

Depreciation

Value

Cost

Loss or impact

Correct answer: Depreciation

The value, cost, and loss or impact are valuable to estimate or assess for an information systems asset. Depreciation is related to the value of an asset.

3.

A keycard-enabled smart lock on a door is an example of what type of control?

- **Physical**
- Technical
- Logical
- Administrative

Correct answer: Physical

Locks manage physical access, so they are physical risk mitigation controls. Technical/logical controls such as access controls manage risk on a computer. Administrative controls are policies and procedures.

4.

Which of the following describes the terms of the relationship between a service provider and customer?

- **SLA**
- NDA
- KPI
- AUP

Correct answer: SLA

An SLA (Service Level Agreement) is a formal document that defines the terms of the relationship between a service provider and a customer. It specifies the expected level of service, performance metrics, responsibilities, and remedies for any breaches of the agreement. The SLA is key to outlining what the customer can expect from the service provider and what actions will be taken if those expectations are not met.

A Non-Disclosure Agreement (NDA) protects the sensitive information disclosed by one or both parties from disclosure.

Key Performance Indicators (KPIs) are a metric by which success is measured.

An Acceptable Use Policy (AUP) describes how corporate systems can be used.

5.

Access control lists (ACLs) and firewalls are examples of what type of risk mitigation control?

Logical

Physical

Deterrent

Administrative

Correct answer: Logical

Logical controls, also known as technical controls, involve the use of software and hardware to protect information systems. This includes mechanisms like firewalls, encryption, intrusion detection systems, software Group Policy Objects, and access control lists (ACLs) that enforce access policies and safeguard digital information.

Physical controls are measures that protect physical assets and facilities, such as locks, fences, and security cameras, rather than digital or logical systems.

Administrative controls are policies, procedures, and guidelines that govern security strategy and personnel behavior, rather than technical measures to protect systems.

Deterrent controls are designed to discourage potential security violations, often by providing visible warnings or imposing penalties. They are not technical controls like firewalls or ACLs.

6.

Espionage is an activity primarily aimed at compromising which of the following security principles?

- **Confidentiality**
- Integrity
- Authenticity
- Availability

Correct answer: Confidentiality

Espionage involves the unauthorized access and collection of sensitive information. The primary goal of espionage is to breach confidentiality, making secret or private information available to unauthorized parties.

Availability refers to ensuring that information and resources are accessible when needed. Espionage is not directly aimed at disrupting availability.

Authenticity involves verifying that information is genuine and from a trusted source. Espionage does not typically target the authenticity of information.

Integrity ensures that information is accurate and unaltered. While integrity could be impacted by espionage if data is manipulated, the primary goal of espionage is usually to breach confidentiality, not integrity.

7.

Binary and threshold-based are terms relating to which of the following?

- **Integrity**
- Confidentiality
- Transparency
- Privacy

Correct answer: Integrity

Integrity measures how complete and correct data or a system is. A system's integrity can be measured in a binary (yes/no) fashion or based on whether the integrity level meets a particular threshold.

8.

Which of the following actions is specifically prohibited under the Computer Fraud and Abuse Act (CFAA)?

Accessing a computer without authorization to obtain information

Sending unsolicited commercial emails

Using encryption to protect sensitive data

Sharing software source code publicly

Correct answer: Accessing a computer without authorization to obtain information

The CFAA prohibits unauthorized access to computers to obtain information, reflecting its primary focus on protecting the confidentiality of data.

Sending unsolicited commercial emails is typically addressed by other laws, such as the CAN-SPAM Act, rather than the CFAA.

Using encryption to protect sensitive data is a security best practice and not prohibited by the CFAA.

Unless it involves proprietary or unauthorized code obtained through illegal means, sharing code is not specifically prohibited by the CFAA.

9.

Which of the following deals with the usability of a data format?

- **Availability**
- Confidentiality
- Integrity
- Authenticity

Correct answer: Availability

Availability refers to data that is available when needed in a usable format. Confidentiality restricts unauthorized access to data. Integrity ensures that data is complete and correct. Authenticity verifies that data has only been created and modified by authorized users.

10.

Which of the following is MOST likely to protect an organization against a Business Email Compromise (BEC) attack where an employee is tricked into sending money to a fake supplier?

Separation of duties

Least privilege

Need to know

Defense in depth

Correct answer: Separation of duties

Separation of duties breaks critical processes, such as paying vendors, into multiple stages controlled by different parties. This decreases the probability that a BEC attack would succeed because multiple people would need to be tricked by the email.

Least privilege and need to know would not apply if the employee legitimately had the ability to process vendor payments. Defense in depth refers to the use of multi-layered security controls, and its effectiveness against BEC attacks depends on the controls used.

11.

Which of the following is MOST likely to protect against phishing attacks?

Security awareness training

Email filtering solutions

Multi-factor authentication

Regular software updates

Correct answer: Security awareness training

Security awareness training educates users on how to recognize and respond to phishing attempts. It is critical in preventing these types of attacks since phishing often exploits human behavior. Training is the best line of defense for protecting against phishing attacks.

While email filtering solutions can reduce the number of phishing emails that reach users, they are not foolproof and some phishing attempts may still get through.

Multi-factor authentication (MFA) adds an extra layer of security, but does not prevent phishing attacks; it only helps mitigate the impact if credentials are compromised.

Regular software updates are important for maintaining overall security and patching vulnerabilities, but they do not specifically address the risk of phishing attacks.

12.

Which of the following is used to implement and enforce need to know?

- **Least privilege**
- Separation of duties
- Defense in depth
- Security via obscurity

Correct answer: Least privilege

The principle of least privilege states that an entity should only be granted the access and permissions needed to do their job. This implements and enforces the concept of need to know.

13.

When making a decision as an SSCP, it is MOST important that the decision is which of the following?

Ethical

Technically correct

Cost effective

Compliant with legal and regulatory requirements

Correct answer: Ethical

While decisions made by an SSCP should be technically correct, cost effective, and compliant with applicable laws and regulations, it is most important that they are ethically correct.

14.

Which of the following is NOT one of the phases of the information lifecycle as defined in ISO 27002?

Retention

Storage

Transmission

Deletion and destruction

Correct answer: Retention

Retention is not explicitly listed as a separate phase in the information lifecycle according to ISO 27002. The information lifecycle typically includes phases such as creation/acquisition, classification, storage, use, sharing, transmission, and deletion/destruction.

Deletion and destruction involves securely disposing of information when it is no longer needed.

Transmission involves the transfer of information from one location to another, whether within or outside the organization.

Storage involves securely storing information in a manner that protects its confidentiality, integrity, and availability.

15.

Which of the following organizations publishes widely used guidelines for temperature control for data centers?

ASHRAE

Uptime Institute

IEEE

IEC

Correct answer: ASHRAE

ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers) is the organization that publishes widely used guidelines for temperature control in data centers. Their standards, such as ASHRAE TC 9.9, provide recommendations for the environmental conditions, including temperature and humidity, that should be maintained in data centers to ensure optimal performance and reliability of equipment.

IEEE (Institute of Electrical and Electronics Engineers) develops standards related to electrical and electronic systems, but it does not specifically focus on temperature control for data centers.

The Uptime Institute is known for its Tier Classification System, which rates the reliability and availability of data centers; it does not specifically publish guidelines on temperature control.

IEC (International Electrotechnical Commission) publishes international standards for electrical and electronic technologies; it is not focused on temperature control guidelines for data centers.

16.

Where does an individual have a "reasonable expectation of privacy"?

At home

In a public park

On the sidewalk

At the office

Correct answer: At home

An individual generally has a "reasonable expectation of privacy" in their home. This is one of the most protected areas in terms of privacy rights, where people can expect to be free from unwarranted surveillance.

While there may be some expectation of privacy at work, it is often limited. Employers typically have the right to monitor workspaces, emails, and computer usage, so the expectation of privacy is reduced compared to one's home.

In public spaces like parks, individuals generally do not have a reasonable expectation of privacy. Activities and conversations conducted in these areas are typically open to observation by others.

Similar to a public park, being on a sidewalk is considered being in a public space where there is no reasonable expectation of privacy. People walking on sidewalks are in full view of others, including law enforcement and surveillance cameras.

17.

Which of the following is NOT one of the canons in the (ISC)2 code of ethics?

Obey all applicable laws and regulations.

Advance and protect the profession.

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

Provide diligent and competent service to principals.

Correct answer: Obey all applicable laws and regulations.

The four canons in the (ISC)2 code of ethics are:

1. *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
2. *Act honorably, honestly, justly, responsibly, and legally.*
3. *Provide diligent and competent service to principals.*
4. *Advance and protect the profession.*

Obey all applicable laws and regulations is not one of the core canons of the (ISC)2 code of ethics.

18.

Dual control and two-person integrity are examples of which of the following?

- **Separation of duties**
- Least privilege
- Need to know
- Defense in depth

Correct answer: Separation of duties

Dual control and two-person integrity require two parties to perform actions to complete a task. This is an example of separation of duties because no single person can independently complete the task.

19.

Which of the following BEST protects against fraudulent activity within an organization?

Job rotation

Need to know

Separation of duties

Least privilege

Correct answer: Job rotation

Job rotation protects against fraudulent activities because it creates opportunities for employees rotated into a role to detect these activities and limits the opportunity of an employee to abuse their role and permissions.

20.

Which of the following limits the systems and information that a user has access to?

Least privilege

Need to know

Separation of duties

Defense in depth

Correct answer: Least privilege

Need to know defines what a user needs to know or access, but least privilege actually enforces those limits by defining access and permissions.

Separation of duties divides responsibility for critical tasks between multiple users, and defense in depth deals with the importance of never relying on a single security control.

21.

Which of the following is highest on the knowledge pyramid?

- **Wisdom**
- Data
- Information
- Knowledge

Correct answer: Wisdom

The knowledge pyramid from bottom to top is data, information, knowledge, wisdom, and insight.

22.

Which of the following parts of CIANA is essential to achieving the others?

Authentication

Confidentiality

Integrity

Non-repudiation

Correct answer: Authentication

Confidentiality, integrity, and non-repudiation all make the assumption that the identities of users are known and verified. Therefore, authentication is essential for all of these.

23.

Which of the following is MOST closely related to regulatory oversight?

Transparency

Integrity

Availability

Safety

Correct answer: Transparency

Transparency deals with the ability of regulators, auditors, and other authorities to view and audit data.

24.

In the CIANA acronym, which component is primarily concerned with preventing unauthorized access to sensitive information?

Confidentiality

Integrity

Availability

Non-repudiation

Correct answer: Confidentiality

Confidentiality is specifically focused on preventing unauthorized access to sensitive information. It ensures that data is only accessible to those who have the necessary permissions, protecting it from being exposed to unauthorized individuals.

The CIANA acronym stands for:

- ***C**onfidentiality: Limiting who has access to data*
- ***I**ntegrity: Protecting the completeness and correctness of data*
- ***A**vailability: Ensuring that data is available in a timely manner and usable format*
- ***N**on-Repudiation: Preventing someone from denying that they took an action*
- ***A**uthentication: Proving that data was created or modified only by approved parties*

25.

Which of the following is a protocol used for configuration control?

SCAP

CMP

CCP

SCP

Correct answer: SCAP

The Security Content Automation Protocol (SCAP) shares data between security tools, including configuration information. This makes it easier to standardize threat detection across an organization's security infrastructure.

26.

Which of the following refers to information about a person that is not publicly known and is protected due to its sensitive nature?

NPI

PII

PNI

CPI

Correct answer: NPI

NPI (Non-Published Information) refers to sensitive information about a person that is not publicly known and is protected due to its confidentiality. This term is often used in financial and legal contexts to describe data that must be safeguarded from unauthorized disclosure.

PII (Personally Identifiable Information) refers to any information that can uniquely identify an individual; it might include both public and private details. It is broader than NPI and may include publicly available information.

PNI (Personally Non-Identifiable Information) refers to information that is private but not necessarily identifiable to a specific person; it is not as specific or commonly used as NPI.

CPI (Confidential Personal Information) is not a standard term and is less commonly used compared to NPI or PII, making it less relevant in this context.

27.

Which of the following in the CIANA acronym refers to preventing a user from denying their actions?

N

I

A

C

Correct answer: N

The CIANA acronym stands for:

- ***C**onfidentiality: Limiting who has access to data*
- ***I**ntegrity: Protecting the completeness and correctness of data*
- ***A**vailability: Ensuring that data is available in a timely manner and usable format*
- ***Non-Repudiation: Preventing someone from denying that they took an action***
- ***A**uthentication: Proving that data was created or modified only by approved parties*

28.

Which of the following BEST protects an organization against single points of failure?

Job rotation

Separation of duties

Least privilege

Need to know

Correct answer: Job rotation

Need to know, least privilege, and separation of duties can create single points of failure if only one party is authorized to perform a task or fulfill a role. Job rotation helps to prevent single points of failure because employees know how to perform other roles and can step in as needed.

29.

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

Deterrent

Detective

Corrective

Compensating

Correct answer: Deterrent

Deterrent security controls attempt to dissuade an attacker from carrying out an attack, making them proactive.

30.

Which of the following organizations publishes standards for describing data center requirements and capabilities?

- **Uptime Institute**
- ASHRAE
- IEEE
- IEC

Correct answer: Uptime Institute

The Uptime Institute has a four-tier standard that describes the capabilities and requirements of data centers. These tiers range from Tier 1, which is capable of supporting an office environment, to Tier 4, which is a highly redundant and fault-tolerant data center.

ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers) publishes standards related to HVAC systems, including guidelines for data center cooling, but it does not focus on the overall requirements and capabilities of data centers.

IEEE (Institute of Electrical and Electronics Engineers) develops standards for a wide range of technologies, including networking and power systems, but it does not specifically publish standards for describing data center requirements and capabilities.

IEC (International Electrotechnical Commission) publishes international standards for electrical, electronic, and related technologies, but it does not specifically focus on data center requirements in the way the Uptime Institute does.

31.

Registered mail, which requires a recipient to sign for a letter or package, is an example in the postal system of a service that provides what?

Nonrepudiation

Confidentiality

Privacy

Integrity

Correct answer: Nonrepudiation

Registered mail requires the recipient to sign for a letter or package, which makes it infeasible for them to deny or repudiate receiving it. This concept aligns with non-repudiation, which is the assurance that someone cannot deny the validity of their signature or receipt of a message or transaction.

Confidentiality ensures information is accessible only to those authorized to access it. Registered mail does not inherently protect the contents from being seen by unauthorized individuals.

Integrity ensures the content of a message or data remains unchanged and unaltered during transit. While registered mail tracks the delivery, it does not specifically guarantee the contents of the mail have not been tampered with.

Privacy refers to the protection of personal information from being disclosed. Registered mail does not inherently protect personal information beyond ensuring delivery to the intended recipient.

32.

"A-ha" moments create what in the DIKW pyramid?

- **Insights, wisdom**
- Information, data
- Knowledge, information
- Wisdom, knowledge

Correct answer: Insights, wisdom

"A-ha" moments create insights from wisdom.

Generating and testing hypotheses helps to move from information to knowledge. Performing processing to create models is the activity that moves from data to information. As ideas become more established, they move from knowledge to wisdom.

33.

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

Fence

Camera

Buried line

Motion sensor

Correct answer: Fence

A fence is a physical barrier that is designed to prevent unauthorized access to a property or restricted area. It is a classic example of a preventive physical security control because it aims to stop intruders from entering a secured space.

A camera is an example of a detective control, as it records activities and helps in monitoring for security breaches but does not prevent them on its own.

A buried line, typically used for detecting underground movement or intrusions, is also a detective control, as it alerts security personnel to potential breaches but does not physically prevent them.

A motion sensor is another detective control. It detects movement within an area and triggers an alert, but it does not physically prevent access.

34.

Which of the following is NOT one of the fundamental security control principles?

Defense in depth

Need to know

Separation of duties

Least privilege

Correct answer: Defense in depth

The three fundamental security control principles are need to know, separation of duties, and least privilege. Defense in depth, which refers to not relying on a single security control for a particular threat, is not one of the primary three.

35.

Which of the following is an example of a sanitization method for hard drives (as compared to a disposal method)?

Zeroization

Degaussing

Abrasion

Shredding

Correct answer: Zeroization

Zeroization involves overwriting the data stored on a drive with random data, making it suitable for reuse. Degaussing, abrasion, and shredding all render the drive unusable.

36.

Which of the following is NOT one of the three core management processes for IT systems?

Inventory management

Asset management

Change management

Configuration control

Correct answer: Inventory management

Asset management, change/configuration management, and configuration control are the three core management processes for IT systems. Inventory management is a fabricated term.

37.

Which of the following is NOT a type of information that confidentiality applies to?

Marketing materials

Intellectual property

Customer data

Internal financial reports

Correct answer: Marketing materials

Marketing materials are designed to be publicly disseminated. Intellectual property, customer data, and data protected by an NDA must be kept private.

Confidentiality is essential for protecting intellectual property to prevent unauthorized access, use, or disclosure, thus maintaining the owner's competitive advantage and legal rights.

Confidentiality is crucial for protecting customer data and ensuring that personal or sensitive information is not disclosed to unauthorized individuals or entities.

Internal financial reports often contain sensitive information about the organization's financial status and are typically kept confidential to prevent unauthorized access or misuse.

38.

Which of the following is a high-level document describing what a company is trying to accomplish?

- **Policy**
- Standard
- Baseline
- Guideline

Correct answer: Policy

Policies are high-level documents describing an organization's goals, such as complying with compliance requirements or putting the company's strategic vision into practice.

Standards define consistent ways of accomplishing something based on best practices and may originate from inside or outside the organization. Baselines tailor a standard to a specific scenario, such as laying out the minimum set of security controls for a system, while guidelines provide looser instructions for performing a task while encouraging and allowing flexibility. Procedures are detailed descriptions of how to perform a specific task.

39.

Which of the following is NOT part of the CIA triad?

Authentication

Confidentiality

Integrity

Availability

Correct answer: Authentication

While authentication is a critical concept in security, it is not part of the CIA triad. The CIA triad consists of three core principles: Confidentiality, Integrity, and Availability, which are fundamental to information security.

Confidentiality ensures that information is accessible only to those authorized to have access, protecting data from unauthorized access.

Integrity ensures that information is accurate and unaltered, protecting data from unauthorized modification.

Availability ensures that information and resources are available to authorized users when needed, protecting systems from being inaccessible.

40.

Which of the following is NOT one of the three main legal principles of privacy?

Protection of intellectual property and trade secrets

Illegal search and seizure

Self-incrimination

Government disclosure of information

Correct answer: Protection of intellectual property and trade secrets

Protection of intellectual property and trade secrets is important in legal contexts, particularly in business and intellectual property law, but it is not one of the three main legal principles of privacy. Privacy law primarily deals with the protection of personal information and individual rights rather than intellectual property or trade secrets.

The illegal search and seizure principle protects individuals from unwarranted intrusions by the government, as outlined in the Fourth Amendment to the U.S. Constitution.

The self-incrimination principle, protected by the Fifth Amendment, ensures that individuals cannot be forced to testify against themselves, preserving their right to privacy in legal proceedings.

The government disclosure of information principle involves the regulation of how government entities collect, store, and disclose personal information, often governed by laws such as the Privacy Act.

41.

An organization requires that applications be tested by a team that includes none of the original developers. This is an example of which of the following?

Separation of duties

Least privilege

Defense in depth

Security through obscurity

Correct answer: Separation of duties

The separation of duties principle involves dividing responsibilities among different individuals or teams to reduce the risk of fraud or error. By ensuring that applications are tested by a team that does not include the original developers, the organization ensures that no single person or group has control over all aspects of the application, thereby reducing the potential for undetected errors or malicious actions.

Least privilege involves granting users only the minimum level of access necessary to do their jobs. While important, it is not directly related to ensuring that developers and testers are separate.

Defense in depth refers to using multiple layers of security controls to protect an asset. While it contributes to overall security, it does not specifically address the separation between development and testing teams.

Security through obscurity is an approach that relies on keeping details about a system secret as a security measure. It is generally not recommended as a primary security strategy and is unrelated to the separation of responsibilities.

42.

You need to securely dispose of a solid state drive. Which of the following is an effective technique?

Shredding

Degaussing

Zeroization

Smashing

Correct answer: Shredding

Shredding is the most effective way of disposing of an SSD. Degaussing doesn't work on it, and data may be recoverable after zeroization or smashing it.

43.

Which of the following is NOT one of the three "dues"?

Due consideration

Due care

Due diligence

Due process

Correct answer: Due consideration

The three "dues" are due care, due diligence, and due process.

Due consideration is a fabricated term.

44.

Which of the following is typically part of an investigation or analysis but is NOT a key part of accountability?

Assigning responsibility for a particular event

Knowing what is supposed to happen

Verifying that certain events didn't happen

Determining why an event that didn't happen didn't happen

Correct answer: Assigning responsibility for a particular event

While assigning responsibility is crucial for accountability, the focus of this question is on tasks that are more aligned with investigation or analysis. Accountability typically involves tracking actions, verifying occurrences, and understanding expected outcomes, but assigning responsibility is a broader management function rather than a specific investigative task.

Accountability is about identifying what should happen, verifying that it did, and, if not, finding out why.

45.

The (ISC)2 Code of Ethics consists of a preamble and how many canons or principles?

Four

Three

Five

Eight

Correct answer: Four

The four canons or principles of the (ISC)2 code of ethics are:

1. *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
2. *Act honorably, honestly, justly, responsibly, and legally.*
3. *Provide diligent and competent service to principals.*
4. *Advance and protect the profession.*

46.

Which of the following is NOT a major phase in the lifecycle of an asset?

Configuration

Acquisition

Deployment

Retirement and disposal

Correct answer: Configuration

The major faces in an asset's lifecycle are:

- *Planning*
- *Assigning security needs*
- *Acquisition*
- *Deployment*
- *Management*
- *Retirement and disposal*

Configuration is not part of the asset lifecycle.

47.

Managing licensing restrictions is part of which of the following management processes?

Asset management

Change management

Configuration control

IP configuration

Correct answer: Asset management

Identifying and tracking licensing restrictions is part of the asset management process.

Change management and configuration control deal with management of baseline configurations of an asset. IP configuration is a fabricated term

48.

Which of the following implements changes to system baselines?

Configuration control

Change management

Asset management

Inventory configuration

Correct answer: Configuration control

Asset management involves identifying an organization's assets and tracking information about them, such as their costs, users, licenses, and location.

Configuration control implements the changes approved under change management processes.

Change management processes govern how baselines are changed on managed IT assets. Inventory configuration is a fabricated term.

49.

Which of the following intellectual property protections fails if the information in question is not kept private?

Trade secret

Patent

Copyright

Trademark

Correct answer: Trade secret

A trade secret relies on the information being kept confidential. If the information is disclosed or becomes public, the protection is lost, and the trade secret is no longer enforceable. Trade secrets are typically business practices, formulas, processes, or information that give a company a competitive edge and are not publicly known.

A copyright protects original works of authorship such as literary, musical, and artistic works. It does not depend on the information being private; once created, copyright protection automatically applies.

A patent protects inventions and allows the inventor exclusive rights to the invention for a period of time. Patents require public disclosure of the invention details as part of the application process.

A trademark protects symbols, names, and slogans used to identify goods or services. Trademarks are meant to be public and do not require the information to be kept private to maintain protection.

50.

Which of the following is MOST likely to originate from outside of the organization?

Standard

Policy

Procedure

Guideline

Correct answer: Standard

Policies are high-level documents describing an organization's goals, such as complying with compliance requirements or putting the company's strategic vision into practice.

Standards define consistent ways of accomplishing something based on best practices and may originate from inside or outside the organization, and procedures are detailed descriptions of how to perform a specific task. Baselines tailor a standard to a specific scenario, such as laying out the minimum set of security controls for a system. Guidelines provide looser instructions for performing a task while encouraging and allowing flexibility.

51.

Which of the following is NOT a common component of resource protection for removable media?

Access management

Marking

Transport

Sanitization and disposal

Correct answer: Access management

While access management is crucial for controlling who can access resources, it is not typically considered a specific component of resource protection for removable media.

Marking involves labeling removable media to identify its classification level, owner, or usage restrictions, ensuring it is handled appropriately.

Transport refers to the secure movement of removable media from one location to another, ensuring it is protected from loss, theft, or unauthorized access during transit.

Sanitization and disposal involves securely wiping or destroying removable media that is no longer needed to prevent unauthorized access to the data it once contained.

52.

Which of the following establishes a minimum level of security or performance that can be tailored to meet specific needs or requirements?

Baseline

Policy

Guideline

Standard

Correct answer: Baseline

A baseline establishes a minimum set of criteria, such as security controls or performance measures, that can be tailored or adjusted to meet the specific needs or requirements of an organization or project.

Policies are high-level documents describing an organization's goals, such as complying with compliance requirements or putting the company's strategic vision into practice.

Standards define consistent ways of accomplishing something based on best practices and may originate from inside or outside the organization.

Guidelines provide looser instructions for performing a task while encouraging and allowing flexibility.

53.

Read receipts in email are intended to provide which of the following?

Nonrepudiation

Confidentiality

Integrity

Authenticity

Correct answer: Nonrepudiation

Read receipts are intended to provide nonrepudiation by confirming the recipient has received and opened the email. This provides the sender with evidence the email was viewed, making it difficult for the recipient to deny having received or read it.

Read receipts do not provide confidentiality, as they do not protect the content of the email from unauthorized access.

Read receipts do not verify the authenticity of the sender or recipient; they only confirm that the email was opened.

Read receipts do not ensure the integrity of the email's content; they do not guarantee the content has not been altered during transmission.

54.

Which of the following is MOST commonly seen as in conflict with privacy?

Security

Confidentiality

Availability

Authentication

Correct answer: Security

Privacy and security are often seen as in conflict because privacy protections may help criminals and terrorists conceal their activities. Additionally, security mechanisms might involve collecting more data than necessary, leading to privacy issues if not managed correctly.

Authentication is the process of verifying identity, which does involve privacy concerns, but its purpose is typically aligned with protecting privacy by ensuring that only authorized individuals have access to certain data.

Confidentiality is a fundamental aspect of privacy, ensuring that information is accessible only to those authorized to have access.

Availability ensures that information and resources are accessible when needed. While availability must be balanced with security measures, it is not inherently in conflict with privacy.

55.

Which type of security control must be detectable to an attacker?

Deterrent

Detective

Corrective

Preventive

Correct answer: Deterrent

Deterrent controls are designed to dissuade an attacker from carrying out an attack, which means that the attacker needs to know that they exist. Preventive, detective, and corrective controls are often more effective when concealed from an attacker.

56.

Which of the following is MOST closely related to change/configuration management?

Baseline

Policy

Procedure

Standard

Correct answer: Baseline

Change/configuration management involves creating configuration baselines for IT assets. As the state or needs of the system changes, updates to the baseline will be made via the change management procedure.

57.

Which of the following describes EXACTLY how to perform a particular task?

Procedure

Guideline

Baseline

Policy

Correct answer: Procedure

A procedure provides a detailed, step-by-step set of instructions on how to perform a specific task. It is designed to ensure consistency and accuracy in the execution of tasks, leaving little to no ambiguity.

Policies are high-level documents describing an organization's goals, such as following compliance requirements or implementing the company's strategic vision.

Baselines tailor a standard to a specific scenario, such as laying out the minimum set of security controls for a system.

Guidelines provide looser instructions for performing a task while encouraging and allowing flexibility.

58.

Which of the following is NOT a category of risk mitigation controls?

Preventive

Physical

Logical

Administrative

Correct answer: Preventive

The three categories of risk mitigation controls are physical (locks, guards, etc.), technical/logical (access controls, etc.), and administrative (policies, procedures, etc.). Preventive is not one of them.

59.

Privacy is MOST closely related to which aspect of CIANA?

Confidentiality

Integrity

Authenticity

Availability

Correct answer: Confidentiality

Confidentiality and privacy are both related to controlling access to information.

Integrity verifies that information is complete and correct.

Availability refers to data or systems that are accessible and in a usable form.

Authenticity ensures that only vetted and trusted users or systems can create or modify data.

60.

Which of the following is intended to ensure that security controls are effective?

Audit

Baseline

Standard

Policy

Correct answer: Audit

An audit reviews the security and risk controls that an organization has in place to ensure that they are effective. Baselines, standards, and policies are examples of risk controls.

61.

Generating and testing hypotheses helps to move from which point to another in the DIKW pyramid?

Information, knowledge

Data, information

Knowledge, wisdom

Wisdom, insight

Correct answer: Information, knowledge

Generating and testing hypotheses helps to move from information to knowledge.

Performing processing to create models is the activity that moves from data to information. As ideas become more established, they move from knowledge to wisdom. "A-ha" moments create insights from wisdom.

62.

Which of the following is NOT a physical security control deployed at the entrance to a facility?

Secure processing areas

Flow control

Reception staff

Visitor log

Correct answer: Secure processing areas

Secure processing areas are designated zones within a facility where sensitive information or operations are handled. While they are important for physical security, they are not specifically deployed at the entrance to a facility. Instead, they are internal security measures.

Flow control is a physical security control used at the entrance to manage and direct the movement of people entering and exiting the facility, ensuring that only authorized individuals gain access.

Reception staff are positioned at the entrance to monitor and control access, greet visitors, and ensure that only authorized individuals enter the facility.

A visitor log is used at the entrance to record the details of visitors entering the facility. This helps track who has entered and serves as a security measure to ensure that only authorized individuals are allowed in.

63.

In the context of a chain of custody, which of the following is MOST important for verifying the identity of individuals handling evidence?

Authentication

Integrity

Confidentiality

Availability

Correct answer: Authentication

In a chain of custody, authentication is crucial for verifying the identities of individuals who handle or transfer evidence. Ensuring that only authorized personnel have access to the evidence helps maintain the integrity and reliability of the chain of custody.

While integrity is important for ensuring that evidence remains unaltered, the focus of this question is on verifying the identities of those handling the evidence, which is directly related to authentication.

Confidentiality involves protecting information from unauthorized access, but it is not the primary focus when verifying identities in the chain of custody.

Availability ensures that evidence is accessible when needed, but it does not pertain to verifying the identities of individuals handling the evidence.

64.

Information classification schemes are used to inform which of the following?

Need to know

Least privilege

Separation of duties

Defense in depth

Correct answer: Need to know

Information classification schemes detail the sensitivity of information. This is used to determine need to know.

65.

Which of the following involves identifying and tracking information about an organization's IT systems?

Asset management

Change management

Configuration control

Inventory configuration

Correct answer: Asset management

Asset management involves identifying an organization's assets and tracking information about them, such as their costs, users, licenses, and location.

Change management processes govern how baselines are changed on managed IT assets.

Configuration control implements the changes approved under change management processes. Inventory configuration is a fabricated term.

66.

In CIANA, which of the following refers to the completeness and correctness of data?

- **I**
- C
- A
- N

Correct answer: I

The CIANA acronym stands for:

- ***C**onfidentiality: Limiting who has access to data*
- ***Integrity: Protecting the completeness and correctness of data***
- ***A**vailability: Ensuring that data is available in a timely manner and usable format*
- ***N**on-Repudiation: Preventing someone from denying that they took an action*
- ***A**uthentication: Proving that data was created or modified only by approved parties*

67.

Which of the following is NOT an example of a physical security control typically used to protect the perimeter of an organization?

Flow control

Fences

Cameras

Patrols

Correct answer: Flow control

Fences, cameras, and patrols are all common access controls at the perimeter of a property. Flow control mechanisms, such as turnstiles, are usually deployed at the facility entry point.

68.

A session timeout is an example of what type of security control?

Technical

Physical

Administrative

Detective

Correct answer: Technical

Technical or logical controls are often implemented using software and control access to IT systems. Session timeouts are an example of a technical/logical control.

69.

Which of the following does NOT relate to managing baselines for IT assets?

Asset management

Change management

Change control

Configuration control

Correct answer: Asset management

Asset management deals with tracking IT assets and the relevant data about them.

Change management and change/configuration control relate to approving and implementing changes to these assets' baseline configurations.

70.

Which of the following provides the MOST flexibility?

Guideline

Procedure

Baseline

Standard

Correct answer: Guideline

Guidelines provide looser instructions for performing a task while encouraging and allowing flexibility.

Policies are high-level documents describing an organization's goals, such as complying with compliance requirements or putting the company's strategic vision into practice.

Standards define consistent ways of accomplishing something based on best practices and may originate from inside or outside the organization.

Procedures are detailed descriptions of how to perform a specific task.

Baselines tailor a standard to a specific scenario, such as laying out the minimum set of security controls for a system.

71.

Which of the following is MOST true of confidentiality and privacy?

Confidentiality is about sharing secrets, while privacy is about keeping secrets.

Confidentiality is about keeping secrets, while privacy is about sharing secrets.

Confidentiality and privacy are about keeping secrets.

Confidentiality and privacy are about sharing secrets.

Correct answer: Confidentiality is about sharing secrets, while privacy is about keeping secrets.

Confidentiality is about sharing secret information with only authorized parties. Privacy is about keeping sensitive information secret.

72.

Personally identifiable information (PII) falls at which level of the DIKW pyramid?

- **Data**
- Information
- Knowledge
- Wisdom

Correct answer: Data

PII is an example of individual pieces of information or "data".

Information includes conclusions or inferences that result from processing data, while knowledge is a general conclusion based on a lot of information. Wisdom is an insight extracted from applying knowledge.

73.

Which of the following is a European Union regulation related to privacy?

- **GDPR**
- HIPAA
- PCI DSS
- Privacy Act of 1974

Correct answer: GDPR

The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union (EU) that governs how organizations collect, process, and store personal data of individuals within the EU. It aims to protect individuals' privacy and give them more control over their personal data.

HIPAA (Health Insurance Portability and Accountability Act) is a U.S. regulation that protects the privacy and security of individuals' health information.

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. It is not specific to privacy and is not an EU regulation.

The Privacy Act of 1974 is a U.S. law governing the collection, maintenance, use, and dissemination of personally identifiable information by federal agencies.

74.

Performing processing to create models is the activity that moves from which point to another in the DIKW pyramid?

Data, information

Information, Knowledge

Knowledge, wisdom

Wisdom, insight

Correct answer: Data, information

Performing processing to create models is the activity that moves from data to information.

Generating and testing hypotheses helps to move from information to knowledge, and as ideas become more established, they move from knowledge to wisdom. "A-ha" moments create insights from wisdom.

75.

Which type of control may need to EXCEED regulatory requirements?

Compensatory

Detective

Preventive

Corrective

Correct answer: Compensatory

Compensatory controls are used when the required or "best" control will not work for a particular situation. When dealing with regulatory requirements, compensatory controls must meet or exceed the protection offered by the original or reference control.

76.

As ideas become more established, they move from which point to another in the DIKW pyramid?

Knowledge, wisdom

Data, information

Information, knowledge

Wisdom, insight

Correct answer: Knowledge, wisdom

In the DIKW (Data, Information, Knowledge, Wisdom) pyramid, ideas typically progress as they become more established from knowledge to wisdom. As ideas evolve, they move from the stage of knowledge—where they are understood and contextualized—to wisdom, where they are applied in a broader context with understanding and insight, leading to informed decision-making and action.

The information to knowledge transition involves understanding and contextualizing raw data to form knowledge but does not represent the final stage of established ideas.

Wisdom to insight does not follow the DIKW model as "insight" is not a formal stage in the DIKW pyramid.

Data to information is the initial transformation of raw data into something more meaningful (information) but not the final stages of idea establishment.

77.

Which of the following defines how baselines can be changed on an organization's IT assets?

Change management

Configuration control

Asset management

Inventory configuration

Correct answer: Change management

Change management processes govern how baselines are changed on managed IT assets.

Asset management involves identifying an organization's assets and tracking information about them, such as their costs, users, licenses, and location. Configuration control implements the changes approved under change management processes. Inventory configuration is a fabricated term.

78.

Baselines and standards are examples of which type of risk management control?

Administrative

Logical

Technical

Physical

Correct answer: Administrative

Baselines and standards are examples of administrative controls because they describe how a task should be accomplished.

79.

An IPS is NOT an example of which of the following types of security controls?

Corrective

Deterrent

Detective

Preventive

Correct answer: Corrective

An IPS (Intrusion Prevention System) is not a corrective control because it does not take action to limit the impact of an attack after it has occurred. Instead, it is designed to prevent, detect, and potentially deter attacks before they cause damage.

An IPS primarily functions as a preventive control by actively blocking or mitigating malicious activities to prevent security incidents from occurring.

An IPS has detective capabilities because it monitors and identifies potential security threats in network traffic.

An IPS can act as a deterrent by creating barriers to successful attacks, making it harder for attackers to succeed, thus discouraging them from attempting an intrusion.

80.

In a business context, who has the greatest reasonable expectation of privacy?

Business owner

Employee

Contractor

Visitor

Correct answer: Business owner

In a business context, the owner has the greatest reasonable expectation of privacy because they make the rules and control access to the site. Employees, contractors, and visitors have a very limited reasonable expectation of privacy.

Domain 2: Access Controls

81.

Which identity assurance level (IAL) for just-in-time identity might involve checking a social media profile?

IAL2

IAL1

IAL3

IAL0

Correct answer: IAL2

The three Identity Assurance Levels (IALs) in just-in-time identity are the following:

- ***IAL1:*** *No proofing is performed to verify the entity's identity.*
- ***IAL2:*** *The applicant's claim to an identity is validated using an online identity authentication service, which may include checking social media profiles.*
- ***IAL3:*** *The identity documents presented by the applicant are physically verified.*

IAL0 does not exist.

82.

Which IAM protocol divides the three A's into separate components of a single protocol?

TACACS+

RADIUS

LDAP

AD

Correct answer: TACACS+

The Remote Authentication Dial-In User Service (RADIUS) was developed by the NSF in the early 1990s to provide Authentication, Authorization, and Accounting (AAA) in a single service.

The Terminal Access Controller Access Control System Plus (TACACS+) was developed by the US Department of Defense and later taken over by Cisco. TACACS+ divides Authentication, Authorization, and Accounting (AAA) into separate components and uses TCP for network transport.

The Lightweight Directory Access Protocol (LDAP) is derived from the X.500 Directory Access Protocol standard to take advantage of the IP protocol suite. It organizes information about users into a directory tree structure where each entry has a unique Distinguished Name (DN) and associated attributes.

Active Directory is a Microsoft-proprietary protocol that must be run on Windows Server but can support other types of devices. The domain controller, which runs Active Directory Domain Services (AD DS) handles entity authentication and authorization.

83.

What is the name for a virtual extension that can link multiple organizations' virtual LANs?

Extranet

Internet

Intranet

Federated network

Correct answer: Extranet

An extranet is a virtual extension to a corporate LAN that can be used to link multiple federated organizations together.

84.

What is the name for the process of creating a set of credentials for an entity?

- **Provisioning**
- Credentialing
- Identifying
- Proofing

Correct answer: Provisioning

Provisioning is the process of creating credentials for an entity. Proofing is a stage in this process where the proof of identity provided by the entity is validated.

Credentialing and identifying are fabricated terms

85.

Biometrics is an example of which type of authentication factor?

Type III

Type I

Type II

Type IV

Correct answer: Type III

The three main types of authentication factors are:

- ***Type I:*** *Something you know (password, etc.)*
- ***Type II:*** *Something you have (smartcard, etc.)*
- ***Type III:*** *Something you are (biometrics)*

86.

Sign in with Facebook, Google, Apple, etc. are examples of which of the following?

Single sign-on

Password managers

Multi-factor authentication

Centralized identity management

Correct answer: Single sign-on

Sign in with Facebook, Google, Apple, etc. are examples of Single Sign-On (SSO) systems. The user authenticates to the service provider, who passes their identity on to other applications.

87.

Which security property of the Bell-LaPadula model prevents write down?

Star Security Property

Simple Security Property

Discretionary Security Property

Mandatory Security Property

Correct answer: Star Security Property

The security properties of the Bell-LaPadula model are:

- ***Simple Security Property (SS):*** *Prevents a subject from reading up*
- **** (star) Security Property:*** *Prevents a subject from writing down*
- ***Discretionary Security Property:*** *Requires the use of an access matrix to enforce discretionary access control when implementing Bell-LaPadula*

88.

Which of the following is NOT a common trust relationship?

Bilateral

One-way

Two-way

Transitive

Correct answer: Bilateral

The main types of trust relationships are as follows:

- ***One-way**: A trusts B, but B doesn't trust A.*
- ***Two-way**: A trusts B and B trusts A.*
- ***Transitive**: A trusts B and B trusts C, so A trusts C.*

89.

Which access control method is BEST suited to an environment containing highly sensitive information or data protected under data protection regulations?

MAC

DAC

RBAC

ABAC

Correct answer: MAC

Mandatory Access Control (MAC) centrally manages control over files, applications, directories, etc. and denies users the ability to manage access to their own assets. This makes it best suited to managing access to sensitive or restricted information.

Discretionary Access Control (DAC) is the access control model built into most operating systems and allows the owner of an asset to manage privileges associated with it.

Role-Based Access Control (RBAC) assigns access and permissions based upon an entity's role within the organization, making it easier to implement least privilege and separation of duties.

Attribute-Based Access Control (ABAC) assigns sets of attributes to each entity. Access control rules are implemented using Boolean logic that describes the combinations of attributes needed to access a resource or perform a particular action. This allows highly granular access control rules.

90.

Shoulder surfing is an example of what data classification problem?

Read up

Read down

Write up

Write down

Correct answer: Read up

Shoulder surfing is an example of the read up problem because it could allow an entity to read data at a higher classification level than they are authorized to access.

91.

What is the term for the process of disabling and removing an entity's access and permissions on corporate systems?

Deprovisioning

Access removal

Disentitlement

Outprocessing

Correct answer: Deprovisioning

Deprovisioning is the process of disabling and removing an entity's (such as an employee's) access and permissions on corporate systems. This process typically occurs when an individual leaves the organization or when their role changes, requiring the removal of access to certain resources to maintain security.

While access removal is part of the deprovisioning process, it is not the formal term used to describe the comprehensive process of revoking all access and permissions.

Outprocessing refers to the general process of managing an employee's departure from an organization, which may include deprovisioning, but it is not specifically about access and permissions.

Disentitlement is not a widely recognized or formal term in the context of access management.

92.

Which type of access control provides an organization with the greatest control over access to its data and resources?

MAC

DAC

RBAC

ABAC

Correct answer: MAC

Mandatory Access Control (MAC) centrally manages control over files, applications, directories, etc. and denies users the ability to manage access to their own assets.

Discretionary Access Control (DAC) is the access control model built into most operating systems and allows the owner of an asset to manage privileges associated with it.

Role-Based Access Control (RBAC) assigns access and permissions based upon an entity's role within the organization, making it easier to implement least privilege and separation of duties.

Attribute-Based Access Control (ABAC) assigns sets of attributes to each entity. Access control rules are implemented using Boolean logic that describes the combinations of attributes needed to access a resource or perform a particular action.

93.

You are configuring access control for a highly-matrixed organization where employees may wear multiple hats and perform a range of duties. Which access control method is likely the BEST fit?

ABAC

MAC

DAC

RBAC

Correct answer: ABAC

Attribute-Based Access Control (ABAC) assigns sets of attributes to each entity. Access control rules are implemented using Boolean logic that describes the combinations of attributes needed to access a resource or perform a particular action. This allows highly granular access control rules and is well suited to environments where employee roles are difficult to clearly define.

Mandatory Access Control (MAC) centrally manages control over files, applications, directories, etc. and denies users the ability to manage access to their own assets.

Discretionary Access Control (DAC) is the access control model built into most operating systems and allows the owner of an asset to manage privileges associated with it.

Role-Based Access Control (RBAC) assigns access and permissions based upon an entity's role within the organization, making it easier to implement least privilege and separation of duties.

94.

Which of the following access management systems is MOST likely to be used on Windows systems?

Active Directory

LDAP

Kerberos

RADIUS

Correct answer: Active Directory

Active Directory is a Microsoft-developed IAM system commonly used on Windows devices. Linux and Unix systems often use LDAP and Kerberos. RADIUS is another commonly used access management system in enterprise environments.

95.

Which of the following protocols was developed by the National Science Foundation (NSF) to provide AAA in a single service?

RADIUS

TACACS+

LDAP

AD

Correct answer: RADIUS

The Remote Authentication Dial-In User Service (RADIUS) was developed by the NSF in the early 1990s to provide Authentication, Authorization, and Accounting (AAA) in a single service.

The Terminal Access Controller Access Control System Plus (TACACS+) was developed by the US Department of Defense and later taken over by Cisco. TACACS+ divides Authentication, Authorization, and Accounting (AAA) into separate components and uses TCP for network transport.

The Lightweight Directory Access Protocol (LDAP) is derived from the X.500 Directory Access Protocol standard to take advantage of the IP protocol suite. It organizes information about users into a directory tree structure where each entry has a unique Distinguished Name (DN) and associated attributes.

Active Directory (AD) is a Microsoft-proprietary protocol that must be run on Windows Server but can support other types of devices. The domain controller, which runs Active Directory Domain Services (AD DS) handles entity authentication and authorization.

96.

In identity and access control, what is the thing that someone or something acts upon?

Object

Subject

Resource

Entity

Correct answer: Object

In identity and access control, subjects take actions on objects. For example, a user (actor) might read or edit a document (object).

97.

Which of the following is NOT a major activity of Identity and Access Management (IAM)?

Password management

Account access review

Auditing

Enforcement

Correct answer: Password management
Although password management is an important function within IAM, it is not considered one of its major activities. The primary activities of IAM typically include account access review, auditing, and enforcement.

Account access review focuses on ensuring that users have appropriate access levels.

Auditing involves reviewing and ensuring compliance with access policies and detecting any unauthorized access.

Enforcement ensures that access control policies are consistently applied across the organization.

98.

Which of the following uses authentication servers to allow a user to log in once and gain access to all associated applications and systems?

Single sign-on

Password manager

Consolidated authentication

Passwordless authentication

Correct answer: Single sign-on

Single sign-on (SSO) allows users to log into the authentication system, which then provides authentication information to any associated applications or systems the user tries to access. This eliminates the need to memorize and enter many unique passwords for various systems.

Password managers store copies of a user's passwords and may autofill them into web pages.

Passwordless authentication uses non-password factors, such as biometrics or tokens.

Consolidated authentication is a fabricated term.

99.

Which of the following standards is MOST closely associated with federated identity?

SAML

XML

HTML

JSON

Correct answer: SAML

The Security Assertion Markup Language (SAML) is a widely used standard for exchanging authentication and authorization data between parties, particularly in federated identity systems. It allows identity providers to pass authorization credentials to service providers, enabling single sign-on (SSO) across different domains.

HyperText Markup Language (HTML) is a markup language used to define webpages.

JavaScript Object Notation (JSON) and eXtensible Markup Language (XML) are general-purpose data transfer and markup languages.

100.

Behavioral analytics are an example of which type of authentication factor?

Something you do

Something you know

Something you have

Something you are

Correct answer: Something you do

Behavioral analytics measure a person's actions and any deviations from normal. This is an example of a "something you do" authentication factor.