Example Test Questions

4) An accounting employee changes roles with another accounting employee every 4 months. What is this an example of?

a. Separation of duties

b. Mandatory vacation

\*c. Job rotation

d. Onboarding

CORRECT ANSWER: c. Job rotation

DETAILED EXPLANATION OF CORRECT ANSWER: The scenario describes job rotation because it involves employees periodically switching roles within the same department. From the document, we know that job rotation policy "Rotates employees to identify security gaps or procedural issues." This regular 4-month rotation between accounting roles matches this definition perfectly. Job rotation is a security measure that helps detect potential fraud or procedural issues by ensuring multiple employees are familiar with each role.

WHY OTHER OPTIONS ARE INCORRECT:

a. Separation of duties is incorrect because:

* Separation of duties involves splitting critical tasks among different employees to prevent any single person from having complete control over sensitive processes
* This is a permanent division of responsibilities, not a temporary rotation
* The scenario describes employees switching entire roles, not dividing tasks between them

b. Mandatory vacation is incorrect because:

* Mandatory vacation involves requiring employees to take time off from work
* The scenario describes employees continuing to work but in different roles
* Mandatory vacation policy is specifically used to uncover hidden risks or fraud by having employees completely away from their duties

d. Onboarding is incorrect because:

* Onboarding refers to the process of integrating new employees into an organization
* It defines how new employees gain access to resources
* The scenario describes existing employees rotating positions, not new employees joining the organization
* Onboarding is a one-time process when an employee starts, not an ongoing rotation of duties

9) Gurvinder's corporate data center is located in an area that FEMA has identified as being part of a 100-year flood plain. He knows that there is a chance in any given year that his datacenter could be completely flooded and underwater, and he wants to ensure that his organization knows what to do if that happens. What type of plan should he write?

a. A Continuity of Operations Plan

b. A business continuity plan

c. A flood insurance plan

\*d. A disaster recovery plan

**CORRECT ANSWER: d. A disaster recovery plan**

DETAILED EXPLANATION OF CORRECT ANSWER: A disaster recovery plan (DRP) is the correct answer because according to the document, it provides "Steps to restore normal operations after a disaster." The scenario describes a potential natural disaster (flooding) that could completely disable the datacenter, requiring specific steps to restore operations. The DRP would outline the exact procedures needed to recover from such a catastrophic event, including how to restore systems, data, and normal business operations after the flood damage.

WHY OTHER OPTIONS ARE INCORRECT:

a. A Continuity of Operations Plan is incorrect because this term isn't specifically mentioned in the document. While it might sound similar to a business continuity plan, it's not one of the defined plan types discussed in the materials.

b. A business continuity plan (BCP) is incorrect because while it's related, it focuses on "procedures for staying operational during disruptions" rather than recovery after a disaster. A BCP would be more focused on how to keep the business running during the flood, not how to recover after the datacenter is underwater.

c. A flood insurance plan is incorrect because:

* This isn't mentioned in the document as a type of disaster planning
* Insurance is a financial protection mechanism, not a procedural plan for recovery
* While flood insurance would be important to have, it wouldn't provide the necessary steps for restoring operations after a flood
* This focuses on compensation rather than operational recovery

17) Caroline has been asked to find an international standard to guide her company’s choices in implementing information security management systems. Which of the following would be the best choice for her?

\*a. ISO 27002

b. ISO 27701

c. NIST 800-12

d. NIST 800-53

**CORRECT ANSWER: a. ISO 27002**

1. Let's analyze each option:
2. a. ISO 27002
   * This is a code of practice that provides detailed security controls
   * It's meant to be used alongside ISO 27001
   * It's more about specific controls rather than overall ISMS implementation

b. ISO 27701

* + This is a privacy extension to ISO 27001
  + Focuses specifically on privacy information management systems
  + Not the primary standard for ISMS implementation

c. NIST 800-12

* + This is a U.S. government standard
  + Not an international standard
  + More focused on computer security basics

d. NIST 800-53

* + This is a U.S. government standard
  + Not an international standard
  + Focuses on security controls for federal information systems

1. Key observation:
   * None of these options is actually the primary standard for ISMS implementation
   * The standard that would be best for Caroline is ISO 27001, which isn't listed
   * Among the given options, ISO 27002 would be the closest match
2. Conclusion: While not perfect, ISO 27002 (option a) would be the best choice among the given options because:
   * It's an international standard (unlike the NIST options)
   * It's directly related to ISMS implementation (unlike ISO 27701 which is privacy-focused)
   * It provides detailed guidance that can be used for implementation
   * It aligns with ISO 27001 (the main ISMS standard)

The answer is a. ISO 27002.

Note: While this is the best answer among the options provided, ideally Caroline should also look into ISO 27001, which is the primary international standard for ISMS implementation.

25) Eric’s organization has created a policy document that describes how users can and cannot use the organization’s network, systems, and services. What type of policy has he created?

a. Business continuity policy

\*b. An acceptable use policy

c. An incident response policy

d. This is a standard, not a policy

**The correct answer is b. An acceptable use policy.**

An acceptable use policy (AUP) is precisely what Eric has created - a document that outlines how users are permitted and not permitted to use an organization's IT resources, including networks, systems, and services. This type of policy is essential for establishing clear guidelines about appropriate use of company technology assets and helping protect the organization from security risks, legal issues, and resource misuse. AUPs typically include sections on prohibited activities, personal use guidelines, security requirements, and consequences for violations.

Let's examine why the other options are incorrect:

a. Business continuity policy is incorrect because this type of policy focuses on maintaining essential business functions during and after a disaster or disruption. It outlines procedures for disaster recovery, emergency response, and ensuring critical operations can continue. It does not primarily deal with day-to-day user behavior and acceptable use of systems.

c. An incident response policy is incorrect because this type of policy specifically outlines procedures and responsibilities for detecting, reporting, and responding to security incidents and breaches. While it may reference acceptable use violations, its primary focus is on handling security incidents after they occur, not defining acceptable use guidelines.

d. "This is a standard, not a policy" is incorrect because standards are detailed technical specifications or precise criteria that provide rules or requirements for implementing policy objectives. A document describing how users can and cannot use organizational resources is definitively a policy, as it provides high-level guidelines and rules rather than technical specifications.

26) Susan has discovered evidence of a compromise that occurred approximately five months ago. She wants to conduct an incident investigation but is concerned about whether the data will exist. What policy guides how long logs and other data are kept in most organizations?

a. The organization's data classification policy

b. The organization's backup policy

\*c. The organization's retention policy

d. The organization's legal hold policy

**The correct answer is c. The organization's retention policy.**

A retention policy specifically defines how long different types of data, including logs, records, documents, and other information, must be kept by the organization before they can be disposed of or deleted. This policy is crucial for incident investigations as it determines whether historical data will still be available when needed. Retention policies typically consider various factors including legal requirements, regulatory compliance, business needs, and storage costs to establish appropriate retention periods for different types of data.

Let's examine why the other options are incorrect:

a. Data classification policy is incorrect because this type of policy focuses on categorizing data based on its sensitivity level and defining how each category of data should be handled, protected, and accessed. While classification may influence retention requirements, it does not directly specify how long data should be kept.

b. Backup policy is incorrect because this type of policy defines how data should be backed up, including frequency, methods, and storage locations. While backups are related to data preservation, they don't determine how long data should be retained before deletion. A backup policy focuses on protecting against data loss, not establishing retention timeframes.

d. Legal hold policy is incorrect because this type of policy specifically deals with preserving potentially relevant information when litigation is reasonably anticipated or in progress. While it can override normal retention periods, it is a special circumstance that applies only to specific data relevant to legal proceedings, not the general retention of logs and other data throughout the organization.

34) What standard is used for credit card security?

a. GDPR

b. COPPA

\*c. PCI-DSS

d. CIS

**The correct answer is c. PCI-DSS.**

PCI-DSS (Payment Card Industry Data Security Standard) is specifically designed for credit card security and is the global standard that must be followed by all organizations that handle credit card data. Created by major credit card companies, it provides detailed requirements for securing card holder data, including encryption standards, network security measures, access controls, monitoring requirements, and security testing procedures. All merchants and service providers that store, process, or transmit credit card data must comply with PCI-DSS requirements to ensure the protection of cardholder information.

Let's examine why the other options are incorrect:

a. GDPR (General Data Protection Regulation) is incorrect because while it's a comprehensive data protection regulation, it specifically focuses on protecting the personal data and privacy rights of European Union citizens. While it may include provisions that affect credit card data handling for EU citizens, it is not specifically designed for credit card security.

b. COPPA (Children's Online Privacy Protection Act) is incorrect because this is a U.S. federal law that specifically focuses on protecting the privacy of children under 13 years old online. It regulates the collection and use of children's personal information by websites and online services but has nothing to do with credit card security standards.

d. CIS (Center for Internet Security) is incorrect because while it provides valuable security benchmarks and best practices for various technologies and systems, it is not specifically focused on credit card security. CIS creates and maintains security configuration guidelines for various technologies but does not set the standards for credit card security.

41) Which of the following principles stipulates that multiple changes to a computer system should not be made at the same time?

a. Due diligence

b. Acceptable use

\*c. Change management

d. Due care

**The correct answer is c. Change management.**

Change management principles specifically include the requirement that changes to systems should be made one at a time, rather than implementing multiple changes simultaneously. This approach is crucial because it allows organizations to identify the specific cause of any problems that might arise from a change. When multiple changes are made at once, it becomes difficult or impossible to determine which change caused an issue, making troubleshooting and rollback procedures more complex and time-consuming.

Let's examine why the other options are incorrect:

a. Due diligence is incorrect because this principle refers to the practice of thoroughly investigating and assessing a situation or system before making decisions or taking actions. While it's an important security principle, it doesn't specifically address the timing or implementation of system changes.

b. Acceptable use is incorrect because this refers to policies and guidelines that define how users are permitted to use an organization's systems and resources. While it may include rules about making changes to systems, it doesn't specifically address the principle of implementing changes one at a time.

d. Due care is incorrect because this principle refers to taking reasonable steps to protect assets and information. While implementing changes properly could be considered part of due care, the specific principle of making one change at a time falls under change management, not due care.

43) Which of the following rights is not included in the GDPR?

a. The right to access

b. The right to be forgotten

c. The right to data portability

\*d. The right to anonymity

**The correct answer is d. The right to anonymity.**

The right to anonymity is not explicitly included in the GDPR (General Data Protection Regulation). While the GDPR does address various aspects of privacy and data protection, including pseudonymization and data minimization, it does not specifically grant individuals a "right to anonymity." The GDPR focuses on giving individuals control over their personal data and how it's processed, but does not guarantee complete anonymity in data processing.

Let's examine why the other options are incorrect:

a. The right to access is incorrect because this is actually a fundamental right granted by the GDPR. Under Article 15, individuals have the right to obtain confirmation about whether their personal data is being processed and to access that personal data along with information about how it's being used.

b. The right to be forgotten (also known as the right to erasure) is incorrect because this is explicitly included in Article 17 of the GDPR. This right allows individuals to request the deletion of their personal data under certain circumstances, such as when the data is no longer necessary for its original purpose.

c. The right to data portability is incorrect because this is explicitly granted under Article 20 of the GDPR. This right allows individuals to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit this data to another controller without hindrance.

55) Mark is responsible for the execution of his organization’s security awareness program. Why might he deploy multiple training methods like workshops, online training, and simulations as part of the training?

a. To meet compliance requirements

\*b. To address learning preferences

c. To decrease costs for training

d. To meet KPIs

**The correct answer is b. To address learning preferences.**

Using multiple training methods addresses different learning preferences and styles among employees. People learn differently - some are visual learners who benefit from demonstrations and simulations, others learn better through hands-on workshops, while some prefer self-paced online training. By implementing various training methods, Mark ensures that all employees can learn effectively through methods that best suit their individual learning styles. This comprehensive approach increases the likelihood that security awareness training will be effective across the entire organization.

Let's examine why the other options are incorrect:

a. To meet compliance requirements is incorrect because while compliance requirements may mandate security awareness training, they typically don't specify the exact methods of delivery. The use of multiple training methods goes beyond basic compliance requirements and focuses on training effectiveness rather than just checking a compliance box.

c. To decrease costs for training is incorrect because implementing multiple training methods typically increases rather than decreases costs. Each training method requires its own resources, development time, and potentially different tools or platforms, making it more expensive than using a single training approach.

d. To meet KPIs (Key Performance Indicators) is incorrect because while KPIs might measure the effectiveness of training, they don't drive the decision to use multiple training methods. KPIs are metrics used to measure success, not a reason for choosing particular training delivery methods. The use of multiple training methods might help achieve better KPI results, but this would be a benefit rather than the primary reason for their implementation.

58) Mikayla is working remotely in a public space and has been trained to make sure that others cannot see her screen or keyboard. What term is used to describe this?

a. Insider threats

\*b. Situational awareness

c. Social engineering

d. Unintentional risky behavior

**The correct answer is b. Situational awareness.**

Situational awareness refers to being conscious and mindful of one's surroundings and potential security risks in any given environment. When Mikayla ensures that others cannot see her screen or keyboard (preventing visual hacking or shoulder surfing) while working in a public space, she is demonstrating situational awareness. This includes being alert to and aware of potential security threats in her immediate environment and taking appropriate precautions to protect sensitive information.

Let's examine why the other options are incorrect:

a. Insider threats is incorrect because this term refers to security risks posed by people within an organization who have authorized access to systems and information. While someone watching Mikayla's screen could gain insider information, the act of being aware of and preventing such observation is not related to insider threats.

c. Social engineering is incorrect because this refers to psychological manipulation techniques used to trick people into revealing sensitive information or performing actions that compromise security. While social engineering could occur in public spaces, being aware of visual privacy is not specifically related to social engineering tactics.

d. Unintentional risky behavior is incorrect because Mikayla is actually demonstrating the opposite - she is intentionally practicing safe behavior by being aware of her surroundings and taking steps to protect sensitive information. Unintentional risky behavior would involve carelessly exposing sensitive information without realizing the potential consequences.

72) What common terms are used to categorize anomalous behavior?

\*a. Risky, unexpected, and unintentional

b. Recurring, occasional, and unique

c. Unintentional, insider, and accidental

d. Active, passive, and integrated

**The correct answer is a. Risky, unexpected, and unintentional.**

These three categories are specifically used in security awareness training to help employees identify and categorize different types of anomalous behavior:

* Risky behaviors are actions that could potentially harm the organization, such as accessing sensitive data without proper authorization or sharing credentials
* Unexpected behaviors are unusual activities that deviate from normal patterns, such as login attempts from unusual locations or at unusual times
* Unintentional behaviors are accidental actions by legitimate users that could create security risks, such as accidentally sending sensitive information to the wrong recipient or deleting important files

Let's examine why the other options are incorrect:

b. Recurring, occasional, and unique is incorrect because these terms describe the frequency of events rather than the nature of anomalous behaviors. While tracking frequency is important for security monitoring, these aren't the primary categories used to help employees recognize and respond to suspicious activities.

c. Unintentional, insider, and accidental is incorrect because while it includes "unintentional," which is one correct category, "insider" describes the source of a threat rather than the type of behavior, and "accidental" is redundant with "unintentional."

d. Active, passive, and integrated is incorrect because these terms typically describe types of security controls or systems rather than categories of anomalous behavior. They don't help employees identify and categorize suspicious activities.