PassQueen
a.k.a dumpsqueen.com

GIAC Certified ISO-2700 Specialist Practice Test

GIAC G2700

Version Demo

Total Demo Questions: 40

Total Premium Questions: 400

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	114
Topic 2, Volume B	83
Topic 3, Volume C	75
Topic 4, Volume D	108
Total	400

QUESTION NO: 1

You work as an Information Security Manager for uCertify Inc. You need to make the documentation on change management. What are the advantages of change management?

Each correct answer represents a complete solution. Choose all that apply.

A. Improved productivity of users due to more stable and better IT services

B. Improved IT personnel productivity, since there is a reduced number of urgent changes and a back-out of erroneous changes

C. Reduced adverse impact of changes on the quality of IT services

D. Increased ability to absorb frequent changes without making an unstable IT environment

ANSWER: A B C D

Explanation:

Effective change management ensures that changes to IT services are assessed, authorized, planned, implemented, reviewed, and documented in a controlled manner. “Improved productivity of users due to more stable and better IT services” is an important benefit because predictable, reliable services reduce disruption to business work. “Improved IT personnel productivity, since there is a reduced number of urgent changes and a back-out of erroneous changes” is also a benefit: risk assessment, testing, scheduling, and approval help teams avoid unplanned remediation and restore work.

“Reduced adverse impact of changes on the quality of IT services” expresses a central objective of change management. A formal process identifies service risks and dependencies before implementation, enabling appropriate controls, rollback planning, and post-implementation review. “Increased ability to absorb frequent changes without making an unstable IT environment” follows from repeatable governance: an organization can deliver necessary updates while maintaining service stability. These outcomes align with ISO/IEC 27001’s requirement to plan and control changes to the information security management system and with IT service-management change enablement practices. See ISO/IEC 27001 information and AXELOS ITIL practice guides.

QUESTION NO: 2

You want to use PGP files for steganography. Which of the following tools will you use to accomplish the task?

A. Snow

B. Blindside

C. ImageHide

D. Stealth

ANSWER: D

Explanation:

Stealth is the appropriate tool because it is a steganography utility designed to conceal a payload while supporting the use of PGP-protected data. In this workflow, the sensitive content is first protected with PGP encryption and the resulting encrypted material can then be embedded in a carrier file. This provides two distinct protections: steganography reduces the visibility of the communication by concealing the payload’s presence, while PGP protects the payload’s confidentiality if it is discovered or extracted. PGP commonly uses public-key cryptography to protect session keys and symmetric encryption to protect the data itself; its authenticity features can also help establish that the protected content has not been altered. The GNU Privacy Handbook describes the encryption and key concepts used by OpenPGP-compatible PGP implementations at GNU Privacy Handbook. A historical overview of steganography tools, including Stealth, is available from Gary Kessler’s steganography resources. Thus, where the requirement specifically combines a PGP file or encrypted PGP payload with steganographic concealment, Stealth matches the intended capability.

QUESTION NO: 3

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You need to make a document on the usage of information assets. Which of the following controls of the ISO standard deals with the documentation and implementation of rules for the acceptable use of information assets?

A. Control A.7.2.1

B. Control A.7.1.2

C. Control A.7.1.3

D. Control A.7.2

ANSWER: C

Explanation:

Control A.7.1.3 is the correct answer for the ISO/IEC 27001:2005-era control structure reflected in this question. Its subject is acceptable use of assets: rules governing the acceptable use of information and assets associated with information-processing facilities should be identified, documented, and implemented. This directly supports asset management by ensuring that personnel and other authorized users understand the permitted handling and use of organizational information assets, including systems, devices, applications, and information itself.

The control designation is version-specific. In ISO/IEC 27001:2013, the equivalent acceptable-use requirement was reorganized under Annex A asset management as A.8.1.3. ISO/IEC 27001:2022 has a substantially revised control structure and numbering. Because the question supplies the older A.7.x sequence and asks specifically for the control covering documented and implemented acceptable-use rules, Control A.7.1.3 is the intended and technically accurate selection. ISO describes ISO/IEC 27001 as the standard for establishing, implementing, maintaining, and continually improving an information security management system; its supporting guidance is maintained in ISO/IEC 27002. See ISO/IEC 27001 and ISO/IEC 27002:2022.

QUESTION NO: 4

Which of the following are the various domains in the ISO/IEC 27002?

Each correct answer represents a complete solution. Choose all that apply.

A. Management policy

B. Security policy

C. Access control

D. Compliance

ANSWER: B C D

Explanation:

The domain-based structure implied by this question corresponds to earlier editions of ISO/IEC 27002, in which the control guidance was organized into named security domains. **Security policy** is a domain because an information-security policy establishes management direction and the rules that govern the information security management program. **Access control** is a domain because ISO/IEC 27002 includes controls for limiting access to information, systems, and services according to business and security requirements. **Compliance** is also a domain because organizations must identify and meet applicable legal, regulatory, contractual, and internal security obligations, including requirements concerning records, intellectual property, and review of compliance.

The wording **Access security** has been corrected to **Access control**, which is the recognized domain name. ISO/IEC 27002 has since been revised; the current edition organizes guidance using organizational, people, physical, and technological control themes rather than the older domain list. For a question using the term “domains,” the historical domain

structure is therefore the appropriate basis for selecting these answers. See ISO's overview of the current standard at ISO/IEC 27002:2022 and ISO's information-security standards information at ISO/IEC 27001 and the ISO 27000 family.

QUESTION NO: 5

You work as a Security Administrator for uCertify Inc. You have installed ten separate applications for your employees to work. All the applications require users to log in before working on them; however, this takes a lot of time. Therefore, you decide to use SSO to resolve this issue. Which of the following

are the other benefits of Single Sign-On (SSO)?

Each correct answer represents a complete solution. Choose all that apply.

A. Centralized reporting for compliance adherence

B. Reducing IT costs due to lower number of IT help desk calls about passwords

C. Reduces the user experience

D. Reduces phishing success, because users are not trained to enter password everywhere without thinking

ANSWER: A B D

Explanation:

Single Sign-On centralizes authentication through a trusted identity provider, allowing the organization to apply authentication policy, capture sign-in activity, and review access events in one place. This supports centralized reporting for compliance adherence because audit records and access information can be collected consistently rather than separately across every application. SSO also reduces password-related operational burden. When users maintain fewer separate credentials and authenticate through a common service, they are less likely to require password resets or other routine account-support assistance, reducing IT help-desk costs. Microsoft describes SSO as enabling users to sign in once and access multiple applications, improving both user productivity and administrative control: Microsoft Entra SSO overview.

SSO can also reduce phishing success when it is implemented with a well-designed identity provider and strong authentication controls. Users become accustomed to authenticating only at the organization's recognized sign-in service instead of entering passwords into every individual application. This reduces opportunities for credential capture by imitation application login pages, particularly when paired with phishing-resistant authentication methods. NIST explains the value of phishing-resistant authenticators in its digital identity guidance: NIST SP 800-63B.

QUESTION NO: 6

As per a password policy, which of the following rules should be followed by a user while creating a password?

Each correct answer represents a complete solution. Choose all that apply.

A. Inclusion of one or more numerical digits

B. Inclusion of words found in a dictionary or the user's personal information

C. Use of both upper- and lower-case letters (case sensitivity)

D. Inclusion of special characters

ANSWER: A C D

Explanation:

"Inclusion of one or more numerical digits," "Use of both upper- and lower-case letters (case sensitivity)," and "Inclusion of special characters" are standard password-composition requirements used in many organizational password policies. Requiring character types from distinct sets increases the potential search space for a password of a given length and helps ensure that users do not select passwords made solely from simple alphabetic text. A numerical digit adds a character from

the decimal set, mixed case distinguishes uppercase and lowercase characters, and special characters add symbols outside the alphanumeric sets. When these requirements are combined with an appropriate minimum password length, they establish the traditional complexity baseline commonly specified in access-control policy. Password requirements should also be implemented with secure storage, rate limiting, and controls against known compromised passwords. Modern guidance emphasizes that length and screening against compromised-password lists are particularly important, and organizations should define requirements that are usable as well as resistant to guessing attacks. See NIST's Digital Identity Guidelines, SP 800-63B and OWASP's Authentication Cheat Sheet.

QUESTION NO: 7

Which of the following are features of protocol and spectrum analyzers?

Each correct answer represents a complete solution. Choose all that apply.

A. A protocol analyzer can identify physical layer errors in a network switch.

B. A packet analyzer can be used to capture real-time packets and can monitor the network packets on the LAN and the Internet.

C. A protocol analyzer can be used to analyze network traffic to trace specific transactions.

D. A spectrum analyzer should have the sensitive measuring equipment capability for detecting waveform frequencies and can identify and locate the interfering transmitter.

ANSWER: B C D

Explanation:

"A packet analyzer can be used to capture real-time packets and can monitor the network packets on the LAN and the Internet" is correct because packet/protocol analyzers capture traffic observed at a network interface and decode packet headers and contents. This permits real-time observation of communications on a local network and, when traffic is available at an appropriate monitoring point, traffic associated with Internet communications. Wireshark documents live packet capture as a core capability: Wireshark User's Guide: Capturing Live Network Data.

"A protocol analyzer can be used to analyze network traffic to trace specific transactions" is correct because filtering, protocol dissection, stream following, timestamps, and packet-level inspection allow an analyst to reconstruct and investigate exchanges such as DNS lookups, web requests, authentication flows, and application transactions.

"A spectrum analyzer should have the sensitive measuring equipment capability for detecting waveform frequencies and can identify and locate the interfering transmitter" is correct because spectrum analysis measures RF energy across a frequency range. In wireless troubleshooting, this visibility helps identify interference sources and characterize their frequency use; location is supported through directional measurements, multiple observations, or integrated location capabilities. Cisco describes spectrum analysis for detecting and mitigating RF interference in wireless networks: Cisco CleanAir technology overview.

QUESTION NO: 8

Which of the following are process elements for remote diagnostics?

Each correct answer represents a complete solution. Choose all that apply.

A. After detected performance degradation, predict the failure moment by extrapolation.

B. Remotely monitor selected vital system parameters.

C. Compare with known or expected behavior data.

D. Perform analysis of data to detect trends.

ANSWER: A B C D

Explanation:

Remote diagnostics is a condition-monitoring and prognostics process that turns remotely collected operational data into information supporting maintenance decisions. “Remotely monitor selected vital system parameters” is the acquisition stage: relevant measurements, such as temperature, pressure, vibration, utilization, errors, or performance counters, must be collected from the asset. “Compare with known or expected behavior data” supports state detection and health assessment by establishing whether current measurements deviate from an expected baseline, model, or historical normal condition.

“Perform analysis of data to detect trends” is also essential because a single reading may not reveal gradual deterioration. Trend analysis identifies changing behavior over time and provides the evidence needed for prognostic assessment. Where degradation has been detected, “After detected performance degradation, predict the failure moment by extrapolation” represents the prognostic step: observed degradation trends are used to estimate remaining useful life or the likely time at which performance crosses an unacceptable threshold. Together, these activities form a coherent remote-diagnostics workflow from monitoring, through assessment and trend analysis, to prediction. ISO 13374 describes the information-processing framework used for condition monitoring and diagnostics, including data acquisition, state detection, health assessment, prognostic assessment, and advisory functions. See ISO 13374-1:2003 and NIST’s Prognostics and Health Management Framework.

QUESTION NO: 9

You are setting up file permissions on a Windows server. Different users have different access needs. What should be your guiding principal in assigning file permissions?

A. Make three groups (one with low access, 1 moderate, and 1 high) and fit everyone into one of these groups.

B. Give users the minimal access required for their job, as this is more secure.

C. Give everyone access, as this makes administration simpler.

D. Block access to files until a user specifically requests any.

ANSWER: B

Explanation:

Give users the minimal access required for their job, as this is more secure. This applies the principle of least privilege: each user, service account, and administrative role receives only the permissions needed to perform its authorized duties, and no broader access. On a Windows file server, this means assigning NTFS and share permissions through appropriately scoped groups and granting only the necessary rights, such as read access for users who only need to view files or modify access for users who must update them. Least privilege reduces the attack surface and limits the effect of compromised credentials, accidental deletion, unauthorized disclosure, and inappropriate changes. It also supports ISO/IEC 27001-style access-control objectives by ensuring access rights are provisioned according to business need and reviewed as job responsibilities change. Microsoft similarly recommends granting users only the access required to complete their work and using groups to manage permissions consistently. This approach should be paired with periodic access reviews and prompt removal or adjustment of permissions when a user changes roles or leaves the organization. See Microsoft’s guidance on security groups and NIST’s least-privilege access-control discussion.

QUESTION NO: 10

Sam works as a Project Manager for Blue Well Inc. He is working on a new project. He wants to access high level risks for the project. Which of the following steps should Sam take in order to accomplish the task?

A. Developing risk management plan to identify risks based on documents

B. Developing project charter and risk management plan to identify risks based on documents

C. Developing project charter to identify risks based on documents

D. Identifying and analyzing risk events using qualitative and quantitative techniques

ANSWER: C

Explanation:

Developing project charter to identify risks based on documents is correct because the project charter is created during project initiation and records the project's high-level information, including high-level risks. It gives the project manager and key stakeholders an early, documented view of uncertainty that may affect the project's objectives, assumptions, constraints, funding, schedule, scope, or expected benefits. The charter is developed from available business documents and agreements, such as the business case, benefits management plan, contracts, enterprise environmental factors, and organizational process assets. Reviewing these sources enables the project manager to identify risks before detailed planning begins.

High-level risks in the charter support informed authorization of the project and provide an initial basis for planning. After authorization, risk management is planned in greater detail and risks are identified, analyzed, prioritized, and addressed through the project's risk-management activities. Thus, to access the early, strategic risk information for a new project, Sam should use the project-charter development process and its supporting documents. PMI describes the charter as the document that formally authorizes a project and provides high-level project information: PMI: The Project Charter. PMI's standards and resources also address the role of risk management throughout the project life cycle: PMI Risk Management.

QUESTION NO: 11

An Active Attack is a type of steganography attack in which the attacker changes the carrier during the communication process. Which of the following techniques is used for smoothing the transition and controlling contrast on the hard edges, where there is significant color transition?

A. Sharpen

B. Rotate

C. Blur

D. Soften

ANSWER: C

Explanation:

Blur is the image-processing technique used to smooth transitions at hard edges and reduce abrupt changes in color or intensity. A blur operation applies a filter that combines each pixel's value with values from nearby pixels. This averaging reduces high-frequency detail, including sharp boundaries where neighboring regions have significantly different colors. The result is a more gradual visual transition and reduced local contrast around the edge.

In the context of an active steganography attack, altering a carrier image with blur can modify embedded data because steganographic payloads are often stored through subtle pixel-level changes. Smoothing affects those small differences, particularly when the hidden information is embedded in image detail or high-frequency components. This makes blur a relevant carrier-modification technique: it can visually soften the image while potentially degrading or disrupting concealed content. The underlying principle is standard spatial-domain filtering, in which a low-pass filter attenuates rapid image variations. For further background, see OpenCV's image-smoothing documentation and the Gaussian blur overview.

QUESTION NO: 12

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You need to create a document following the Business Model of information security to provide guidelines for information assets. Which of the following are the elements of the Business Model for information security?

Each correct answer represents a complete solution. Choose all that apply.

A. Process

B. Technology

C. People

D. Training

E. Organization Design and Strategy

ANSWER: A B C E

Explanation:

The Business Model for Information Security frames security as an organizational capability rather than solely a technical function. **Organization Design and Strategy** establishes governance, decision rights, accountability, business alignment, and the strategic direction for protecting information assets. It ensures that asset-management guidance supports enterprise objectives, risk appetite, and leadership oversight.

People covers the human roles that create, own, use, administer, and protect assets. Clear ownership and accountability are essential to assigning classifications, approving access, and accepting or treating asset-related risk. **Process** provides the repeatable operational practices for the asset life cycle, including inventory, classification, handling, retention, review, and disposal. **Technology** enables these practices through mechanisms such as asset-discovery tools, access controls, logging, data protection, and configuration management.

These elements operate together: strategy and organizational design direct security activities; people perform and govern them; processes make them consistent and auditable; and technology provides scalable implementation and evidence. This is consistent with the NIST Cybersecurity Framework's emphasis on governance, organizational roles, policy, and risk-management processes, as described in NIST CSF 2.0, and with ISO/IEC 27001's information-security management-system approach: ISO/IEC 27001.

QUESTION NO: 13

Which of the following can be protected by the RAID implementation?

A. Switch failure

B. Disk failure

C. Network failure

D. Host failure

ANSWER: B

Explanation:

Disk failure is the correct answer because RAID (Redundant Array of Independent Disks) combines multiple physical disks into a logical storage arrangement that can provide redundancy when an individual drive fails. Depending on the RAID level used, data is duplicated through mirroring or protected using parity information distributed across drives. For example, RAID 1 maintains a mirrored copy of data on another disk, while RAID 5 and RAID 6 use parity to permit reconstruction of data after a supported number of member disks fail. This availability benefit allows a system to continue operating, or permits data recovery and replacement of the failed drive, without immediate loss of the protected data volume.

The protection level is determined by the selected RAID configuration and the number of failed disks it is designed to tolerate. RAID should therefore be implemented with suitable monitoring, documented replacement procedures, and tested backups. RAID redundancy improves resilience against physical disk-device failures, but it is not itself a substitute for backups or a complete business-continuity design. The National Institute of Standards and Technology discusses storage-system redundancy and fault tolerance in its contingency-planning guidance, available at NIST SP 800-34 Rev. 1. Additional technical background on RAID levels and their redundancy characteristics is provided by the Storage Networking Industry Association.

QUESTION NO: 14

The guidelines that are defined in the ISO/IEC 27002:2005 standard deal with which of the following aspects of information security?

Each correct answer represents a complete solution. Choose all that apply.

A. Procedural

B. Situational

C. Logical

D. Physical

ANSWER: A C D

Explanation:

ISO/IEC 27002:2005 provided guidance for selecting, implementing, and managing information-security controls in support of an information security management system. Its control guidance covered procedural, logical, and physical aspects of information security. Procedural safeguards are reflected in management-direction, policy, asset-management, incident-management, continuity, and compliance practices. These establish repeatable processes and governance for protecting information. Logical safeguards are represented by technical and system-oriented controls, including access control, cryptography, secure operations, communications security, and secure development practices. They are used to enforce security requirements through systems, configurations, and technical mechanisms. Physical safeguards are specifically addressed through controls for secure areas, equipment security, entry controls, environmental protections, and protection of facilities and supporting utilities. Together, these categories recognize that effective security requires coordinated administrative processes, technical enforcement, and protection of the physical environment. ISO describes ISO/IEC 27002 as a source of best-practice guidance on information security controls, while the current edition has evolved since the 2005 publication. See the ISO catalogue entry for ISO/IEC 27002:2005 and ISO's overview of the ISO/IEC 27001 information-security standards family.

QUESTION NO: 15

Which of the following plans provides measures and capabilities for recovering a major application or general support system?

A. Disaster recovery plan

B. Crisis communication plan

C. Contingency plan

D. Business continuity plan

ANSWER: C

Explanation:

Contingency plan is correct because it documents the coordinated measures, procedures, resources, and recovery capabilities needed to restore an information system after a disruption. In this context, a major application or general support system requires an organized approach for resuming essential system functions, recovering data and services, activating alternate processing arrangements where necessary, and returning the system to an acceptable operational state. The plan is based on the system's business and security requirements and defines recovery roles, notification and activation procedures, recovery steps, testing, training, and ongoing maintenance.

This use of the term aligns with NIST guidance for information-system contingency planning. NIST describes contingency planning as the preparation of interim measures to recover information-system services following disruption and identifies the information-system contingency plan as the central document for implementing those measures. The plan therefore provides the practical recovery capability for the affected application or support system, rather than merely setting high-level organizational resilience objectives. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and the NIST definition of contingency plan.

QUESTION NO: 16

David works as the Network Administrator for Blue Well Inc. One of his tasks is to develop and maintain risk management plan. Which of the following are the objectives of risk management plan?

Each correct answer represents a complete solution. Choose all that apply.

A. Eliminating risks

B. Accepting risks cautiously that cannot be eliminated

C. Developing required risks

D. Transferring risks by insurance

ANSWER: A B D

Explanation:

A risk management plan establishes how an organization will identify, assess, treat, monitor, and communicate risks so that risk exposure remains within approved tolerance. Eliminating risks is a valid objective where a risk can be avoided, such as discontinuing an activity, removing a vulnerable process, or choosing a design that does not create the exposure. This is commonly described as risk avoidance.

Accepting risks cautiously that cannot be eliminated is also appropriate. After evaluating likelihood, impact, controls, cost, and residual risk, management may formally accept a risk that is within the organization's risk appetite. Acceptance should be a deliberate, documented decision with appropriate review and monitoring.

Transferring risks by insurance is a recognized treatment approach. Insurance can shift specified financial consequences of an event to an insurer, subject to policy terms and exclusions. Risk transfer does not remove the organization's operational responsibility for managing the underlying exposure, but it can reduce the financial impact. These treatments align with ISO guidance on selecting risk-treatment options and with NIST guidance describing avoidance, acceptance, mitigation, and transfer as risk-response approaches. See ISO 31000 risk management and NIST SP 800-39.

QUESTION NO: 17

Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography.

Victor performs the following techniques to accomplish the task:

1. Smoothening and decreasing contrast by averaging the pixels of the area where

significant color transitions occurs.

2. Reducing noise by adjusting color and averaging pixel value.

3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?

A. Chosen-Stego Attack

B. Active Attacks

C. Stegdetect Attack

D. Steg-Only Attack

ANSWER: B

Explanation:

Active Attacks is correct because the described actions deliberately modify the suspected stego image in an effort to disrupt, remove, or make its concealed payload unrecoverable. Smoothing and pixel averaging alter local pixel relationships, particularly around edges and color transitions where image-based hiding schemes may embed data. Noise reduction and color adjustment similarly modify sample values that can carry hidden bits. Sharpening, softening, rotation, and resampling are image-processing transformations that change the image data and can desynchronize or destroy embedded information, especially when the hiding method depends on precise pixel positions or least-significant-bit values.

In steganographic terminology, an active attack is characterized by manipulating the carrier object rather than merely observing it or attempting passive statistical detection. The objective can be to degrade the hidden message, test its robustness against transformations, or prevent reliable extraction while retaining a visually plausible image. This matches the scenario because Victor is applying a series of intentional signal-processing operations directly to the image. For background on steganography and the distinction between detecting and modifying hidden communications, see NIST's steganography glossary entry and ScienceDirect Topics: Steganalysis.

QUESTION NO: 18

Sam is one of the four network administrators in Blue Well Inc. They have been assigned together the task to implement PDCA on the project. Sam has to work on the Plan stage of the project. Which of the following tasks should be performed by Sam?

Each correct answer represents a complete solution. Choose all that apply.

A. Preparing a statement of applicability

B. Defining the scope of ISMS

C. Defining the information security policy

D. Managing operations and resources

ANSWER: A B C

Explanation:

In the PDCA planning stage for an information security management system, the organization establishes the foundations for a managed, risk-based security program. **Defining the scope of ISMS** is a planning activity because it identifies the organizational boundaries, locations, processes, technologies, and interested-party considerations to which the management system applies. **Defining the information security policy** is also central to planning: leadership establishes the direction, objectives, and commitment that guide subsequent ISMS implementation and operation.

Preparing a statement of applicability belongs in planning because it documents the controls determined to be necessary from the risk-treatment process, including justification for their inclusion or exclusion and implementation status. This creates a traceable connection between assessed information-security risks, selected treatments, and the applicable control set. Together, scope, policy, and the statement of applicability establish the intended ISMS boundaries, governance direction, and control-treatment baseline before the organization proceeds with implementation and operation. ISO/IEC 27001 describes requirements for establishing, implementing, maintaining, and continually improving an ISMS, while ISO's overview highlights its risk-management basis. See ISO/IEC 27001 information-security management systems and ISO's ISO/IEC 27001 overview.

QUESTION NO: 19

You work as a Network Security Administrator for uCertify Inc. You feel that someone has accessed your computer and used your e-mail account. To check whether there is any virus installed into your computer, you scan your computer but do not find any illegal software. Which of the following types of security attacks generally runs behind the scenes on your computer?

A. Zero-day

B. Rootkit

C. Hybrid

D. Replay

ANSWER: B

Explanation:

Rootkit is correct because a rootkit is specifically designed to maintain concealed, privileged access to a compromised system. Rather than behaving like an obvious standalone virus, it can operate at a low level of the operating system and hide its files, processes, services, network connections, registry entries, or other evidence from normal users and many conventional security tools. This ability to evade ordinary inspection fits the scenario in which suspicious account activity occurred but a routine scan did not identify illegal software.

Rootkits may be installed after an attacker obtains access through another vulnerability or stolen credentials. Their purpose is often persistence and stealth: the attacker can return to the device, monitor activity, collect credentials, or use the system while minimizing visible signs of compromise. Because a rootkit can interfere with what the operating system reports to security software, detection may require trusted offline scanning, endpoint-detection tooling, integrity checking, or rebuilding the affected system from known-good media. NIST describes rootkits as software that hides processes, files, or system data to conceal malicious activity. See the NIST rootkit glossary entry and CISA's guidance on rootkits and defensive actions.

QUESTION NO: 20

You work as an Information Security Manager for uCertify Inc. You are working on the documentation of ISMS. Which of the following steps are concerned with the development of ISMS?

Each correct answer represents a complete solution. Choose all that apply.

A. Risk management

B. Selection of appropriate controls

C. HR security planning

D. Statement of Applicability

ANSWER: A B D

Explanation:

ISMS development is driven by a structured, risk-based process. **Risk management** is central because the organization must establish how it will identify, analyze, evaluate, and treat information-security risks within the defined ISMS scope. The results provide the evidence for deciding which security measures are necessary and proportionate to the organization's risk appetite.

Selection of appropriate controls follows risk treatment planning. Controls are selected to address identified risks and to meet applicable information-security requirements. ISO/IEC 27001 does not require an organization to adopt every control verbatim; rather, it requires the organization to determine necessary controls based on its risk-treatment decisions and to compare them with the control set in Annex A.

The **Statement of Applicability** is a required documented output of this process. It records the controls determined to be necessary, justifies inclusions, identifies whether Annex A controls are included or excluded, and provides justification for exclusions. This document links the risk assessment and treatment process to the controls that will operate in the ISMS, making it an essential part of ISMS documentation and implementation. See ISO's overview of ISO/IEC 27001 and the ISO/IEC 27002 controls guidance at ISO/IEC 27002.

QUESTION NO: 21

You work as an Information Security Manager for uCertify Inc. The company has made a contract with a third party software company to make a software program for personal use. You have been assigned the task to share the organization's personal requirements regarding the tool to the third party. Which of the following documents should be first signed by the third party?

A. Non disclosure agreement (NDA)

B. Acknowledgement papers

C. Copyright papers

D. Legal disclaimer

ANSWER: A

Explanation:

Non disclosure agreement (NDA) should be signed before the organization provides its requirements to the third-party developer. Requirements for a bespoke software tool can reveal confidential business processes, internal system details, security controls, architecture decisions, personal or proprietary data-handling needs, and planned capabilities. An NDA establishes the receiving party's legal duty to protect that information, limit its use to the agreed purpose, restrict further disclosure, and handle the information appropriately after the engagement ends.

Signing the NDA first creates a defined confidentiality boundary before sensitive details leave the organization's control. This is particularly important during early supplier discussions, when information may be exchanged before the full development agreement, statement of work, or technical specifications are finalized. The agreement should clearly identify protected information, permitted recipients and uses, safeguarding expectations, reporting obligations for unauthorized disclosure, and return or destruction requirements. NIST supply-chain guidance emphasizes establishing security requirements and protections in agreements with external service providers, while NIST's controlled-unclassified-information guidance recognizes nondisclosure agreements as a mechanism for ensuring authorized recipients protect sensitive information. See NIST SP 800-161 Rev. 1 and NIST SP 800-171 Rev. 3.

QUESTION NO: 22

Which of the following is a legal system that gives great precedential weight to common law, on the principle that it is unfair to treat similar facts differently on different occasions?

A. Religious law

B. Common law

C. Civil law

D. Customary law

ANSWER: B

Explanation:

Common law is correct because it is a legal tradition in which judicial decisions are a primary source of law. Courts apply the doctrine of *stare decisis*, meaning that they generally follow binding decisions made by higher courts in earlier cases. This promotes consistency: where materially similar facts arise, similar legal rules and outcomes should ordinarily be applied. The precedential value of earlier judgments is therefore central to common-law systems, rather than merely informative. In an ISO/IEC 27001 context, understanding the applicable legal system helps an organization identify the external legal and regulatory requirements that must be considered within its information security management system. For example, case law may clarify how statutory duties, contractual obligations, privacy requirements, or negligence standards are interpreted and enforced in a relevant jurisdiction. The principle described in the question specifically reflects the common-law approach of deriving and applying legal rules through prior judicial rulings. See the Encyclopaedia Britannica overview of common law and the Cornell Legal Information Institute definition of stare decisis.

QUESTION NO: 23

Which of the following phases of the PDCA model is the monitoring and controlling phase of the Information Security Management System (ISMS)?

A. Check

B. Plan

C. Do

D. Act

ANSWER: A

Explanation:

Check is the monitoring and controlling phase in the Plan-Do-Check-Act cycle as applied to an Information Security Management System. During this phase, the organization evaluates whether information-security processes, controls, and objectives are operating as intended. It involves monitoring and measuring relevant ISMS performance indicators, assessing control effectiveness, conducting internal audits, reviewing compliance obligations, and reporting results to relevant management and stakeholders. The evidence gathered allows the organization to identify deviations, nonconformities, emerging risks, and opportunities for improvement based on actual operational results rather than assumptions made during planning.

This monitoring activity is central to maintaining an effective ISMS because security controls must be continually evaluated as business processes, threats, technologies, and legal requirements change. ISO/IEC 27001 frames the management-system lifecycle around performance evaluation, including monitoring, measurement, analysis, evaluation, internal audit, and management review. These activities correspond to the control-oriented intent represented by the Check phase of PDCA. The resulting findings provide the factual basis for subsequent corrective action and continual improvement. See the ISO/IEC 27001 standard overview and the ISO Online Browsing Platform's PDCA-related management-system requirements.

QUESTION NO: 24

You work as a Security Administrator for uCertify Inc. You are working on the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity. Which of the following should you include in your plan?

Each correct answer represents a complete solution. Choose all that apply.

A. Resumption of hardware

B. Resumption of data

C. Resumption of sales

D. Resumption of applications

ANSWER: A B D

Explanation:

A disaster recovery plan for IT infrastructure must define how the organization will restore the technical capabilities needed to support prioritized business services after a disruption. **Resumption of hardware** is essential because recovery depends on available, configured, and secure infrastructure such as servers, network equipment, storage, end-user devices, or equivalent cloud resources. The plan should identify recovery locations, replacement arrangements, configuration baselines, dependencies, and responsible personnel.

Resumption of data is also a core recovery activity. A DRP needs documented backup, restoration, validation, protection, and recovery-point procedures so that required information is available with acceptable integrity and within the organization's recovery objectives.

Resumption of applications completes the IT recovery sequence by restoring application software, configurations, interfaces, credentials, and supporting services after the underlying infrastructure and required data are available. Recovery procedures should account for application dependencies and verification that services operate correctly before they are returned to users. NIST describes IT contingency planning as restoring information-system operations following a disruption, including system recovery and reconstitution activities. See NIST SP 800-34 Rev. 1 and the NIST contingency-planning guide overview.

QUESTION NO: 25

Which of the following is used for secure financial transactions over the Internet?

A. ATM

B. VPN

C. SSL

D. SET

ANSWER: D

Explanation:

SET is the correct answer because Secure Electronic Transaction was specifically developed to protect payment-card transactions conducted over open networks such as the Internet. Created through work involving Visa and Mastercard, SET uses cryptography and digital certificates to authenticate participating cardholders, merchants, and payment gateways. Its design separates sensitive card-payment information from the merchant's order information, helping ensure that payment credentials are disclosed only to the appropriate payment-processing party.

In an ISO 27001-oriented context, SET illustrates the application of cryptographic controls to preserve confidentiality, integrity, and authentication for a high-risk business process: electronic payment. Strong identification of transaction participants and protection of payment data address the security needs associated with financial transactions, including the prevention of unauthorized disclosure or modification while data traverses public networks. Although SET itself was not broadly adopted as the dominant modern e-commerce payment mechanism, the term directly identifies a protocol intended for secure electronic card payments and is therefore the best answer to this question. The Internet Engineering Task Force's historical SET documentation describes the protocol's payment-transaction purpose and certificate-based architecture; see RFC 3538. Additional background on the standard is available from Encyclopaedia Britannica's Secure Electronic Transaction entry.

QUESTION NO: 26

Which of the following specifies value of each asset?

A. Asset importance

B. Asset protection

C. Asset responsibility

D. Asset identification

ANSWER: A

Explanation:

Asset importance specifies the value assigned to each asset for information-security risk management. Organizations determine this value by considering the asset's contribution to business processes and the potential impact if its confidentiality, integrity, or availability were compromised. The resulting importance rating—often expressed through categories such as low, medium, and high, or through a numerical scale—allows the organization to prioritize protection efforts, risk treatment, recovery planning, and allocation of security resources. An asset with a high importance rating requires stronger and more timely controls because its loss, alteration, disclosure, or unavailability would create a greater business impact. This valuation is not necessarily a purchase price or accounting value; it represents the asset's business and security significance. Asset valuation is a foundational activity in risk assessment because risk is evaluated in relation to the consequences that a threat event could have for valuable assets. ISO/IEC 27005 addresses information-security risk management and the need to establish asset value and impact considerations as part of the risk process. NIST likewise describes impact assessment as determining the adverse consequences associated with loss or harm to organizational assets. See ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1.

QUESTION NO: 27

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Privacy law

B. Copyright law

C. Security law

D. Trademark law

ANSWER: A

Explanation:

Privacy law is correct because the scenario concerns an organization's collection and subsequent disclosure of an identifiable individual's financial and personal information. Privacy and data-protection rules govern how organizations may collect, use, retain, and share personal data. A credit card issuer generally needs a lawful basis and appropriate notice for processing customer information, and it must limit disclosure to purposes that are authorized, disclosed, or otherwise permitted by applicable law. Providing Mark's details to another company without an appropriate authorization, a clearly communicated purpose, or another valid legal basis is therefore a privacy issue.

Financial information is especially sensitive because unauthorized sharing can expose an individual to profiling, unwanted marketing, identity fraud, and other harms. In the United States, the Gramm-Leach-Bliley Act requires financial institutions to provide privacy notices and restricts disclosure of nonpublic personal information, subject to defined exceptions. Privacy principles also emphasize purpose limitation, transparency, and accountability when personal data is shared with third parties. See the U.S. Federal Trade Commission's Gramm-Leach-Bliley Act guidance and the Australian Privacy Principles for examples of these obligations.

QUESTION NO: 29

Service Level Agreement (SLA) provides one service for all customers of that service.

Which of the following are the contents included by SLAs?

Each correct answer represents a complete solution. Choose all that apply.

A. Scope

B. Mutual responsibilities

C. Vocations

D. Service description

ANSWER: A B D

Explanation:

An SLA should clearly establish the service commitment between a provider and its customers. **Service description** is a core element because it identifies the service being delivered, including its purpose, features, and relevant service-level targets. A meaningful description gives both parties a common understanding of what is being managed and measured.

Scope defines the boundaries of that commitment. It identifies the customers, systems, locations, processes, or service components covered by the agreement, allowing the agreed service to be applied consistently to the intended customer population. Scope also helps ensure that service measurements and expectations are tied to the specific service arrangement.

Mutual responsibilities document what the provider must do to deliver and support the service and what customers must do to enable delivery, such as supplying required information, using approved channels, or meeting agreed dependencies.

Clearly assigning these responsibilities makes the SLA an operational agreement rather than merely a statement of performance goals.

NIST guidance on service agreements emphasizes documenting the services, responsibilities, and expectations governing a provider-customer relationship. See NIST SP 800-35, Guide to Information Technology Security Services and ISO/IEC 20000-1 service management requirements.

QUESTION NO: 30

Which of the following is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

A. Supply chain management

B. Inventory management

C. Information security management

D. Change management

ANSWER: D

Explanation:

Change management is the structured discipline used to move people, teams, and organizations from their present way of working to a defined future state. It focuses on the human and organizational aspects of change: preparing affected stakeholders, communicating the purpose and impacts of the change, building the required knowledge and capability, supporting adoption, and reinforcing the changed practices so that the intended benefits are sustained. In an ISO/IEC 27001 context, change is especially relevant because an information security management system must remain suitable and effective as organizational conditions, risks, technologies, processes, and legal or contractual requirements evolve. Effective change management helps ensure that changes are planned, evaluated, communicated, implemented, and reviewed in a controlled manner rather than being introduced ad hoc. This reduces disruption and resistance while improving the likelihood that the desired new state is actually adopted in day-to-day operations. The Association of Change Management Professionals describes change management as the application of a structured process and tools to achieve a desired outcome, and ISO guidance identifies change management as a management-system consideration. See ACMP: What Is Change Management? and ISO 9001:2015—Quality management systems.

QUESTION NO: 31

Mark works as a System Administrator for uCertify Inc. He has recently installed freeware software from the Internet. He finds that the software displays some advertisements in a corner of the window. He notices that even when he is not downloading anything from the web, downloads are still increasing very frequently, despite the fact he is not using any web browser or Internet applications. After doing some research, Mark finds that the new software is downloading these files. Which of the following types of programs has Mark installed on his computer?

A. Macro

B. MBR

C. Tarpit

D. Adware

ANSWER: D

Explanation:

Adware is the correct classification because the installed freeware displays advertisements and independently downloads advertising-related content in the background. Adware is software designed to present ads to a user, commonly through banners, pop-ups, or embedded advertising areas in an application. It is frequently bundled with free software and may

contact advertising servers to retrieve new advertisements, images, scripts, configuration data, or tracking-related resources. Those recurring background transfers explain why download activity continues even though Mark is not actively using a browser or deliberately downloading files.

Although adware is not necessarily destructive in the same manner as ransomware or a disk-level boot infection, its unsolicited advertising and background network communication can affect bandwidth, privacy, and system performance. In an organizational environment, the appropriate response includes uninstalling the unwanted application, examining installed programs and browser extensions, running endpoint security scans, and reviewing outbound network connections for persistence or additional potentially unwanted software. The U.S. Federal Trade Commission describes adware as software that displays advertisements, often as part of free software, and CISA provides guidance for recognizing and managing potentially unwanted software behavior. See the FTC guidance on protecting computers from malware and CISA security guidance.

QUESTION NO: 32

Which of the following are the things included by sensitive system isolation?

Each correct answer represents a complete solution. Choose all that apply.

A. Construction of appropriately isolated environments where technically and operationally feasible

B. Inclusion of all documents technically stored in a virtual directory

C. Explicit identification and acceptance of risks when shared facilities and/or resources must be used

D. Explicit identification and documentation of sensitivity by each system/application controller (owner)

ANSWER: A C D

Explanation:

Sensitive system isolation is a risk-based protection measure intended to prevent systems with higher security needs from being exposed to threats or weaknesses associated with less sensitive systems, shared infrastructure, or shared operational processes. “Construction of appropriately isolated environments where technically and operationally feasible” is correct because isolation may be implemented through separate physical facilities, network segmentation, dedicated platforms, virtual separation with strong controls, or segregated administration, depending on the system’s risk and requirements.

“Explicit identification and acceptance of risks when shared facilities and/or resources must be used” is correct because complete separation is not always practical. In those cases, the residual risk arising from shared components must be assessed, documented, and formally accepted by an authorized risk owner, with appropriate compensating safeguards applied. “Explicit identification and documentation of sensitivity by each system/application controller (owner)” is also correct because the system owner must establish the system’s sensitivity and protection requirements before an appropriate isolation design and risk decision can be made.

These practices support ISO/IEC 27001’s risk-based information-security management approach and ISO/IEC 27002 guidance for separating and protecting systems, networks, and services according to security needs. See ISO/IEC 27001 and NCSC network security guidance.

QUESTION NO: 33 - (SIMULATION)

Fill in the blank with an appropriate phrase.

_____accord describes the minimum regulatory capital to be allocated by each bank based on its risk profile of assets.

ANSWER: See the explanation for the answer

Explanation:

Answer: Basel II

The **Basel II Accord** describes the minimum regulatory capital that banks must allocate based on the risk profile of their assets. It introduced risk-sensitive capital requirements through its three pillars: minimum capital requirements, supervisory review, and market discipline.

QUESTION NO: 35

Which of the following federal laws are related to hacking activities?

Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030

B. 18 U.S.C. 1028

C. 18 U.S.1029

D. 18 U.S.C. 2510

ANSWER: A C D

Explanation:

18 U.S.C. 1030, commonly called the Computer Fraud and Abuse Act (CFAA), is the principal U.S. federal statute addressing unauthorized access to protected computers. It covers conduct such as accessing a computer without authorization, exceeding authorized access in specified circumstances, obtaining protected information, causing damage, and trafficking in passwords. It is therefore directly central to computer-intrusion and hacking investigations.

18 U.S.1029 addresses fraud and related activity involving access devices, including unauthorized or counterfeit access devices and device-making equipment. Hacking activity can be used to obtain, create, traffic in, or misuse account credentials, card data, authentication tokens, and similar access devices; accordingly, this provision is frequently relevant to cyber-enabled financial and access-device offenses.

18 U.S.C. 2510 is part of the federal Wiretap Act framework. This section supplies definitions that govern the related prohibitions and procedures for interception of wire, oral, and electronic communications. Unauthorized interception or monitoring of electronic communications—a common concern in network compromise, packet capture, and malicious surveillance—can implicate this statutory framework. The statutory text is available through Cornell Law's 18 U.S.C. § 1030 page and Cornell Law's 18 U.S.C. § 2510 page.

QUESTION NO: 36

Which of the following is a technique for a threat, which creates changes to the project management plan?

A. Risk transference

B. Risk avoidance

C. Risk mitigation

D. Risk acceptance

ANSWER: B

Explanation:

Risk avoidance is correct because it is the threat-response strategy in which the project team acts to eliminate the threat entirely or protect the project from its impact. Avoidance commonly requires changing the planned approach—for example, removing a risky scope element, changing requirements, selecting a different technical solution, altering the delivery method, extending the schedule, or changing the project's objectives. Because these actions modify how the project will be executed, monitored, or controlled, they result in updates to the project management plan and potentially its subsidiary plans and baselines.

This response is appropriate when the threat is unacceptable or when its potential impact cannot be reduced to an acceptable level through other planned controls. The key characteristic is not merely reducing the probability or impact of the risk, but changing the project plan so that the source or exposure to the threat no longer applies. The Project Management Institute describes avoidance as acting to eliminate the threat or protect the project from its impact. This aligns directly with the question's reference to changes in the project management plan. See the Project Management Institute's risk-management guidance and ISO 31000 risk-management principles and guidelines.

QUESTION NO: 37

You have just taken control over network administration services for a sales and marketing firm. The sales staff (consisting of 10 people) rely heavily on both phone and internet connections for business. You notice that the sales staff has a single T1 line handling their phone and internet connections. Which of the following would be the best suggestion for improving this situation?

A. Move to fiber optic.

B. Move them to a T3 line.

C. Nothing, the system is fine as is.

D. Add an additional T1 line for redundancy.

ANSWER: D

Explanation:

Add an additional T1 line for redundancy. The existing design places two business-critical services—telephone connectivity and Internet access—on one circuit. A failure affecting that circuit, its provider connection, or the associated termination equipment can therefore interrupt both sales communications and online business activity at once. For a sales team that depends heavily on these services, reducing this single point of failure is the most immediate operational improvement.

A second circuit provides an alternate communications path that can be used when the primary connection is unavailable. To obtain meaningful resilience, the organization should configure failover for the applicable voice and data services, monitor both connections, and, where feasible, obtain the backup circuit through a separate provider and physically diverse path. Those measures reduce the chance that a common carrier, building-entry, or equipment failure disables both links. This recommendation follows contingency-planning principles that call for alternate capabilities and communications arrangements to sustain essential operations during disruptions. NIST describes alternate processing and telecommunications considerations in its Contingency Planning Guide for Federal Information Systems; CISA also identifies resilient communications as an important component of organizational continuity planning in its critical infrastructure resilience guidance.

QUESTION NO: 38

You work as a Security Administrator for uCertify Inc. You are concerned about the password security. Therefore, you have decided to apply a policy that will be helpful for others to create strong passwords. Which of the following are the important things that should be remembered to create a strong password?

Each correct answer represents a complete solution. Choose all that apply.

A. It should be of eight characters.

B. It should be a known word.

C. It should contain at least one number or punctuation character.

D. It should contain at least one capital letter.

ANSWER: A C D

Explanation:

An eight-character password provides a basic minimum length threshold in the conventional password-policy model used by this question. Password length increases the number of possible character combinations and therefore increases the effort required for an attacker to guess or exhaustively search for the password. Including at least one number or punctuation character adds character-type variety, increasing the possible password space beyond one made entirely from lowercase letters. Including at least one capital letter likewise adds another character type and supports a policy requiring mixed case. Together, these characteristics establish a baseline complexity standard: a password with sufficient length and a mixture of letter case, numbers, and punctuation is more resistant to simple guessing and common password-cracking approaches than a short, single-character-type password. Current guidance also emphasizes choosing passwords that are unique to each account and using substantially longer passwords or passphrases where possible. NIST notes that length is a primary factor in password strength and provides modern digital-identity guidance in NIST SP 800-63B. The UK National Cyber Security Centre similarly recommends long, unique passwords and password managers in its password-manager guidance.

QUESTION NO: 39

David works as the Network Administrator for Blue Well Inc. He has been asked to perform risk analysis. He decides to perform it by using CRAMM. The CEO of the company wants to know the stronger points of CRAMM that is going to be used by David. Which of the following points will David tell the CEO of the organization?

Each correct answer represents a complete solution. Choose all that apply.

A. It requires protecting a high risk system.

B. It is effective to meet the objectives of its sub-group.

C. It does not provide protection against any threat.

D. It is expensive to implement.

ANSWER: A B D

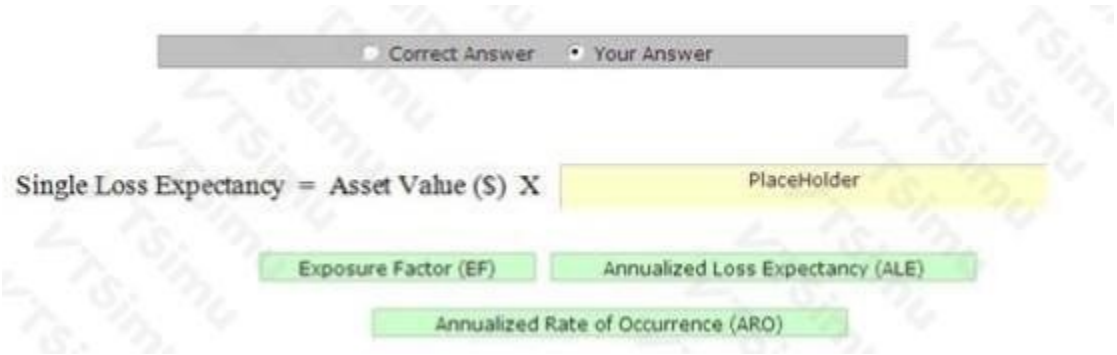
Explanation:

CRAMM (CCTA Risk Analysis and Management Method) is a structured risk-analysis approach intended to identify important assets, assess relevant threats and vulnerabilities, determine the level of risk, and select controls suited to that risk. Its control-selection approach emphasizes protecting systems whose assessed risk warrants protection, reflected by “It requires protecting a high risk system.” CRAMM also organizes controls into groups or categories with defined security objectives. Consequently, “It is effective to meet the objectives of its sub-group” describes the method’s use of control objectives to guide the selection of safeguards appropriate to the identified risks.

“It is expensive to implement” is also applicable as a practical characteristic of a full CRAMM engagement. A thorough assessment requires asset and dependency information, interviews, threat and vulnerability assessment, control selection, documentation, and personnel with suitable expertise. Organizations therefore commonly need a significant investment of time, trained resources, and often supporting tooling when applying CRAMM comprehensively, particularly across a large or high-value environment. This investment is consistent with using a disciplined, defensible method for systems where the consequences of unmanaged risk justify the effort. The underlying risk-management lifecycle aligns with ISO/IEC 27005 guidance on identifying, analyzing, evaluating, and treating information-security risks. See ISO/IEC 27005:2022 and the UK NCSC’s risk-management guidance collection.

QUESTION NO: 40

Drop the appropriate value to complete the formula.



A.

A. A

ANSWER: A

Explanation:

The appropriate completion is **A**. In this drag-and-drop fill-in-the-blank item, the available value is presented as the literal value “A,” and it is the value designated to occupy the blank in the formula shown in the accompanying image. The answer should therefore preserve the value exactly as supplied, including its uppercase form, rather than expanding it into a word or attempting to infer a different formula component from the incomplete OCR text. Accurate interpretation of visual evidence is important in ISO/IEC 27001-related assessment work because formulas, diagrams, process models, and control mappings must be read in their stated context. ISO’s overview of ISO/IEC 27001 describes the standard as a framework for establishing, implementing, maintaining, and continually improving an information security management system; precise handling of documented information supports that disciplined approach. See ISO/IEC 27001 information security management and ISO’s ISO/IEC 27001 overview.