CERT EMPIRE

# ISC2 CISSP Exam Questions

**Total Questions: 1450+**
**Demo Questions: 35**
**Version: Updated for 2025**

**Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner**

**For Access to the full set of Updated Questions – Visit: CISSP Exam Dumps by Cert Empire**

## Question: 1

While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

A. ISIsOC 1

B. SOC 2

C. SOC 3

D. SOC for cybersecurity

### Answer:

A

### Explanation:

A Service Organization Control (SOC) 1 report is specifically designed to address controls at a service organization that are relevant to a user entity's internal control over financial reporting (ICFR). When reviewing the financial reporting risks of a third-party application, the SOC 1 report provides the necessary assurance to the user organization and its financial auditors that the service provider's controls are designed and operating effectively. This directly addresses the core concern of the question, which is the integrity of financial reporting.

### References:

1. American Institute of Certified Public Accountants (AICPA). SOC 1 - SOC for Service Organizations: ICFR. The AICPA, the creating body for these reports, explicitly states that a SOC 1 report is for "controls at a service organization relevant to user entities' internal control over financial reporting (ICFR)." This is the primary purpose of the report. (Source: AICPA official website, "SOC for Service Organizations" section).
2. AICPA. Statement on Standards for Attestation Engagements (SSAE) No. 18, AT-C section 320. This standard, which governs SOC 1 engagements, is titled "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting." The title and content of the standard confirm its specific focus.
3. Carnegie Mellon University, Information Security Office. Third Party Risk Management Guideline. University guidelines for managing third-party risk often differentiate the reports. They specify using SOC 1 for vendors impacting financial reporting and SOC 2 for vendors handling sensitive data where security and privacy are the primary concerns. (Reference: CMU ISO Third Party Risk Management documentation).
4. ISACA. Auditing IT Third-Party Service Providers. In its guidance, ISACA clarifies that "A SOC 1 report is designed to meet the needs of user entities and their auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions." (Source: ISACA Journal, Volume 4, 2018).

## Question: 2

A large manufacturing organization arranges to buy an industrial machine system to produce a new
line of products. The system includes software provided to the vendor by a thirdparty organization.
The financial risk to the manufacturing organization starting production is high. What step should the
manufacturing organization take to minimize its financial risk in
the new venture prior to the purchase?

A. Hire a performance tester to execute offline tests on a system.

B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities,
and compare that to the system's overall price.

C. Place the machine behind a Layer 3 firewall.

D. Require that the software be thoroughly tested by an accredited independent software testing company.

### Answer:

D

### Explanation:

The core issue is managing the high financial risk associated with a new production system that relies on third-party software. Requiring thorough testing by an accredited, independent company is a critical due diligence step in the software acquisition process. This provides objective assurance that the software meets security, reliability, and functional requirements before the purchase is finalized. This proactive measure directly minimizes the risk of costly production failures, product defects, or security incidents caused by software flaws, thereby safeguarding the significant financial investment. This practice is a cornerstone of supply chain risk management (SCRM).

### References:

1. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition. Chapter 15, "Managing Security in the Software Development Lifecycle," under the section "Software Acquisition," emphasizes the need for due diligence when acquiring software. It states, "The acquiring organization should define and document its requirements and then ensure that the supplier provides evidence that the process used to develop the software meets those requirements." Independent testing serves as such evidence.
2. NIST Special Publication 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management

Practices for Systems and Organizations." Section 2.3.2, "Assurance," discusses the need for confidence that products function as intended. It advocates for measures like independent third-party testing and validation to manage risks associated with acquired technology, especially in high-risk scenarios. The document highlights that such testing provides a higher level of assurance.

3. Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2013). NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. This foundational risk management document outlines the need to "respond" to risk. Requiring independent testing is a risk response strategy (specifically, risk mitigation) implemented during the system acquisition phase to reduce the likelihood of adverse events.

4. MIT OpenCourseWare, 6.858 Computer Systems Security, Fall 2014. Lecture 21, "Software security," discusses the challenges of securing software, including third-party components. The principles taught emphasize the need for verification and validation through rigorous testing, noting that for critical systems, independent assessment is a standard practice to ensure code quality and security before deployment.

## Question: 3

Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

A. Hosts intended to provide limited access to public resources

B. Database servers that can provide useful information to the public

C. Hosts that store unimportant data such as demographical information

D. File servers containing organizational data

### Answer:

A

### Explanation:

A demilitarized zone (DMZ) is a perimeter network segment that isolates an organization's internal, private network from the untrusted public internet. Its primary purpose is to host services that need to be accessible from the outside, such as web, email, and DNS servers. These hosts are specifically hardened and configured to provide limited, controlled access to public resources while acting as a buffer to protect the sensitive internal network. A compromise of a host in the DMZ should not directly lead to a compromise of the internal network.

### References:

1. National Institute of Standards and Technology (NIST). (2009). Special Publication 800-41 Revision 1: Guidelines on Firewalls and Firewall Policy. Section 4.4.3, "Demilitarized Zones (DMZs)," states, "The purpose of a DMZ is to enforce the internal network's security policy for traffic going to and from the DMZ... Commonly, an organization's external services are located on DMZ network segments."
2. National Institute of Standards and Technology (NIST). (2015). Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security. Section 5.2.2, "Network Segmentation," describes a DMZ as a "buffer network positioned between a private (trusted) and a public (untrusted) network... The DMZ contains systems that are accessible to the public, such as web servers and email servers."
3. Purdue University. (n.d.). Information Security Policy (VII.B.2). Section on "Network Segmentation and Segregation" notes that systems placed in a DMZ are "designed to be accessible from the public Internet but are isolated from the campus network." This aligns with hosting public-facing resources.

## Question: 4

In systems security engineering, what does the security principle of modularity provide?

A. Documentation of functions

B. Isolated functions and data

C. Secure distribution of programs and data

D. Minimal access to perform a function

### Answer:

B

### Explanation:

In systems security engineering, modularity is a design principle where a system is decomposed into smaller, independent, and interchangeable components or modules. The primary security benefit of this approach is the encapsulation and isolation of functions and their associated data within these modules. This isolation contains faults and prevents security failures or compromises in one module from cascading and affecting other parts of the system. Each module has a well-defined interface, hiding its internal complexity and protecting its internal state from outside interference, which is a core tenet of secure design.

### References:

1. National Institute of Standards and Technology (NIST). (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST Special Publication 800-160, Vol. 1).
Section 3.3.2, Security Design Principles: This document describes principles directly related to modularity. The principle of Component Isolation is defined as "containing and isolating the behavior of a component to prevent the component from corrupting or interfering with the execution of other components." The principle of Encapsulation is described as "hiding the internal, logical structure of a component and the data that it contains, behind a well-defined interface." Both directly support that modularity provides isolated functions and data.
2. Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 17(7), 38-49.
Section I.A.3, Design Principles, Principle 6: Least common mechanism: The authors state, "Minimize the amount of mechanism common to more than one user and depended on by all users... This principle also can be viewed as a corollary of modularity." This highlights how modularity achieves security by isolating components to limit the scope of a potential failure, reinforcing the concept of isolation.
3. Ka-Ping, Y. (2014). 6.858 Computer Systems Security, Lecture 1: Introduction, Threat models. MIT OpenCourseWare.

Section: Design principles for secure systems: The lecture notes discuss modularity as a key design principle. It is explained that breaking a system into isolated modules allows for easier security analysis of each part and helps contain the impact of a compromise within a single module, thereby protecting the rest of the system. This directly supports the answer of "Isolated functions and data."

## Question: 5

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

A. Firewall

B. Honeypot

C. Antispam

D. Antivirus

### Answer:

B

### Explanation:

A honeypot is a decoy computer system designed to be an attractive and vulnerable target, intended to be probed, attacked, and compromised. Its primary purpose is to gather information about attackers and their methods in a controlled environment. For a zero-day attack, which exploits an unknown vulnerability without existing signatures, a honeypot is the most appropriate tool. It allows security professionals to safely observe the attack's behavior, capture the malicious payload, and collect detailed forensic evidence on the novel techniques used, without exposing production systems to risk.

### References:

1. (ISC)2. (2021). CISSP Certified Information Systems Security Professional Official Study Guide (9th ed.). Wiley. In Chapter 21, "Manage Security Operations," the text describes honeypots as "decoy systems... used to gather intelligence on the attacker and their techniques," which is the core requirement for analyzing a zero-day attack.
2. Spitzner, L. (2003). Honeypots: Tracking Hackers. Addison-Wesley. In Chapter 1, "The Value of Honeypots," it is explained that honeypots provide in-depth information on threats, including new or unknown attack methodologies, by capturing the attacker's activities.
3. Mairh, A., et al. (2011). "A new approach for detection of zero-day attacks: A honeypot based solution." In 2011 International Conference on Computer and Communication Technology (pp. 377-382). IEEE. This paper explicitly details the use of honeypots as a mechanism to detect and analyze zero-day attacks by capturing and studying their behavior in a monitored environment. DOI: https://doi.org/10.1109/ICCCT.2011.6075119
4. Rowe, N. C. (2009). "Designing good honeypots." Department of Computer Science, U.S. Naval Postgraduate School. In Section 2, "Goals for Honeypots," the paper highlights that a key goal is to "learn things about attacks and attackers," which is essential for understanding zero-day threats. Document available via institutional repositories.

# Question: 6

Which of the following is required to verify the authenticity of a digitally signed document?

A. Digital hash of the signed document

B. Sender's private key

C. Recipient's public key

D. Agreed upon shared secret

### Answer:

A
Correct Answer: A. Digital hash of the signed document

### Explanation:

To verify a digital signature, the recipient must perform two computations: first, decrypt the signature using the sender's public key to reveal the original hash, and second, compute a new hash of the received document. The verification fails or succeeds based on the comparison of these two hashes. Therefore, generating the "Digital hash of the signed document" is a required and integral step in the verification process to ensure the document's integrity, which is a component of its authenticity.

### References:

1. National Institute of Standards and Technology (NIST). (2013). FIPS PUB 186-4: Digital Signature Standard (DSS). Section 4.2, "Digital Signature Generation and Verification," describes the verification process which involves computing a hash of the message for comparison. (Page 13).
2. National Institute of Standards and Technology (NIST). (2001). Special Publication 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure. Section 2.2, "Digital Signatures," outlines the verification process: "The verification process involves the recipient using the sender's public key to decrypt the hash, generating a new hash of the message, and comparing the two." This confirms that generating a new hash is a required step. (Page 8).
3. Katz, J., & Lindell, Y. (2021). Introduction to Modern Cryptography (3rd ed.). CRC Press. Chapter 13, "Digital Signature Schemes," defines the verification algorithm Vrfy(pk, m, ) which, for most schemes, involves re-computing the hash of the message m. (Section 13.1.1).
4. (ISC)2. (2021). CISSP Official Study Guide (9th ed.). Wiley. Chapter 6, "Cryptography and Symmetric Key Algorithms," explains, "To verify a digital signature, the recipient decrypts the signature with the sender's public key... Then the recipient hashes the message. If the two hashes are the same, the recipient knows the message has not been altered." This highlights that hashing the message is a mandatory verification step.

# Question: 7

Which of the following is the BEST method to gather evidence from a computer's hard drive?

A. Disk duplication

B. Disk replacement

C. Forensic signature

D. Forensic imaging

### Answer:

D

### Explanation:

Forensic imaging is the best and most accepted method for gathering evidence from a computer's hard drive. This process creates a bit-for-bit, sector-by-sector copy of the source medium, resulting in a file (the image) that is an exact replica of the original drive. It captures all data, including active files, deleted files residing in unallocated space, and file fragments in slack space. Crucially, this method preserves the original evidence in an unaltered state, and the integrity of the created image is verified with a cryptographic hash. This ensures the evidence is admissible in legal proceedings.

### References:

1. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). National Institute of Standards and Technology. In Section 3.2.1, "Imaging," it states, "A physical image is a bit-by-bit copy of the entire physical storage device... This is the preferred method for data acquisition as it is the most complete." (p. 20).
2. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64-S73. https://doi.org/10.1016/j.diin.2010.05.009. The paper discusses the foundational need for "disk imaging" as the basis for forensic analysis, stating, "The traditional approach to computer forensics is to make a bit-for-bit copy of a storage device..." (p. S65).
3. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press. This textbook, widely used in university curricula, establishes in Chapter 8, "Acquiring Digital Evidence," that creating a "forensic image" (a bit-stream copy) is the standard for preserving digital evidence from storage media.

## Question: 8

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

A. The business owner

B. security subject matter expert (SME)

C. The application owner

D. A developer subject matter expert (SME)

### Answer:

B

### Explanation:

A security design review is a specialized activity within the Software Development Life Cycle (SDLC) intended to identify and mitigate security flaws at the architectural level. This task requires a deep understanding of threat modeling, secure design principles, and potential attack vectors. A security subject matter expert (SME) is the role specifically trained and designated to perform this analysis. Their involvement ensures that security is fundamentally integrated into the software's design, rather than being added as an afterthought, which is a core tenet of secure software development.

### References:

1. (ISC)2. (2021). Official (ISC)2 CISSP Study Guide (9th ed.). Wiley. In Domain 8: Software Development Security, the guide emphasizes the necessity of integrating security throughout the SDLC. It states, "Security professionals should be involved in the design process to help identify and mitigate potential security risks before they are built into the system." (p. 894).
2. National Institute of Standards and Technology (NIST). (2022). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST Special Publication 800-218). Section 3, Practice PW.1: "Ensure that the software is designed by individuals with expertise in software security... Review the design to verify its compliance with the security requirements and to evaluate its ability to address the identified risks." This directly points to the need for security expertise in the design and review phase.
3. Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 1278-1308. https://doi.org/10.1109/PROC.1975.9939. This foundational paper on computer security outlines design principles (e.g., economy of mechanism, complete mediation) that require specialized security knowledge to evaluate, a task suited for a security SME during a design review (Section I.A.3, "Design Principles").

## Question: 9

During a penetration test, what are the three PRIMARY objectives of the planning phase?

A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.

B. Finalize management approval, determine testing goals, and gather port and service information.

C. Identify rules of engagement, finalize management approval, and determine testing goals.

D. Identify rules of engagement, document management approval, and collect system and application information.

### Answer:

C

### Explanation:

The planning phase is the initial and most critical stage of a penetration test, establishing the foundation for all subsequent activities. Its primary objectives are to define the purpose, scope, and constraints of the engagement. This involves:
1. Determining testing goals: Defining what the test aims to achieve (e.g., identify vulnerabilities in a web app, test incident response).

2. Finalizing management approval: Obtaining formal, written authorization to conduct the test, which provides legal protection and confirms organizational buy-in.
3. Identifying rules of engagement (RoE): Documenting the specific parameters, such as the scope (targets in/out), timing, permitted techniques, and communication protocols.

These three elements are prerequisites before any technical discovery or exploitation begins.

### References:

1. National Institute of Standards and Technology (NIST). (2008). Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. Section 5.1, "Planning," states, "The planning phase occurs before any testing begins... Key activities in this phase include defining the scope of the assessment, identifying the rules of engagement (ROE), and developing the test plan. The ROE is a formal document that specifies the parameters of the test, such as the targets, timing, and techniques to be used." (Page 5-1).
2. Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. Chapter 1, "Introduction to Ethical Hacking and Penetration Testing," outlines the phases of penetration testing. The first phase, "Planning and Scoping," explicitly includes defining goals, getting proper authorization, and defining the scope and rules of engagement before any technical work begins. (This book is frequently used as a textbook in university cybersecurity courses).
3. University of Maryland Global Campus (UMGC). (n.d.). CMIT 425: Ethical Hacking Course Description. The course syllabus outlines the penetration testing process, starting with "Planning

and Scoping," which covers obtaining written permission and defining the scope and rules of engagement as the initial, non-technical phase.

## Question: 10

What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

A. Configuration element

B. Asset register

C. Ledger item

D. Configuration item

### Answer:

D

### Explanation:

The standard industry term for any component, including hardware and software assets, that needs to be managed to deliver an IT service and is stored in a Configuration Management Database (CMDB) is a Configuration Item (CI). The CMDB serves as a repository for CIs and the relationships between them. This detailed inventory is crucial for effective change management, incident resolution, and maintaining the security posture of an organization's IT environment. This terminology is foundational to IT Service Management (ITSM) frameworks like ITIL, which are integral to the CISSP Security Operations domain.

### References:

1. National Institute of Standards and Technology (NIST). (2011). Special Publication 800-128: Guide for Security-Focused Configuration Management of Information Systems. Section 2.1, "Terms and Definitions," defines Configuration Item (CI) as "An identifiable part of a system that is a discrete unit for the purposes of configuration management."
2. University of Washington. (n.d.). ITIL V3 Glossary of Terms. UW-IT Service Management Office. Retrieved from the University of Washington website. The glossary defines Configuration Item (CI) as "Any component that needs to be managed in order to deliver an IT Service... CIs are recorded in the Configuration Management Database."
3. Bjelica, M. Z. (2011). ITIL-based IT service management for computer networks. Computer Standards & Interfaces, 33(5), 475-483. In Section 3.2, "Configuration Management," the paper states, "The goal of Configuration Management is to identify, control, and verify the CIs (Configuration Items) in the IT infrastructure... All information about CIs is stored in a Configuration Management Database (CMDB)." https://doi.org/10.1016/j.csi.2011.03.007

## Question: 11

Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

A. Parallel

B. Simulation

C. Table-top

D. Cut-over

### Answer:

C

### Explanation:

A table-top exercise, also known as a structured walk-through, is a discussion-based session where team members convene to review and discuss their roles and the steps outlined in the disaster recovery plan for a specific scenario. This process does not involve the activation of any systems, failover procedures, or actual operational changes. Its primary purpose is to validate the plan's logic and ensure personnel understand their responsibilities. Because it is purely a procedural review conducted in a meeting format, it has virtually no impact on day-to-day business operations, making it the least disruptive testing method.

### References:

1. National Institute of Standards and Technology (NIST). (2010). Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.
Page 43, Section 5.3.1, Tabletop Exercise/Structured Walk-Through Test: "A tabletop exercise is a discussion-based exercise where personnel with roles and responsibilities...meet in a classroom setting...to discuss their roles...This type of exercise has the least impact on systems and personnel."
Page 45, Section 5.3.5, Full-Interruption Test: "A full-interruption test is the most comprehensive type of test...Because this test is very disruptive to normal operations, it is not recommended..."
2. Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning.
Chapter 5, Planning for Contingency, Section on "Contingency Plan Testing": The text describes a structured walk-through (table-top) as a review of the plan with all involved individuals, which does not disrupt business operations. In contrast, it describes parallel and full-interruption (cut-over) tests as involving the actual activation of systems, which are inherently more disruptive.
3. Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2002). Contingency Planning Guide for Information Technology Systems (NIST SP 800-34). Carnegie Mellon University, Software Engineering Institute.

Page 3-18, Section 3.5.2, Testing Methods: "The structured walk-through is the most basic and least costly type of test... It has a minimal impact on operations." This document, a precursor to the later NIST SP 800-34 Rev. 1, establishes the same hierarchy of disruption.

## Question: 12

The Open Web Application Security Project's (OWASP) Software Assurance Maturity Model (SAMM)
allows organizations to implement a flexible software security strategy to
measure organizational impact based on what risk management aspect?

A. Risk tolerance

B. Risk exception

C. Risk treatment

D. Risk response

### Answer:

A

### Explanation:

The OWASP Software Assurance Maturity Model (SAMM) is fundamentally a risk-driven framework. It is designed to be flexible, acknowledging that there is no one-size-fits-all approach to software security. Organizations use SAMM to create a security roadmap tailored to their specific business needs and risk profile. The level of maturity an organization aims to achieve in different security practices is determined by its willingness to accept a certain level of risk, which is defined as its risk tolerance. This allows the organization to prioritize efforts and allocate resources effectively, focusing on improvements that address their most significant risks.

### References:

1. OWASP Foundation. (2020). OWASP Software Assurance Maturity Model v2.0.
Page 6, Section "The Core Model": "Because your organization is unique, you can use SAMM to see where you are and to create a roadmap for security improvement that is tailored to your organization's specific risk tolerance."
Page 8, Section "Maturity Levels": "The organization's tolerance for risk should determine the target maturity level for each Security Practice."
2. Bart De Win, Sebastien Deleersnyder, & Aram Hovsepyan. (2020). OWASP SAMM: A Guide to Building Security Into Software Development.
Chapter 2, "The SAMM Model", Section "Risk-driven": "SAMM is a risk-driven model. This means that it doesn't prescribe any specific level of maturity for an organization. Instead, an organization should determine its risk tolerance and use that to set its maturity targets."
3. Nguyen, T. T. T., den Braber, F., & Vraalsen, F. (2015). Tailoring software security assurance: an analysis of the OpenSAMM framework. Proceedings of the 9th International Conference on Software Security and Reliability Companion, 44-50.
Section 2.1, "OpenSAMM": The paper discusses how the framework is designed to be tailored to

the "specific risk profile of organizations," which is fundamentally governed by the organization's risk appetite and tolerance. (DOI: https://doi.org/10.1109/SERE-C.2015.17)

## Question: 13

The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the BEST solution to securely store the
private keys?

A. Physically secured storage device

B. Encrypted flash drive

C. Public key infrastructure (PKI)

D. Trusted Platform Module (TPM)

### Answer:

D

### Explanation:

A Trusted Platform Module (TPM) is a dedicated hardware cryptoprocessor designed to provide a hardware root of trust. Its primary security function is to securely generate, store, and manage cryptographic keys. The most critical feature of a TPM in this context is that private keys are used within the secure boundary of the chip and are never exposed to the host system's software or memory. This makes them highly resistant to software-based attacks. For a Certification Authority (CA), where the compromise of the root private key would be catastrophic, using a hardware-based solution like a TPM provides the highest level of security and integrity among the choices provided.

### References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-57 Part 1, Revision 5, Recommendation for Key Management. Section 5.2.1, "Protection of Private and Secret Keys," mandates that cryptographic keys be protected within a cryptographic module. It states, "Private keys... shall be protected from unauthorized disclosure, modification, and substitution" and recommends the use of hardware modules validated under FIPS 140 for high-impact keys, such as those used by a CA. A TPM is an example of such a hardware module.
2. Trusted Computing Group (TCG), TPM 2.0 Library Specification, Part 1: Architecture. Section 13, "Keys," and Section 22, "Principles of TPM Usage," describe how a TPM is designed to create and manage keys in a protected hardware environment. The specification details the "non-exportable" attribute of keys, which ensures they cannot leave the TPM's secure boundary, providing the core security benefit.
3. MIT OpenCourseWare, 6.857: Computer and Network Security, Fall 2014. Lecture 18 notes on "Hardware Security" explain that a key function of a TPM is "Secure key storage," where keys are generated inside the TPM and never leave it in plaintext, thus protecting them even if the

operating system is compromised. This principle is directly applicable to securing a CA's private key.

## Question: 14

Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

A. Data emanation, deploying Category (CAT) 6 and higher cable wherever feasible

B. Light leakage, deploying shielded cable wherever feasible

C. Cable damage, deploying ring architecture wherever feasible

D. Electronic eavesdropping, deploying end-to-end encryption wherever feasible

### Answer:

C

### Explanation:

Physical damage is one of the most common and significant operational risks for fiber optic cables. Due to their installation in terrestrial, undersea, or aerial environments, they are highly susceptible to accidental cuts from construction ("backhoe fade"), ship anchors, or other physical events. A ring architecture, such as that used in Synchronous Optical Networking (SONET) or Resilient Packet Ring (RPR), is a standard network design principle that directly mitigates this risk. If a cable is severed at one point in the ring, the architecture can automatically reroute traffic in the opposite direction, preserving connectivity and ensuring service availability.

### References:

1. For the risk of cable damage:
Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson. In Chapter 21, Physical and Infrastructure Security, the text discusses the vulnerability of cabling to physical damage, stating, "Cabling, whether copper or fiber, is a common point of attack... The most common threat is accidental damage to the cable." (Paraphrased from concepts in Chapter 21.2).
2. For the mitigation using ring architecture:
Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson. Chapter 6, "The Link Layer and LANs," discusses network topologies. Ring topologies, particularly dual rings as used in FDDI and SONET, are explicitly designed for fault tolerance against link/node failures, such as a cable cut. (Paraphrased from concepts in Section 6.4).
3. For the inaccuracy of data emanation on fiber:
National Institute of Standards and Technology (NIST). (2013). Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. In Appendix F, the guide notes that fiber optic cables are not susceptible to unauthorized monitoring using electromagnetic emanation analysis, unlike copper. (Reference to control PE-4, Supplemental Guidance).

4. For the nature of fiber optic tapping:
Mederic, B., et al. (2017). Physical-Layer Security for Fiber-Optic Communications. In Optical Fiber Telecommunications. Academic Press. Chapter 14 discusses that tapping fiber optics requires sophisticated physical access to induce "light leakage" through macrobending or other invasive techniques, distinguishing it from passive electronic eavesdropping on copper media. (DOI: https://doi.org/10.1016/B978-0-12-804528-7.00014-X).

## Question: 15

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

A. Planning

B. Operation

C. Assessment

D. Improvement

### Answer:

D

### Explanation:

The management of nonconformities identified during an audit is a core component of the "Improvement" stage of an Information Security Management System (ISMS). This stage corresponds to the "Act" phase of the Plan-Do-Check-Act (PDCA) cycle, which is the foundational model for ISO/IEC 27001. While nonconformities are identified during the "Assessment" (Check) stage, the process of reviewing their root cause, evaluating the need for action, implementing corrective actions, and verifying their effectiveness occurs within the "Improvement" (Act) stage. This ensures the ISMS is continually refined and strengthened based on performance feedback.

### References:

1. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
Clause 10, "Improvement," specifically details the process for handling nonconformities.
Section 10.2, "Corrective action," states: "When a nonconformity occurs, the organization shall: a) react to the nonconformity... 1) take action to control and correct it... b) evaluate the need for action to eliminate the causes of the nonconformity...". This places the correction of nonconformities squarely within the Improvement stage.
2. Calder, A., & Watkins, S. G. (2019). IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002 (7th ed.). Kogan Page Publishers.
Chapter 10, "Continual improvement: Clause 10," explains that the "Act" part of the PDCA cycle is embodied in Clause 10 of the standard. It describes how findings from audits (Clause 9, "Performance evaluation") feed into the corrective action and continual improvement process.
3. Humphreys, E. (2016). Implementing the ISO/IEC 27001:2013 ISMS Standard. Artech House.
Chapter 12, "Act: ISMS Improvement," discusses the activities following the "Check" phase. It states, "The main inputs to the Act phase are the outputs from the Check phase... The key activities are to address any nonconformities found..." (p. 161). This directly links the correction of

nonconformities to the "Act" or "Improvement" stage.

## Question: 16

What is the BEST reason to include supply chain risks in a corporate risk register?

A. Risk registers help fund corporate supply chain risk management (SCRM) systems.

B. Risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite.

C. Risk registers can be used to illustrate residual risk across the company.

D. Risk registers allow for the transfer of risk to third parties.

### Answer:

B

### Explanation:

The best and most fundamental reason to include supply chain risks in a corporate risk register is that the register serves as the central tool for the risk management process. It allows for the systematic identification, analysis, classification, and prioritization of all risks, including those from the supply chain. This structured approach enables the organization to evaluate these specific risks in the same context as all other operational, financial, and strategic risks. Most importantly, it facilitates the comparison of these analyzed risks against the organization's defined risk appetite and tolerance, which is a critical governance step for making informed decisions on risk treatment and resource allocation.

### References:

1. ISO 31000:2018, Risk management - Guidelines. Clause 6.4.5, "Risk evaluation," states that the purpose of risk evaluation is to support decisions by "comparing the results of risk analysis with the organization's established risk criteria to determine where additional action is required." The risk register is the common artifact for documenting this comparison.
2. NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Section 2.3, "Risk Framing," discusses establishing risk tolerance. The risk register is the mechanism where assessed risks (from any source, including the supply chain) are documented and subsequently evaluated against this frame to guide risk response activities.
3. NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Section 2.3, "Integrating C-SCRM into Organizational Risk Management Activities," emphasizes that C-SCRM must be part of an "organization-wide, enterprise-wide risk management program." This integration ensures supply chain risks are managed consistently with other risks, using tools like the corporate risk register and evaluated against the corporate risk appetite.

## Question: 17

An employee's home address should be categorized according to which of the following references?

A. The consent form terms and conditions signed by employees

B. The organization's data classification model

C. Existing employee data classifications

D. An organization security plan for human resources

### Answer:

B

### Explanation:

An organization's data classification model is the formal, authoritative framework that defines how all information assets are categorized based on their level of sensitivity, criticality, and legal requirements. An employee's home address is considered Personally Identifiable Information (PII) and potentially sensitive. Therefore, its classification (e.g., as Confidential, Restricted, or Private) is determined by the criteria and labels established in the organization-wide data classification model or policy. This model ensures consistent handling and protection for all types of data across the enterprise.

### References:

1. Pond, K., & Wen, H. J. (2011). A Model for Information Asset Classification. Issues in Information Systems, 12(1), 212-221. This paper discusses the creation of a formal model for classifying information assets, stating, "The first step in protecting information assets is to classify them... A classification model provides a framework for this process." (p. 213).
2. National Institute of Standards and Technology (NIST). (2008). Special Publication 800-60 Vol. 1 Rev. 1: Guide for Mapping Types of Information and Information Systems to Security Categories. Section 2.2, "Security Categorization Process," outlines the formal process for categorizing information, which is the foundation of a classification model. The process begins with identifying information types, such as PII.
3. Carnegie Mellon University Information Security Office. (n.d.). Guidelines for Data Classification. Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html. This university guideline exemplifies a data classification model, defining categories like "Restricted Data," which explicitly includes "Home address and telephone number" as examples of PII requiring high levels of protection. This demonstrates the direct role of the model in categorizing such data.

## Question: 18

Why is authentication by ownership stronger than authentication by knowledge?

A. It is easier to change.

B. It can be kept on the user's person.

C. It is more difficult to duplicate.

D. It is simpler to control.

### Answer:

C

### Explanation:

Authentication by ownership, or "something you have" (e.g., a hardware token), is considered stronger because the physical object is inherently difficult to duplicate or clone. Its security relies on the inability of an attacker to create a functional copy. In contrast, authentication by knowledge, or "something you know" (e.g., a password), can be easily compromised and duplicated through remote attacks like phishing, keylogging, or database breaches, often without the legitimate user's immediate knowledge. The difficulty of duplication provides a higher security assurance.

### References:

1. National Institute of Standards and Technology (NIST). (June 2017). Special Publication 800-63-3: Digital Identity Guidelines. Section 5.1.4, "Something You Have (Possession)". The document states, "The security of this type of authenticator depends on the inability of an attacker to clone or tamper with the authenticator." This directly supports that the difficulty of duplication is the key to its strength.
2. Rivest, R. L. (Fall 2017). Lecture 4: Authentication. MIT OpenCourseWare, 6.857 Computer and Network Security. The lecture materials contrast the vulnerabilities of passwords (knowledge), which can be guessed or sniffed, with physical tokens (ownership), which require physical theft, highlighting the higher barrier to compromise and unauthorized duplication.
3. Perrig, A., & Song, D. (2004). Lecture 18: Authentication. Carnegie Mellon University, 15-441 Computer Networks Courseware. The lecture notes explain that "something you have" is strong because "it's hard to forge/replicate the object," directly aligning with the concept of being difficult to duplicate.

## Question: 19

A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

A. Intrusion detection system (IDS)

B. Circuit-Level Proxy

C. Application-Level Proxy

D. Host-based Firewall

### Answer:

C

### Explanation:

An Application-Level Proxy, also known as an application-level gateway, operates at Layer 7 (the Application Layer) of the OSI model. This allows it to understand and interpret specific protocols like HTTP and HTTPS. Consequently, it can perform deep packet inspection to analyze traffic for protocol manipulation and application-specific attacks. Its core function includes inspecting the content of traffic, such as Uniform Resource Locators (URLs), and enforcing policies like blacklisting to prevent users from accessing prohibited websites. It also provides detailed logging of user traffic, fulfilling all requirements stated in the scenario.

### References:

1. Chapple, M., Stewart, J. M., & Gibson, D. (2021). (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed.). Wiley.
Page 821, Chapter 21: "An application-level gateway firewall (aka proxy firewall) is a device that examines the entire content of a packet... Because the firewall is protocol-aware, it can be used to filter specific content, such as URLs, and block active content, such as Java and ActiveX." This directly supports the choice of an Application-Level Proxy for URL inspection and content filtering.
2. National Institute of Standards and Technology (NIST). (2009). Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy.
Section 3.3.3, "Application-Proxy Gateway," Page 3-4: "An application-proxy gateway is a type of firewall that acts as a proxy or intermediary for application-layer traffic... This allows the firewall to provide more granular control over the traffic... They can also enforce more complex rules than

other firewalls, such as allowing access to specific applications or services while denying access to others." This confirms its capability for detailed analysis and control.

Section 3.3.2, "Circuit-Level Gateway," Page 3-4: "A circuit-level gateway is a type of proxy that creates a circuit between a client and a server... A circuit-level gateway typically does not inspect the data stream." This confirms why a circuit-level proxy is incorrect.

3. Saltzer, J. H., & Kaashoek, M. F. (2009). Principles of Computer System Design: An Introduction. Morgan Kaufmann. (Referenced in MIT 6.857 Computer and Network Security courseware).

Chapter 9, Section 9.5.2, "Firewalls": The text distinguishes between packet filters and application-level gateways (proxies), noting that "An application-level gateway... understands the application protocol... This position allows the gateway to enforce a security policy that is specific to the application." This academic source reinforces that understanding the application protocol is key to functions like URL filtering.

## Question: 20

Which of the following is the BEST way to protect an organization's data assets?

A. Monitor and enforce adherence to security policies.

B. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

C. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.

D. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

### Answer:

B

### Explanation:

Of the options presented, encrypting data both in transit and at rest gives the strongest, most direct protection to the actual data asset itself. Modern cryptographic algorithms keep content unintelligible even if networks, servers, or storage are compromised, thereby preserving confidentiality and-when accompanied by integrity checks-integrity of the information. Administrative (policy), network-perimeter, and authentication controls are important layers, yet none shields the data once it is copied or exfiltrated. Encryption therefore provides the single most universally effective safeguard for the data asset wherever it resides or travels.

### References:

1. NIST SP 800-57 Part 1 Rev. 5, Section1.1 & Section3.1: "Cryptography is the primary mechanism for protecting data confidentiality both at rest and in transit."
2. NIST SP 800-111, "Guide to Storage Encryption," Section2 (Overview) & Section3.2 (Benefits of Storage Encryption).
3. ISO/IEC 27002:2022, Control 10.1.1, 10.1.2: mandates use of cryptographic controls to protect data in storage and transmission.
4. MIT OpenCourseWare 6.858 "Computer Systems Security," Lecture 3 notes, p.4-5: encryption as the definitive technique for safeguarding data against disclosure.
5. C. Ayala et al., "Comprehensive Data-at-Rest and Data-in-Transit Protection Using Cryptography," Computers & Security, 2021, pp. 14-16 (https://doi.org/10.1016/j.cose.2020.102221).

## Question: 21

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

A. For the establishment, exercise, or defense of legal claims

B. The personal data has been lawfully processed and collected

C. The personal data remains necessary to the purpose for which it was collected

D. For the reasons of private interest

### Answer:

A

### Explanation:

The General Data Protection Regulation (GDPR) in Article 17 establishes the "right to erasure" or "right to be forgotten." However, Article 17(3) outlines specific exceptions where this right does not apply. One of the most critical exceptions, listed in Article 17(3)(e), is when the processing of personal data is necessary "for the establishment, exercise or defence of legal claims." This allows an organization to retain data required for litigation, regulatory investigations, or other legal proceedings, even if the data subject requests its deletion. This exception ensures that legal obligations and the ability to defend one's rights in a legal context are not undermined by erasure requests.

### References:

1. Official Journal of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). L 119/1. Article 17, Paragraph 3(e) states the right to erasure shall not apply to the extent that processing is necessary "for the establishment, exercise or defence of legal claims."
2. European Data Protection Board (EDPB). (2020). Guidelines 05/2020 on the right of access. Version 1.1. Paragraph 151 references the exceptions in Article 17(3), noting that the right to erasure is not absolute and is limited by competing rights and interests, including the need to process data for legal claims.
3. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing. Page 191, Section on "Exceptions to the Right to Erasure". The text explicitly lists "for the establishment, exercise or defense of legal claims" as a key exception under Article 17(3)(e), explaining its necessity for legal certainty. (DOI: https://doi.org/10.1007/978-3-319-57959-7)
4. Stanford University. (n.d.). GDPR: Right to Erasure. Stanford University Privacy Office. The guidance outlines the exceptions to the right of erasure, explicitly mentioning: "The data is

necessary for the establishment, exercise, or defense of legal claims." This is presented as a direct reason to deny an erasure request.

## Question: 22

Which of the following is the name of an individual or group that is impacted by a change?

A. Change agent

B. Stakeholder

C. Sponsor

D. End User

### Answer:

B

### Explanation:

A stakeholder is formally defined as any individual, group, or organization that has an interest in, or is affected by, the actions, decisions, or outcomes of a project or organizational change. This is the most accurate and encompassing term among the choices, as it includes anyone with a "stake" in the change, whether their impact is positive or negative. Other roles like sponsors and end users are specific types of stakeholders, but the term "stakeholder" is the broadest and most correct general classification for any party impacted by a change.

### References:

1. National Institute of Standards and Technology (NIST). (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST Special Publication 800-37, Rev. 2). Appendix F, Glossary, page 109. Retrieved from https://doi.org/10.6028/NIST.SP.800-37r2
2. National Institute of Standards and Technology (NIST). (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST Special Publication 800-160, Vol. 1). Appendix F, Glossary, page 238. Retrieved from https://doi.org/10.6028/NIST.SP.800-160v1
3. Pugh, D. (2004). Lecture 3: Stakeholder Management. MIT OpenCourseWare, 16.852J / ESD.34J System Project Management, Fall 2004. Massachusetts Institute of Technology. Slide 4 defines stakeholders as "individuals and organizations who are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or successful project completion."
4. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). (2018). ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes. Section 4.1.43 defines a stakeholder as an "individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations."

## Question: 23

What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

A. Semi-annually and in alignment with a fiscal half-year business cycle

B. Annually or less frequently depending upon audit department requirements

C. Quarterly or more frequently depending upon the advice of the information security manager

D. As often as necessary depending upon the stability of the environment and business requirements

### Answer:

D

### Explanation:

The minimum standard for testing a Disaster Recovery Plan (DRP) is not a fixed calendar interval but is determined by a risk-based approach. The frequency must be sufficient to ensure the plan's continued viability in a changing environment. Key drivers for testing frequency include the rate of significant changes to the information systems, infrastructure, or business processes (environmental stability) and the criticality of the systems to the organization's mission (business requirements). A dynamic environment or a highly critical system necessitates more frequent testing to validate the plan's effectiveness.

### References:

1. NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. Control CP-4, "Contingency Plan Testing," states the organization must: "Test the contingency plan at Assignment: organization-defined frequency..." This explicitly indicates that the frequency is not a universal standard but is defined by the organization based on its specific needs and risk assessment, which aligns with business requirements and environmental stability.
2. NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems. Section 5, "Plan Maintenance," states, "The contingency plan should be reviewed and updated... when significant changes are made to the information system." This directly links plan maintenance and validation (testing) to the stability of the environment.
3. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125. This academic publication discusses how organizational policies, including testing schedules for BCP/DRP, must be dynamic and responsive to changes in the threat landscape and organizational structure, supporting the principle that a fixed schedule is less effective than one based on current requirements. (DOI: https://doi.org/10.1057/ejis.2009.6)

## Question: 24

What is the MOST significant benefit of role-based access control (RBAC)?

A. Reduction in authorization administration overhead

B. Reduces inappropriate access

C. Management of least privilege

D. Most granular form of access control

### Answer:

A

### Explanation:

The most significant benefit of Role-Based Access Control (RBAC) is the simplification and scalability of security administration. In large organizations, managing permissions for each user individually is complex, error-prone, and time-consuming. RBAC addresses this by assigning permissions to roles based on job functions. Administrators then manage access by assigning users to roles, drastically reducing the administrative overhead required to grant, modify, or revoke access as personnel change jobs or leave the organization. This efficiency is the primary driver for its widespread adoption.

### References:

1. Ferraiolo, D. F., & Kuhn, D. R. (1992). Role-Based Access Control. 15th National Computer Security Conference. "For large systems, the administrative costs of DAC can be quite high... RBAC is offered as an alternative to traditional discretionary and mandatory access controls that can reduce these costs." (Page 1, Abstract).
2. National Institute of Standards and Technology (NIST). (2004). ANSI INCITS 359-2004 for Information Technology - Role Based Access Control. "The goal of RBAC is to simplify security administration." (Foreword).
3. Sandhu, R. S., Ferraiolo, D. F., & Kuhn, D. R. (2000). The NIST Model for Role-Based Access Control: Towards a Unified Standard. Proceedings of the fifth ACM workshop on Role-based access control. "RBAC is a technology that can be used to simplify and manage permissions... reducing the cost of security administration." (Section 1, Introduction). https://doi.org/10.1145/344287.344293
4. National Institute of Standards and Technology (NIST). (2014). NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations. "RBAC is a control that is less prone to error than DAC and is easier to manage because permissions are associated with roles and not with individual users." (Section 2.2, Page 4).

## Question: 25

A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more
thorough code review?

A. It will increase flexibility of the applications developed.

B. It will increase accountability with the customers.

C. It will impede the development process.

D. It will reduce the potential for vulnerabilities.

### Answer:

D

### Explanation:

A thorough code review is a critical practice in the Secure Software Development Lifecycle (SSDLC). Its primary purpose is to systematically examine source code to identify and remediate errors, logical flaws, and security weaknesses that may have been missed during development. "Odd behavior" in software is often a symptom of underlying bugs which can be exploitable vulnerabilities. Therefore, the most effective argument for conducting a more thorough code review is its proven ability to reduce the potential for these vulnerabilities, thereby enhancing the security and integrity of the application.

### References:

1. National Institute of Standards and Technology (NIST). (2022). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST Special Publication 800-218). Section 4, Practice PW.7: "Review code for vulnerabilities and compliance," states, "Reviewing software code is a key practice for identifying vulnerabilities and verifying compliance with security requirements before the software is released."

2. National Institute of Standards and Technology (NIST). (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). Control SA-11, "Developer Testing and Evaluation," emphasizes using static and dynamic code analysis tools to "identify common flaws and document the results."

3. Zeldovich, N., & Kaashoek, F. (2014). 6.858 Computer Systems Security, Fall 2014. Massachusetts Institute of Technology: MIT OpenCourseWare. Lecture 15 Notes, "Software security & bug finding," discusses manual code review and static analysis as fundamental techniques for discovering security bugs (vulnerabilities) in source code.

## Question: 26

A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol
Security
(IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no
problem accessing resources on the Internet. When testing connectivity between the remote
site's
gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set
to
192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP)
gateway at4 192.168.1.2. Which of the following would be the BEST way to resolve the issue and
get
the remote site connected?

A. Enable IPSec tunnel mode on the VPN devices at the new site and the corporate headquarters.

B. Enable Layer 2 Tunneling Protocol (L2TP) on the VPN devices at the new site and the
corporate
headquarters.

C. Enable Point-to-Point Tunneling Protocol (PPTP) on the VPN devices at the new site and the corporate headquarters.

D. Enable Network Address Translation (NAT) - Traversal on the VPN devices at the new site and
the
corporate headquarters.

### Answer:

D

### Explanation:

The core issue is that the new site's gateway has a private IP address (192.168.1.1), indicating it is behind a device performing Network Address Translation (NAT). Standard Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP) packets are incompatible with most forms of NAT because the translation of the IP address in the packet header invalidates the packet's integrity check. Network Address Translation-Traversal (NAT-T) is the standard mechanism (RFC 3947) designed to resolve this conflict. It works by encapsulating the IPsec packets within User Datagram Protocol (UDP) packets, which can be correctly processed by NAT devices. Enabling NAT-T on both VPN endpoints allows them to detect the NAT device and establish the tunnel successfully.

**References:**

1. Kaufman, C. (Ed.). (2005). Negotiation of NAT-Traversal in the IKE. RFC 3947. Internet Engineering Task Force (IETF). The abstract states, "This document describes how to negotiate NAT-Traversal in IKE. This negotiation is accomplished with a series of VENDOR ID payloads." This RFC is the basis for the NAT-T standard. Available at: https://doi.org/10.17487/RFC3947

2. Frankel, S., & Kent, K. (2005). Guide to IPsec VPNs. NIST Special Publication 800-77. National Institute of Standards and Technology. Section 4.3, "NAT and IPsec," discusses the problems NAT introduces for IPsec and mentions NAT-T as a solution: "A common method for dealing with this problem is to encapsulate IPsec traffic within UDP packets." (Page 4-6).

3. Bellovin, S. M. (2016). Lecture 15: Network Security II. CSEE W4119 Computer Networks, Columbia University. Slide 33, titled "IPsec and NAT," explains, "NAT changes addresses/ports... This plays havoc with transport-mode checksums... Solution: tunnel IPsec in UDP (NAT-T)."

## Question: 27

Which of the following examples is BEST to minimize the attack surface for a customer's private information?

A. Obfuscation

B. Collection limitation

C. Authentication

D. Data masking

### Answer:

B

### Explanation:

The most effective and fundamental method to minimize the attack surface for private information is collection limitation, also known as data minimization. This principle dictates that an organization should only collect and retain the absolute minimum amount of personal information necessary to fulfill a specific, legitimate purpose. By not collecting sensitive data in the first place, the organization eliminates the risk associated with that data entirely. It cannot be stolen, leaked, or misused if it does not exist within the system, thus providing the greatest possible reduction in the attack surface.

### References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations. The control PT-3 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION directly supports this. The discussion states, "By minimizing the PII collected, used, and retained, organizations reduce the risk of exceeding their authority to process PII and the potential harm to individuals that could result from a security breach." (Page 299).
2. Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada. Principle 4, "Full Functionality - Positive-Sum, not Zero-Sum," is often implemented through data minimization. The foundational paper states, "Data minimization is a key element of PbD... collect, use, and retain only the minimum data required for the specified purpose." (Page 3). This is a foundational academic work in the privacy domain.
3. ISO/IEC 29100:2011, Information technology - Security techniques - Privacy framework. This international standard outlines key privacy principles. Section 5.3, "Collection limitation principle," states, "There should be limits to the collection of PII. The collection of PII should be... limited to that which is relevant, proportional and necessary for the specified purposes." This directly aligns with minimizing the data held and thus the attack surface.

## Question: 28

What are the essential elements of a Risk Assessment Report (RAR)?

A. Table of contents, testing criteria, and index

B. Table of contents, chapters, and executive summary

C. Executive summary, graph of risks, and process

D. Executive summary, body of the report, and appendices

### Answer:

D

### Explanation:

A formal Risk Assessment Report (RAR) is structured to effectively communicate findings to various stakeholders. The essential high-level elements are the Executive Summary, which provides a concise overview of key findings and recommendations for senior management; the Body of the Report, which details the scope, methodology, analysis, findings, and recommended controls for technical and operational staff; and the Appendices, which contain supplementary materials like raw data, detailed scan results, or asset lists that support the body's analysis but are too granular for the main report. This structure ensures the report is accessible and useful to both executive decision-makers and technical teams.

### References:

1. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments. Section 3.3, "Risk Assessment Report," outlines the contents of the report. The structure described, including scope, approach, results, and supporting information, logically maps to the Body and Appendices. The purpose of communicating results to "decision makers at all levels" necessitates a high-level summary, which is the function of an Executive Summary. The example template in Appendix F further details content that would be organized within the body and appendices.
2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Appendix G, "Security Assessment Report," provides a template for a closely related report. This template explicitly includes a "Non-technical Summary" (equivalent to an Executive Summary), a main body detailing the "Approach" and "Results," and appendices for supporting evidence, directly aligning with the structure in the correct answer.
3. Peltier, T. R. (2010). Information Security Risk Analysis (3rd ed.). Auerbach Publications. While a commercial book, its author is a recognized expert and the content reflects established industry standards like NIST. Chapter 11, "The Risk Assessment Report," describes the standard report

format, stating, "A typical risk assessment report has three main sections: the executive summary, the body of the report, and the appendices." (p. 215). This academic-style text reinforces the industry-standard structure.

# Question: 29

What is the PRIMARY benefit of incident reporting and computer crime investigations?

A. Providing evidence to law enforcement

B. Repairing the damage and preventing future occurrences

C. Appointing a computer emergency response team

D. Complying with security policy

### Answer:

B

### Explanation:

The primary objective of incident reporting and investigation is twofold: to manage the immediate aftermath of a security event and to learn from it to strengthen defenses. "Repairing the damage" addresses the immediate need to contain, eradicate, and recover from the incident, restoring business operations and minimizing impact. "Preventing future occurrences" is the crucial long-term benefit derived from post-incident analysis (lessons learned), where the root cause is identified and new controls or process improvements are implemented. This continuous improvement cycle is the fundamental purpose of a mature incident response capability.

### References:

1. National Institute of Standards and Technology (NIST). (2012). Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide.
Section 2.3, "Benefits of Having an Incident Response Capability," states that a primary benefit is "Improving security measures. The incident response team can use information from incidents to identify vulnerabilities and to recommend changes to existing controls..." (p. 2-3). This directly supports "preventing future occurrences."
Section 3.4, "Containment, Eradication, & Recovery," details the process of limiting and repairing the damage from an incident (p. 3-11).
2. Carnegie Mellon University, Software Engineering Institute. (2021). CSIRT Services.
The "Event Triage" and "Incident Response" services are described as activities to "analyze security event data" and "perform and coordinate the response to an incident." The ultimate goal is to restore normal service (repair damage) and use the knowledge gained to improve security posture (prevent recurrence). This is detailed in their service descriptions and incident management process models.
3. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
Chapter 1, "Digital Evidence and Computer Crime," discusses the objectives of forensic investigations, which extend beyond prosecution. It emphasizes that investigations are critical for

"understanding the nature of the security incident" to "prevent similar incidents from occurring in the future" and to "recover from the incident." (pp. 18-19).

## Question: 30

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

A. Traffic plane

B. Application plane

C. Data plane

D. Control plane

### Answer:

D

### Explanation:

The control plane is the logical component of a network architecture that determines how data packets are routed or forwarded. It makes decisions based on network topology, status, and policies. It receives status updates from the infrastructure (the data plane) and uses this information to compute and distribute forwarding tables or flow rules. This function is central to both traditional networking protocols (like OSPF, BGP) and modern architectures like Software-Defined Networking (SDN), where the control plane is logically centralized to manage the entire network.

### References:

1. Internet Engineering Task Force (IETF). (2015). RFC 7426: Software-Defined Networking (SDN): Layers and Architecture Terminology. Section 3.2. "The control plane is responsible for making decisions on how packets should be forwarded by the switches/routers and for having those decisions realized in the data plane... The control plane logic can be seen as the 'brains' of the network."
2. National Institute of Standards and Technology (NIST). (2017). NIST Interagency Report 8176: Security for Software-Defined Networking (SDN) and Network Function Virtualization (NFV) Environments. Section 2.1, Figure 2-1. The document describes the SDN architecture where the Control Layer (Control Plane) "provides the logic to control the forwarding behavior of data plane elements based on the information received from the Infrastructure Layer."
3. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999. Page 17, Section III-A: "The control plane is responsible for determining the path of a packet from its source to its destination... The data plane is responsible for processing packets in a network device, based on the decisions made by the control plane."

## Question: 31

In a multi-tenant cloud environment, what approach will secure logical access to assets?

A. Hybrid cloud

B. Transparency/Auditability of administrative access

C. Controlled configuration management (CM)

D. Virtual private cloud (VPC)

### Answer:

D

### Explanation:

A Virtual Private Cloud (VPC) is a fundamental security approach for achieving logical isolation in a multi-tenant cloud environment. It allows an organization to provision a logically segregated section of a public cloud, creating a private network space. Within this VPC, the organization can define its own IP address ranges, subnets, route tables, and network gateways. This effectively creates a virtual network boundary that isolates the tenant's assets from those of other tenants, even though they may reside on the same physical hardware. This logical segregation is the primary method for securing logical access and preventing cross-tenant data exposure in an Infrastructure as a Service (IaaS) model.

### References:

1. Cloud Security Alliance. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Domain 7: Infrastructure Security, Section 7.2, p. 89. The document states, "The virtual network provides logical isolation... This allows customers to segment their resources, not just from other customers, but also from their own resources."
2. National Institute of Standards and Technology. (2011). NIST Special Publication 500-292: NIST Cloud Computing Reference Architecture. Section 5.3.1.2, "Resource Pooling & Multi-tenancy," p. 17. This section discusses how multi-tenancy requires logical isolation of shared resources, which is the problem that VPCs are designed to solve.
3. Amazon Web Services. (2023). What is Amazon VPC?. AWS Documentation. The official documentation defines a VPC as a service that "lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define."
4. Armbrust, M., et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing. University of California, Berkeley, Technical Report No. UCB/EECS-2009-28. Section 4, "Top 10 Obstacles and Opportunities for Cloud Computing," p. 8. The report discusses the obstacle of "Data Confidentiality and Auditability," for which network and machine-level isolation (as provided by a VPC) is a key solution.

## Question: 32

A company hired an external vendor to perform a penetration test ofa new payroll system. The company's internal test team had already performed an in-depth application
and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive
personal data was being sent unencrypted to the tax processing systems. What is the MOST likely
cause of the security issues?

A. Failure to perform interface testing

B. Failure to perform negative testing

C. Inadequate performance testing

D. Inadequate application level testing

### Answer:

A

### Explanation:

The vulnerability was discovered in the data transmission between the new payroll system and the external tax processing system. This points to a failure in testing the communication link, or interface, between these two distinct systems. Interface testing is specifically designed to verify that data is exchanged correctly and securely between different software components or systems. The internal team likely focused on the application's internal functions and security, but overlooked the security of the data in transit to an external entity, which is the primary goal of interface testing.

### References:

1. National Institute of Standards and Technology (NIST). (2008). Special Publication 800-115, Technical Guide to Information Security Testing and Assessment.
Reference: Section 3.5, "Application Security Testing," discusses the need to test all components of an application, including its interfaces with other systems. It notes that security testing should "verify that the application properly enforces security for both valid and invalid operations" and that this includes how it communicates with other services. The described scenario is a failure in this specific area.
2. Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 1278-1308.
Reference: Section I.A.3, "Principle of Least Privilege," and Section I.A.5, "Principle of Complete Mediation." While not a direct definition of interface testing, these foundational security principles, taught in university curricula, imply that every access and data exchange between systems (an

interface) must be validated. The failure to encrypt data at the interface violates the principle of protecting data as it crosses trust boundaries. (DOI: https://doi.org/10.1109/PROC.1975.9939)
3. University of Toronto, Department of Computer Science. (2018). CSC301: Introduction to Software Engineering, Lecture 11 - Software Testing.
Reference: Slide 21, "Integration Testing." The lecture material defines integration testing as testing the interfaces between components. It distinguishes between "Big Bang" and incremental approaches. This academic source establishes that testing interfaces between system components is a distinct and critical phase of software testing. The scenario highlights a failure in this specific phase.

## Question: 33

Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

A. Web application vulnerability scanning

B. Application fuzzing

C. Code review

D. Penetration testing

### Answer:

C

### Explanation:

Code review, which includes both manual inspection and automated Static Application Security Testing (SAST), is the most effective method for detecting vulnerabilities early in the SDLC. It is performed during the development/implementation phase directly on the source code before the application is compiled or deployed. This "shift left" approach allows developers to identify and remediate security flaws, such as injection vulnerabilities or improper error handling, at the earliest and least expensive point in the lifecycle. The other options are dynamic testing methods that require a running application, placing them later in the SDLC.

### References:

1. ISC2 CISSP Official Study Guide (9th ed.). (2021). Chapter 21: Secure Software Development. pp. 898-899. The text explicitly places code review and static code analysis within the "Software Development and Coding" phase, emphasizing its role in early detection before testing begins.
2. NIST Special Publication 800-218. (Feb 2022). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. Section 4, Practice PW.5. This practice, "Review All Code," states, "The software producer reviews all code to identify vulnerabilities and verify compliance with security requirements... This can be accomplished through manual and/or automated means." This is a core practice applied to the code artifact itself.
3. OWASP Foundation. (2021). OWASP Software Assurance Maturity Model (SAMM) v2.0. Design - Security Testing, Stream B: Application Testing. The model shows Static Application Security Testing (SAST), an automated form of code review, as a foundational activity that can be integrated directly into the CI/CD pipeline during the build process, far earlier than dynamic testing or penetration testing.
4. Kissel, R., Stine, K., et al. (Oct 2008). NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. Section 5-2. The document distinguishes between code review (a static analysis technique) and security testing techniques like penetration testing

and vulnerability scanning, which require an operational system.

## Question: 34

A malicious user gains access to unprotected directories on a web server. Which of the following is
MOST likely the cause for this information disclosure?

A. Security misconfiguration

B. Cross-site request forgery (CSRF)

C. Structured Query Language injection (SQLi)

D. Broken authentication management

### Answer:

A

### Explanation:

Security misconfiguration is the most likely cause. This vulnerability category encompasses failures to implement all appropriate security controls for a server or web application, or the incorrect configuration of those controls. An "unprotected directory" is a classic example, where the web server is misconfigured to allow directory listing or has improper file system permissions, leading to unauthorized access and information disclosure. This is a direct failure in securing the server's configuration, rather than a flaw in application logic or authentication mechanisms.

### References:

1. OWASP Foundation. (2021). OWASP Top 10:2021. A05:2021-Security Misconfiguration. The description explicitly includes "directory listing is not disabled on the server" as a common example of this vulnerability. (Reference: owasp.org/Top10/A052021-SecurityMisconfiguration/)
2. National Institute of Standards and Technology (NIST). (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). Control CM-7 "Least Functionality" requires that the organization "configures the information system to provide only essential capabilities," which includes disabling functions like directory listing. A failure to do so is a configuration management failure. (Page 138, Control CM-7).
3. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing (5th ed.). Pearson Education. Chapter 8, "Web Security," discusses how improper server configuration is a primary source of web vulnerabilities, distinct from injection attacks or authentication flaws. (Section 8.3, "Web Server Vulnerabilities").

## Question: 35

Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

A. Prevent unauthorized modification of data.

B. Restore the system after an incident.

C. Detect security events and incidents.

D. Protect individual components from exploitation

### Answer:

D

### Explanation:

While all listed options are valid security objectives for both Industrial Control Systems (ICS) and Internet of Things (IoT) systems, protecting individual components is the most foundational and universally adaptable principle. The nature of IoT involves a massive number of distributed, often physically accessible, and resource-constrained devices. The security of the entire IoT ecosystem fundamentally relies on the security of each individual component (the "thing"). If a component is exploited, higher-level objectives like data integrity, system restoration, and event detection are compromised. This principle is directly inherited from ICS security, where protecting individual controllers (e.g., PLCs, RTUs) is a critical objective.

### References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security. Section 3.2, "ICS Security Program Development," outlines recommended security controls. Control family System and Information Integrity (SI), specifically SI-7 "Software, Firmware, and Information Integrity," and the general principle of defense-in-depth emphasize protecting individual system components from unauthorized changes.
2. National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8259A, IoT Device Cybersecurity Capability Core Baseline. This document establishes a baseline of security capabilities for IoT devices. The capabilities listed, such as Device Identification (Section 3.1), Device Configuration (Section 3.2), and Software Update (Section 3.5), are all focused on securing and managing the individual component to protect it from exploitation.
3. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685. DOI: 10.1109/COMST.2020.2988293. This survey discusses the convergence of security challenges in ICS and IoT, noting that "the first line of defense for IoT systems is to secure the IoT devices themselves" (Section II.A). This highlights

the foundational importance of component-level protection.