Free Questions for ISO-IEC-27001-Lead-Auditor

Shared by Lee on May 31, 2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Questions # 1:

You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre. Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.

Select four options for the actions you could take.

Options:

○ A.

Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared

○ B.

Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit

○ C.

Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity

○ D.

Note the progress made but hold the audit open until all corrective action has been cleared

○ E.

Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified

○ F.

Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity

○ G.

Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale

Answer

B, E, F, H

Explanation

According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1. The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1. Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:

Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame. The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.

Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.

Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.

Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised by implementing effective corrective actions for most of them and agreeing on a plan for the remaining

one. The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

Questions # 2:

The auditor used sampling to ensure that event logs recording information security events are maintained and regularly reviewed. Sampling was based on the audit objectives, whereas the sample selection process was based on the probability theory. What type of sampling was used?

Options:

○ A.

Statistical sampling

○ B.

Judgment-based sampling

○ C.

Systematic sampling

Answer

A

Explanation

The use of probability theory in the sample selection process indicates that "statistical sampling" was used. Statistical sampling allows auditors to make inferences about the population based on the properties of the sample, relying on the principles of probability to select representative elements.

References: ISO 19011:2018, Guidelines for auditing management systems

Questions # 3:

Scenario 6: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle

management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles This phase was crucial for aligning the team with the audit's objectives and scope However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber Acrypt's policies This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert s objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the

behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

Based on the scenario above, answer the following question:

Question:

According to Scenario 6, Cyber ACrypt **modified the SoA and the ISMS policy** after the **Stage 1 audit report**. How do you define this situation?

Options:

○ A.

Unacceptable, once the external audit passes Stage 1, the SoA and the ISMS policy cannot be modified

○ B.

Acceptable, situations that lead to major nonconformities during the Stage 2 audit should be corrected

○ C.

Acceptable, minor modifications to the SoA and ISMS policy can be made until the submission of the final audit report

Answer

B

Explanation

Comprehensive and Detailed In-Depth Explanation:

B. Correct Answer:

Stage 1 audits identify gaps and allow the organization to correct major nonconformities before **Stage 2 certification**.

ISO/IEC 27006 requires organizations to address major nonconformities before proceeding to Stage 2.

A. Incorrect:

Organizations are allowed to correct nonconformities identified in

Stage 1.

C. Incorrect:

Major changes must be addressed, not just minor modifications.

Relevant Standard Reference:

ISO/IEC 27006:2020 Clause 9.2.3 (Stage 1 and Stage 2 Audit Process)

Questions # 4:

Scenario 7: Webvue. headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software. Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users. CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously Webvue takes pride in its strictness regarding asset confidentiality They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use. restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud

The audit team comprised five persons Keith. Sean. Layla, Sam. and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application) Their tasks included audit planning according to Webvue’s internal systems and processes Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys

are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue. focusing on how the company adhered to its policies and regulatory standards. As part of this process. Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the non conformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Based on the scenario above, answer the following question:

Question:

Based on Scenario 7, the audit team checked **Webvue’s cryptography policy** to obtain **reasonable assurance** of the information obtained during **interviews**. Which type of **audit procedure** has been used?

Options:

○ A.

Observation

○ B.

Corroboration

○ C.

Evaluation

Answer

B

Explanation

Comprehensive and Detailed In-Depth Explanation:

B. Correct Answer:

Corroboration is the process of **validating verbal statements with documented evidence**.

ISO 19011:2018 emphasizes cross-verification of audit evidence to ensure accuracy.

A. Incorrect:

Observation involves witnessing real-time processes, but here, the audit team **compared interview data with documentation**.

C. Incorrect:

Evaluation assesses compliance with criteria, but **corroboration focuses on evidence validation**.

Relevant Standard Reference:

ISO 19011:2018 Clause 6.4.7 (Corroboration of Audit Evidence)

Questions # 5:

You are an experienced ISMS Audit Team Leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-

Do-Check-Act cycle in respect of the operation of the information security management system.

You do this by asking him to select the answer which best describes the purpose of the check activity 'management review.

The purpose of the management review is to: Select 1

Options:

○ A.

Assess the information security management system at random intervals to ensure its continuing efficiency, adequacy and effectiveness.

○ B.

Consider the information security management system at regular intervals to ensure its continuing compliance, adequacy and effectiveness.

○ C.

Review the information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

○ D.

Update the information security management system at documented intervals to ensure its continuing conformity, adequacy and effectiveness.

Answer

C

Explanation

The management review is a key component of the "Check" stage in the Plan-Do-Check-Act (PDCA) cycle. Its primary purpose is to evaluate the overall ISMS and make strategic decisions for improvement. Here's why the other options are less accurate:

•A. Random intervals: Reviews should be conducted at planned intervals for consistency and tracking progress.

•B. Compliance: While compliance is a consideration, the main focus is on the system's suitability for the organization's needs, its adequacy in managing risks, and its overall effectiveness in achieving information security objectives.

•D. Update: The management review might lead to updates, but its primary goal is evaluation, not immediate modification.

References:

•ISO/IEC 27001:2022, Section 9.3 (Management Review): Outlines the purpose and

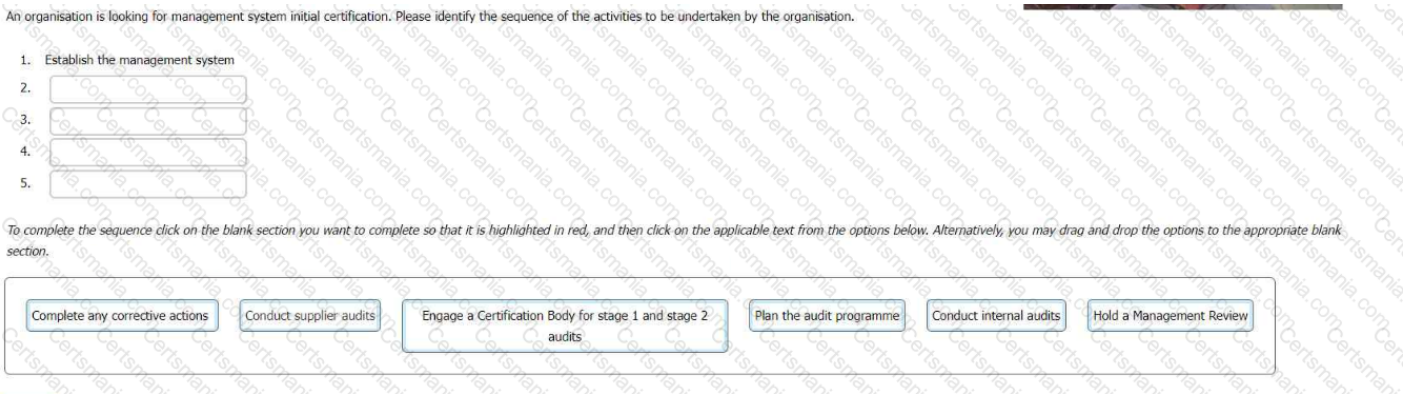
requirement for conducting management reviews.

•PECB Candidate Handbook, ISO/IEC 27001 Lead Auditor: Emphasizes the management review's role in evaluating the ISMS's suitability, adequacy, and effectiveness, driving continuous improvement.

Questions # 6:

An organisation is looking for management system initial certification. Please identify the sequence of the activities to be undertaken by the organisation.

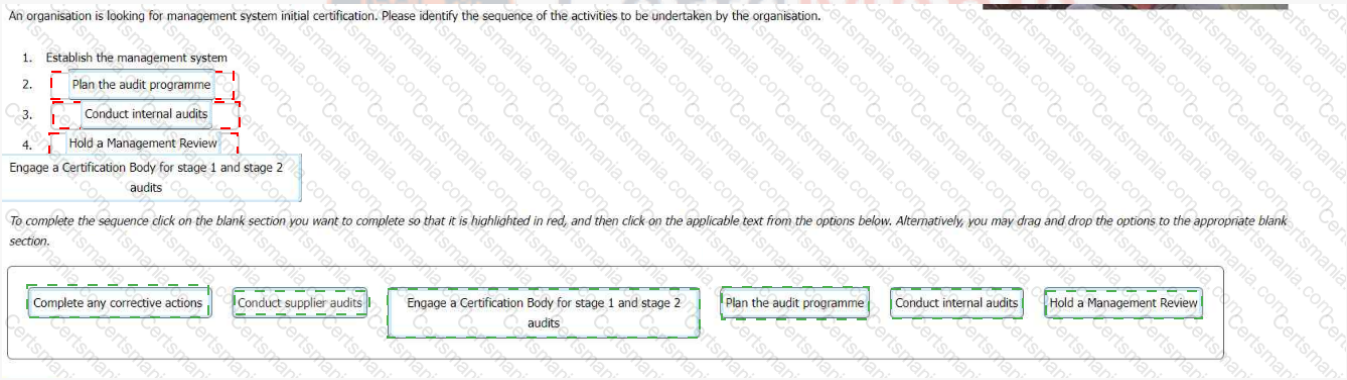
To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.



Options:

Answer

Answer:



Explanation

The correct sequence of activities is:

Establish the management system

Plan the audit programme

Conduct internal audits

Hold a Management Review

Engage a Certification Body for stage 1 and stage 2 audits

Complete any corrective actions

Comprehensive but Short Explanation: = According to the PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, the steps for achieving certification are as follows1:

Establish the management system: This involves defining the scope, objectives, policies, procedures, and controls of the ISMS, as well as ensuring the availability of resources and top management commitment.

Plan the audit programme: This involves defining the audit objectives, criteria, scope, frequency, methods, and responsibilities for conducting internal audits of the ISMS.

Conduct internal audits: This involves verifying the conformity and effectiveness of the ISMS, as well as identifying any nonconformities or opportunities for improvement.

Hold a Management Review: This involves reviewing the performance and suitability of the ISMS, as well as deciding on any changes or actions needed to improve it.

Engage a Certification Body for stage 1 and stage 2 audits: This involves selecting a reputable and accredited certification body to conduct an external audit of the ISMS, consisting of two stages: a documentation review and an on-site assessment.

Complete any corrective actions: This involves addressing any nonconformities or findings identified by the certification body, and providing evidence of their implementation and effectiveness.

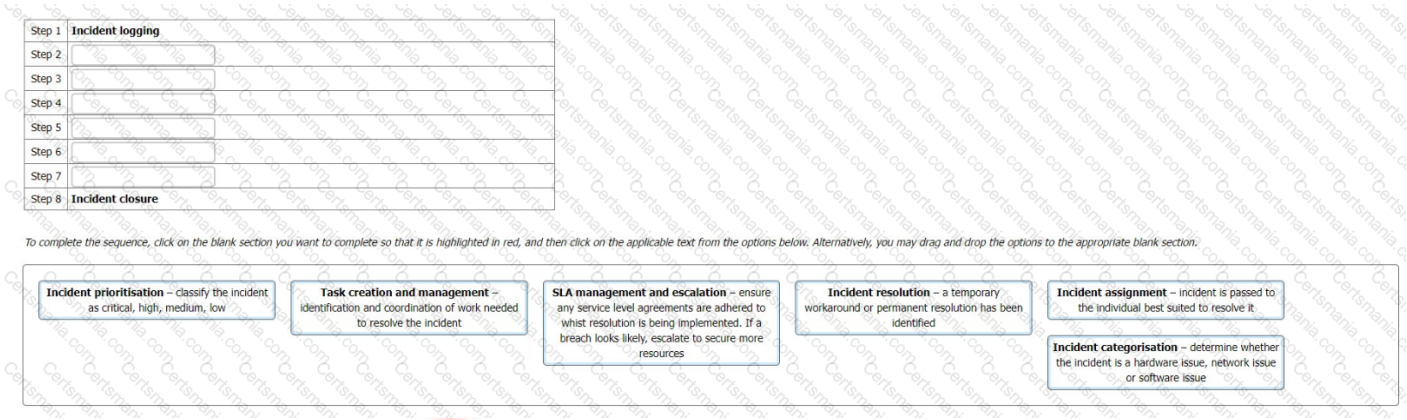
References: = 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, pages 25-26.

Questions # 7:

Your organisation is currently seeking ISO/IEC27001:2022 certification. You have just qualified as an Internal ISMS auditor and the ICT Manager wants to use your newly acquired knowledge to assist him with the design of an information security incident management process.

He identifies the following stages in his planned process and asks you to confirm which order

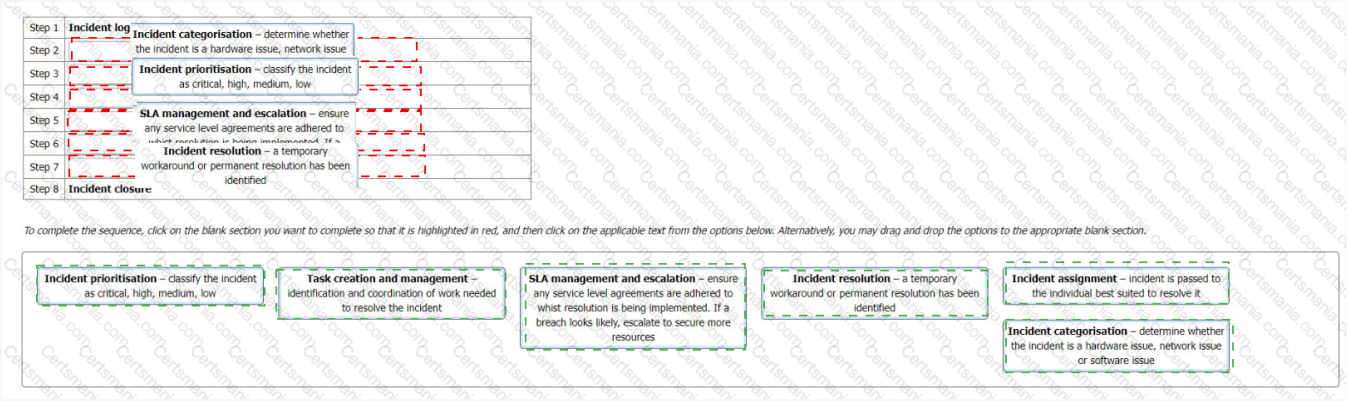
they should appear in.



Options:

Answer

Answer:



Explanation

Step 1 = Incident logging Step 2 = Incident categorisation Step 3 = Incident prioritisation Step 4 = Incident assignment Step 5 = Task creation and management Step 6 = SLA management and escalation Step 7 = Incident resolution Step 8 = Incident closure

The order of the stages in the information security incident management process should follow a logical sequence that ensures a quick, effective, and orderly response to the incidents, events, and weaknesses. The order should also be consistent with the best practices and guidance provided by ISO/IEC 27001:2022 and ISO/IEC 27035:2022. Therefore, the following order is suggested:

Step 1 = Incident logging: This step involves recording the details of the potential incident, event, or weakness, such as the date, time, source, description, impact, and reporter. This step is important to provide a traceable record of the incident and to facilitate the subsequent analysis and response. This step is related to control A.16.1.1 of ISO/IEC 27001:2022, which requires the organization to establish

responsibilities and procedures for the management of information security incidents, events, and weaknesses. This step is also related to clause 6.2 of ISO/IEC 27035:2022, which provides guidance on how to log the incidents, events, and weaknesses.

Step 2 = Incident categorisation: This step involves determining the type and nature of the incident, event, or weakness, such as whether it is a hardware issue, network issue, or software issue. This step is important to classify the incident and to assign it to the appropriate resolver or team. This step is related to control A.16.1.2 of ISO/IEC 27001:2022, which requires the organization to report information security events and weaknesses as quickly as possible through appropriate management channels. This step is also related to clause 6.3 of ISO/IEC 27035:2022, which provides guidance on how to categorize the incidents, events, and weaknesses.

Step 3 = Incident prioritisation: This step involves assessing the severity and urgency of the incident, event, or weakness, and classifying it as critical, high, medium, or low. This step is important to prioritize the incident and to allocate the necessary resources and time for the response. This step is related to control A.16.1.3 of ISO/IEC 27001:2022, which requires the organization to assess and prioritize information security events and weaknesses in accordance with the defined criteria. This step is also related to clause 6.4 of ISO/IEC 27035:2022, which provides guidance on how to prioritize the incidents, events, and weaknesses.

Step 4 = Incident assignment: This step involves passing the incident, event, or weakness to the individual or team who is best suited to resolve it, based on their skills, knowledge, and availability. This step is important to ensure that the incident is handled by the right person or team and to avoid delays or confusion. This step is related to control A.16.1.4 of ISO/IEC 27001:2022, which requires the organization to respond to information security events and weaknesses in a timely manner, according to the agreed procedures. This step is also related to clause 6.5 of ISO/IEC 27035:2022, which provides guidance on how to assign the incidents, events, and weaknesses.

Step 5 = Task creation and management: This step involves identifying and coordinating the work needed to resolve the incident, event, or weakness, such as performing root cause analysis, testing solutions, implementing changes, and documenting actions. This step is important to ensure that the incident is resolved effectively and efficiently, and that the actions are tracked and controlled. This step is related to control A.16.1.5 of ISO/IEC 27001:2022, which requires the organization to apply lessons learned from information security events and weaknesses to take corrective and preventive actions. This step is also related to clause 6.6 of ISO/IEC 27035:2022, which provides guidance on how to create and manage the tasks for the incidents, events, and weaknesses.

Step 6 = SLA management and escalation: This step involves ensuring that any service level agreements (SLAs) are adhered to while the resolution is being implemented, and that the incident is escalated to a higher level of authority or support if a breach looks likely or occurs. This step is important to ensure that the incident is resolved within the agreed time frame and quality, and that any deviations or issues are communicated and addressed. This step is related to control

A.16.1.6 of ISO/IEC 27001:2022, which requires the organization to communicate information security events and weaknesses to the relevant internal and external parties, as appropriate. This step is also related to clause 6.7 of ISO/IEC 27035:2022, which provides guidance on how to manage the SLAs and escalations for the incidents, events, and weaknesses.

Step 7 = Incident resolution: This step involves applying a temporary workaround or a permanent solution to resolve the incident, event, or weakness, and restoring the normal operation of the information and information processing facilities. This step is important to ensure that the incident is resolved completely and satisfactorily, and that the information security is restored to the desired level. This step is related to control A.16.1.7 of ISO/IEC 27001:2022, which requires the organization to identify the cause of information security events and weaknesses, and to take actions to prevent their recurrence or occurrence. This step is also related to clause 6.8 of ISO/IEC 27035:2022, which provides guidance on how to resolve the incidents, events, and weaknesses.

Step 8 = Incident closure: This step involves closing the incident, event, or weakness, after verifying that it has been resolved satisfactorily, and that all the actions have been completed and documented. This step is important to ensure that the incident is formally closed and that no further actions are required. This step is related to control A.16.1.8 of ISO/IEC 27001:2022, which requires the organization to collect evidence and document the information security events and weaknesses, and the actions taken. This step is also related to clause 6.9 of ISO/IEC 27035:2022, which provides guidance on how to close the incidents, events, and weaknesses.

References:

ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements1

PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2

ISO 27001:2022 Lead Auditor - PECB3

ISO 27001:2022 certified ISMS lead auditor - Jisc4

ISO/IEC 27001:2022 Lead Auditor Transition Training Course5

ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6

ISO/IEC 27035:2022, Information technology — Security techniques — Information security incident management

Questions # 8:

Which two of the following standards are used as ISMS third-party certification audit criteria?

Options:

○ A.

ISO/IEC 27002

○ B.

ISO/IEC 20000-1

○ C.

ISO 19011

○ D.

ISO/IEC 27001

○ E.

Relavent legal, statutory, and regulatory requirements

○ F.

ISO/IEC 17021-1

Answer

D, E

Explanation

The two standards that are used as ISMS third-party certification audit criteria are ISO/IEC 27001 and relevant legal, statutory, and regulatory requirements. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS)1. Relevant legal, statutory, and regulatory requirements are those that apply to the organization’s information security aspects and objectives2. The other options are either not standards (E) or not directly related to the ISMS certification audit criteria (A, B, C, F). References: 1: ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements, Clause 1 \n2: ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements, Clause 4.2

Questions # 9:

Scenario 4: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs. Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology. equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.

During the last audit. Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence based approach, particularly in light of two information security incidents reported by Techvology in the past year The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement

The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards The auditors also verified whether Techvology complied with the contractual requirements established between the two entities This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.

Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.

The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.

Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives'

claims about the incident management processes.

Based on the scenario above, answer the following question:

Question:

Based on Scenario 4, what type of audit did Branding conduct?

Options:

○ A.

First-party audit

○ B.

Second-party audit

○ C.

Third-party audit

Answer

B

Explanation

Comprehensive and Detailed In-Depth Explanation:

B. Correct Answer:

A second-party audit is conducted by an **organization on its suppliers or outsourced service providers** to ensure compliance with contractual and regulatory requirements.

Branding audited Techvology, an **outsourced IT service provider**, making this a **second-party audit**.

A. Incorrect:

A first-party audit is an internal audit, but Techvology is **not an internal entity**.

C. Incorrect:

A third-party audit is performed by an independent certification body, which is **not the case here**.

Relevant Standard Reference:

ISO 19011:2018 Clause 3.8 (Types of Audits: First, Second, and Third-Party Audits)

Questions # 10:

Scenario 8: Tessa. Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organization's security controls and its risk tolerance in accurately characterizing the risk level within an organization On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting They analyzed one of Michael s findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organization's daily operations, which he believed was caused by one of the organization's IT technicians As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification

recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

Based on the scenario above, answer the following question:

Question:

Tessa was **advised to avoid providing unnecessary evidence** in the audit report for Clastus's **certification audit**. Is this recommended?

Options:

○ A.

Yes, to avoid including information that may compromise the audit's confidentiality

○ B.

Yes, to simplify the report for a better understanding

○ C.

No, to ensure that all relevant evidence is considered and addressed

Answer

C

Explanation

Comprehensive and Detailed In-Depth Explanation:

C. Correct Answer:

ISO 19011:2018 requires audit reports to include all relevant evidence supporting audit conclusions.

Omitting evidence for conciseness undermines transparency and credibility.

A. Incorrect:

Audit confidentiality is protected through controlled access, not by omitting evidence.

B. Incorrect:

Clarity is important, but not at the expense of completeness.

Relevant Standard Reference:

ISO 19011:2018 Clause 6.7 (Audit Reporting Best Practices)

Questions # 11:

You are an experienced ISMS audit team leader providing guidance to an auditor in training.

The auditor in training appears to be confused about the interpretation of competence in ISO 27001:2022 and is seeking clarification from you that his understanding is correct. He sets out a series of mini scenarios and asks you which of these you would attribute to a lack of competence. Select four correct options.

Options:

○ A.

An employee recently transferred from the IT networks team to Software development was unaware of the need to complete product release forms prior to shipping

○ B.

A senior programmer did not check their coding for errors as they were running late for a doctor's appointment

○ C.

A new starter was unable to switch on CCTV monitoring because they had not been shown how to do this

○ D.

An IT technician failed to configure a new model of server correctly as a result of not reading the supplied instructions

○ E.

An experienced receptionist allowed a contractor she recognised to enter the data centre without his access card

○ F.

A system administrator deleted two live accounts as well as five redundant accounts as a result of receiving an incorrect instruction

○ G.

A data centre operator inadvertently placed a backup tape into an incorrect drive because they were in a hurry to move on to another task

Answer

A, C, D, H

Explanation

These four scenarios are examples of a lack of competence, which is defined as the ability to apply the knowledge and skills needed to perform a work role or a task effectively and efficiently12. Competence in ISO 27001:2022 is determined by the organisation's needs and expectations, and it is based on the relevant education, training, or experience of the people involved in the ISMS34. The organisation is required to ensure that all the people who affect the performance of the ISMS are competent, and to provide them with the necessary training and awareness to fulfil their roles and responsibilities35. The four scenarios indicate that the people involved either lack the knowledge or skills to perform their tasks, or have not received the appropriate training or guidance to do so. The other scenarios are not related to competence, but to other factors such as negligence, error, or policy violation.

References: = 1: ISO 19011:2018 Guidelines for auditing management systems, clause 3.72: ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing, clause 53: ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements, clause 7.24: ISO 27001 Requirement 7.2 – Competence | ISMS.online15: ISO27001 Clause 7.2 Competence - Ultimate Certification Guide - High Table3

Questions # 12:

Question:

Which of the following can be considered a **minor nonconformity**?

Options:

○ A.

Employees lack training to recognize phishing attempts, increasing malware risks

○ B.

Lack of multi-factor authentication leaves accounts vulnerable to unauthorized access

○ C.

The information security policy lacks reference to continual ISMS improvement

Answer

C

Explanation

Comprehensive and Detailed In-Depth Explanation:

C. Correct Answer:

A missing reference to continual improvement is a documentation issue, not an immediate security risk, making it a **minor nonconformity**.

A. Incorrect:

Lack of employee training poses a direct security risk (major nonconformity).

B. Incorrect:

Missing multi-factor authentication significantly weakens security (major nonconformity).

Relevant Standard Reference:

ISO/IEC 27001:2022 Clause 10.1 (Continual Improvement)