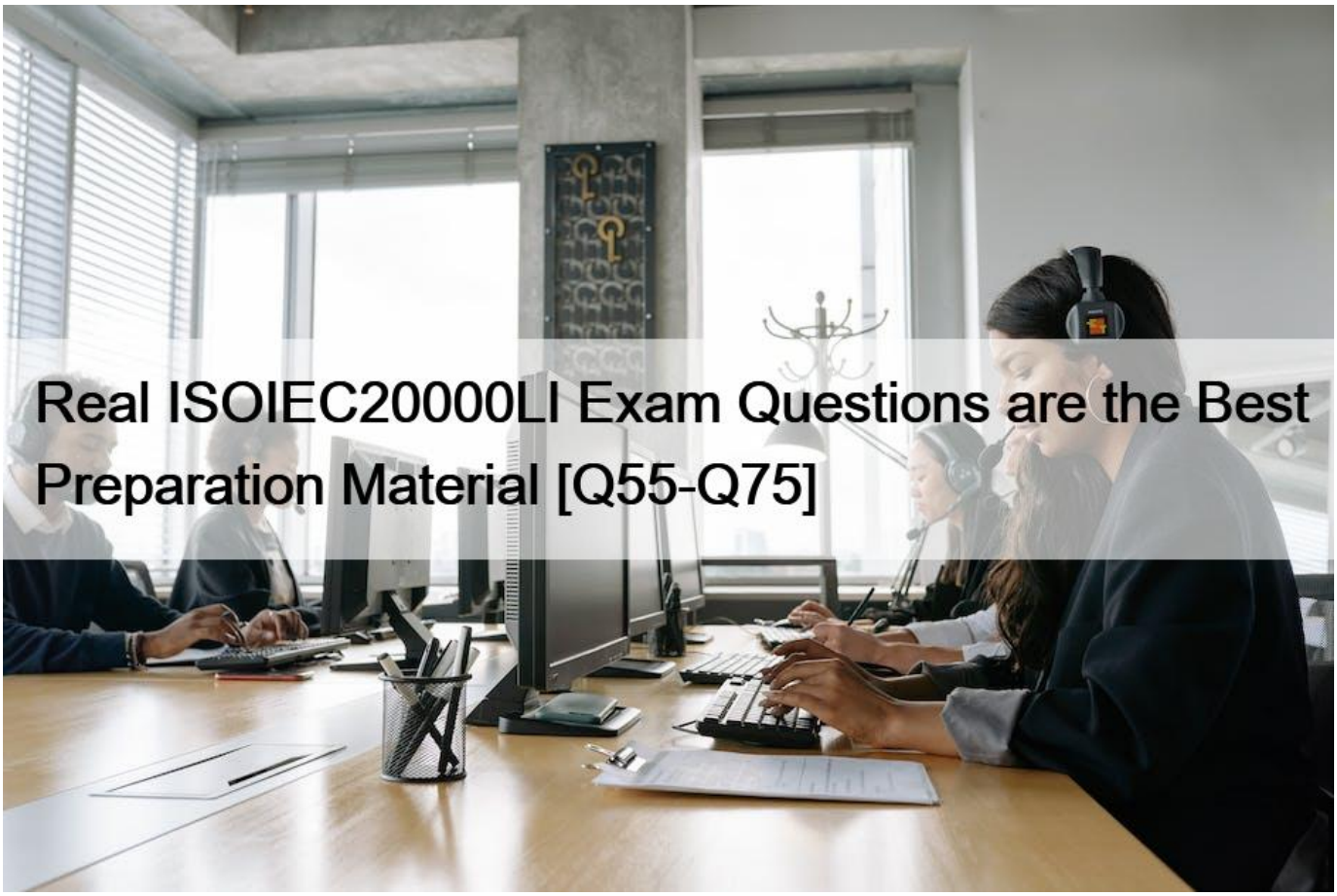
Real ISOIEC20000LI Exam Questions are the Best Preparation Material [Q55-Q75



Real ISOIEC20000LI Exam Questions are the Best Preparation Material
Practice on 2025 LATEST ISOIEC20000LI Exam Updated 123 Questions

Q55. Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.

To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was

based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001′ Refer to scenario 3.
* No, the control should be implemented only for defining rules for cryptographic key management
* Yes, the control for the effective use of the cryptography can include cryptographic key management
* No, because the standard provides a separate control for cryptographic key management
According to ISO/IEC 27001:2022, Annex A.8.24, the control for the effective use of cryptography is intended to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This control can include cryptographic key management, which is the process of generating, distributing, storing, using, and destroying cryptographic keys in a secure manner. Cryptographic key management is essential for ensuring the security and functionality of cryptographic solutions, such as encryption, digital signatures, or authentication.

The standard provides the following guidance for implementing this control:

* A policy on the use of cryptographic controls should be developed and implemented.

* The policy should define the circumstances and conditions in which the different types of cryptographic controls should be used, based on the information classification scheme, the relevant agreements, legislation, and regulations, and the assessed risks.

* The policy should also define the standards and techniques to be used for each type of cryptographic control, such as the algorithms, key lengths, key formats, and key lifecycles.

* The policy should be reviewed and updated regularly to reflect the changes in the technology, the business environment, and the legal requirements.

* The cryptographic keys should be managed through their whole lifecycle, from generation to destruction, in a secure and controlled manner, following the principles of need-to-know and segregation of duties.

* The cryptographic keys should be protected from unauthorized access, disclosure, modification, loss, or theft, using appropriate physical and logical security measures, such as encryption, access control, backup, and audit.

* The cryptographic keys should be changed or replaced periodically, or when there is a suspicion of compromise, following a defined process that ensures the continuity of the cryptographic services and the availability of the information.

* The cryptographic keys should be securely destroyed when they are no longer required, or when they reach their end of life, using methods that prevent their recovery or reconstruction.

References:

* ISO/IEC 27001:2022 Lead Implementer Course Guide1

* ISO/IEC 27001:2022 Lead Implementer Info Kit2

* ISO/IEC 27001:2022 Information Security Management Systems – Requirements3

* ISO/IEC 27002:2022 Code of Practice for Information Security Controls4

* Understanding Cryptographic Controls in Information Security5

Q56. Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management

[system implementation, TradeB’s top management contracted two experts to direct and manage the ISMS implementation project.

First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted Based on scenario 4, the fact that TradeB defined the level of risk based on three nonnumerical categories indicates that;
* The level of risk will be evaluated against qualitative criteria
* The level of risk will be defined using a formula
* The level of risk will be evaluated using quantitative analysis

Qualitative risk assessment is a method of evaluating risks based on nonnumerical categories, such as low, medium, and high. It is often used when there is not enough data or resources to perform a quantitative risk assessment, which involves numerical values and calculations. Qualitative risk assessment relies on the subjective judgment and experience of the risk assessors, and it can be influenced by various factors, such as the context, the stakeholders, and the criteria. According to ISO/IEC 27001:2022, Annex A, control A.8.2.1 states: “The organization shall define and apply an information security risk assessment process that: … d) identifies the risk owners; e) analyses the risks: i) assesses the consequences that would result if the risks identified were to materialize; ii) assesses the realistic likelihood of the occurrence of the risks; f) identifies and evaluates options for the treatment of risks; g) determines the levels of residual risk and whether these are acceptable; and h) identifies the risk owners for the residual risks.” Therefore, TradeB’s decision to define the level of risk based on three nonnumerical categories indicates that they used a qualitative risk assessment process.

References:

* ISO/IEC 27001:2022, Annex A, control A.8.2.1

* PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slides 12-13

Q57. Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients’ data and medical history, and communicate with all the

[involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic’s patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients’ privacy.

Which situation described in scenario 1 represents a threat to HealthGenic?
* HealthGenic did not train its personnel to use the software
* The software company modified information related to HealthGenic’s patients
* HealthGenic used a web-based medical software for storing patients’ confidential information

According to ISO/IEC 27001:2022, a threat is any incident that could negatively affect the confidentiality, integrity or availability of an asset1. In this scenario, the asset is the information related to HealthGenic’s patients, which is stored and processed by the web-based medical software. The software company’s modification of some files that comprised sensitive information related to HealthGenic’s patients is an incident that could negatively affect the confidentiality and integrity of the asset, as it resulted in incomplete and incorrect medical reports and invaded the patients’ privacy. Therefore, this situation represents a threat to HealthGenic.

References:

* ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements

* ISO 27001 Key Terms – PJR

Q58. Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Texas M&H Inc. decided to integrate the incident management policy to the existent information security policy. How do you define this situation?
* Acceptable, the incident management policy may be integrated into the overall information security policy of the organization
* Acceptable, but only if the incident management policy addresses environmental, or health and safety issues
* Unacceptable, the incident management policy should be drafted as a separate document in order to be clear and effective

Q59. Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company’s stock.

Tessa was SunDee’s internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee

must evaluate the performance of the ISMS adequately. She defined SunDee’s negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management According to scenario 8, Tessa created a plan for ISMS monitoring and measurement and presented it to the top management Is this acceptable?

* No, Tessa should only communicate the issues found to the top management
* Yes, Tessa can advise the top management on improving the company’s functions
* No, Tessa must implement all the improvements needed for issues found during the audit

According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the roles and responsibilities of an internal auditor is to provide recommendations for improvement based on the audit findings1. Therefore, Tessa can create a plan for ISMS monitoring and measurement and present it to the top management as a way of advising them on how to improve the company’s functions. However, Tessa is not responsible for implementing the improvements or communicating the issues found to the top management. Those tasks belong to the process owners and the management representative, respectively2.

References: 1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 14 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 15

Q60. What risk treatment option has Company A Implemented If it has decided not to collect information from users so that It is not necessary to implement information security controls?

* Risk avoidance
* Risk retention
* Risk modification

Q61. Based on scenario 5, what can be considered as a residual risk to Socket Inc.?

* Files arc decrypted once the user is authenticated
* Users with access to cloud storage files are segregated on a separate network
* The use of passwords with at least 12 characters containing a mixture of uppercase and lowercase letters, symbols, and numbers

Q62. What should an organization demonstrate through documentation?

* That the complexity of processes and their interactions is documented
* That the distribution of paper copies is regularly complete
* That Its security controls are implemented based on risk scenarios

Q63. Who should verily the effectiveness of the corrective actions taken by the auditee after an internal audit?

* An Independent auditor should be contracted to perform this evaluation
* The internal auditor
* The information security manager

Q64. Which situation described in scenario 2 Indicates service unavailability?

* Lucas was no! able to access the website with his credentials
* Attackers still had access to the data when Solena delivered a press release
* Lucas was asked to change his password weekly

Q65. Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the

incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.

To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Based on the scenario above, answer the following question:

Which security control does NOT prevent information security incidents from recurring?
* Segregation of networks
* Privileged access rights
* Information backup
Information backup is a corrective control that aims to restore the information in case of data loss, corruption, or deletion. It does not prevent information security incidents from recurring, but rather mitigates their impact.

The other options are preventive controls that reduce the likelihood of information security incidents by limiting the access to authorized personnel, segregating the networks, and using cryptography. These controls can help Socket Inc. avoid future attacks on its MongoDB database by addressing the vulnerabilities that were exploited by the hackers.

References:

* ISO 27001:2022 Annex A 8.13 – Information Backup1

* ISO 27001:2022 Annex A 8.1 – Access Control Policy2

* ISO 27001:2022 Annex A 8.2 – User Access Management3

* ISO 27001:2022 Annex A 8.3 – User Responsibilities4

* ISO 27001:2022 Annex A 8.4 – System and Application Access Control

* ISO 27001:2022 Annex A 8.5 – Cryptography

* ISO 27001:2022 Annex A 8.6 – Network Security Management

Q66. Scenario 7: InfoSec is a multinational corporation headquartered in Boston, MA, which provides professional electronics, gaming, and entertainment services. After facing numerous information security incidents, InfoSec has decided to establish teams and implement measures to prevent potential incidents in the future Emma, Bob. and Anna were hired as the new members of InfoSec’s information security team, which consists of a security architecture team, an incident response team (IRT) and a forensics team Emma’s job is to create information security plans, policies, protocols, and training to prepare InfoSec to respond to incidents effectively Emma and Bob would be full-time employees of InfoSec, whereas Anna was contracted as an external consultant.

Bob, a network expert, will deploy a screened subnet network architecture This architecture will isolate the demilitarized zone (OMZ) to which hosted public services are attached and InfoSec’s publicly accessible resources from their private network Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company’s network. Bob is also responsible for ensuring that a thorough evaluation of the nature of an unexpected event is conducted, including the details on how the event happened and what or whom it might affect.

Anna will create records of the data, reviews, analysis, and reports in order to keep evidence for the purpose of disciplinary and legal action, and use them to prevent future incidents. To do the work accordingly, she should be aware of the company’s information security incident management policy beforehand Among others, this policy specifies the type of records to be created, the place where they should be kept, and the format and content that specific record types should have.

Based on this scenario, answer the following question:

Based on his tasks, which team is Bob part of?
* Security architecture team
* Forensics team
* Incident response team

Based on his tasks, Bob is part of the incident response team (IRT) of InfoSec. According to ISO/IEC 27035-

2:2023, the IRT is a team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way1. One of the tasks of the IRT is to conduct an evaluation of the nature of an unexpected event, including the details on how the event happened and what or whom it might affect1.

This is consistent with Bob’s responsibility of ensuring that a thorough evaluation of the nature of an unexpected event is conducted. Therefore, Bob belongs to the incident response team.

References:

* ISO/IEC 27035-2:2023 (en), Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response1

* Response to Information Security Incidents | ISMS.online2

Q67. Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a jombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.

However, the company requested from the certification body that the documentation could not be carried off- site However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company’s top management, was a potential conflict of interest. The request was not accepted by the certification body The certification body rejected NetworkFuse’s request to change the audit team leader. Is this acceptable?

Refer to scenario 10.

* No, because an auditee cannot request the rejection of an audit team member
* Yes, because NetworkFuse did not give a valid reason to support their claims
* No, auditee’s requests for the replacement of auditors must be accepted

According to the ISO/IEC 27001 : 2022 Lead Implementer course, the certification body is responsible for selecting and appointing the audit team members, taking into account the competence, impartiality, and objectivity of the auditors1. The auditee can request the replacement of an audit team member only if there is a valid reason to doubt their competence or impartiality, such as a personal or professional conflict of interest, a lack of relevant experience or qualifications, or a previous involvement in the auditee’s activities2.

However, NetworkFuse did not give a valid reason to support their claims, as the fact that the audit team leader issued a recommendation for certification to their main competitor does not imply a conflict of interest or a bias. Therefore, the certification body rejected NetworkFuse’s request to change the audit team leader, which is acceptable.

References: 1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 11: Certification Audit of the ISMS, slide 13 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 11: Certification Audit of the ISMS, slide 14

Q68. An organization wants to enable the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. Which control should it implement7

* Use of privileged utility programs
* Clock synchronization
* Installation of software on operational systems

Clock synchronization is the control that enables the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. According to ISO/IEC

27001:2022, Annex A, control A.8.23.1 states: “The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.” This ensures that the timestamps of the events and data are consistent and accurate across different systems and sources, which facilitates the identification of causal relationships, patterns, trends, and anomalies. Clock synchronization also helps to establish the sequence of events and the responsibility of the parties involved in an incident.

References:

* ISO/IEC 27001:2022, Annex A, control A.8.23.1

* PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 21

Q69. Why should the security testing processes be defined and implemented in the development life cycle?

* To protect the production environment and data from compromise by development and test activities
* To validate if information security requirements are met when applications are deployed to the production environment
* To Identify organizational assets and define appropriate protection responsibilities

Q70. Based on scenario 5. Socket Inc. decided to assign users lo a separate network when accessing cloud storage tiles. What does this ensure?

* Belter security when using cloud storage files
* Elimination of risks related to the use of cloud storage services
* Creation of backup copies of files

Q71. Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.

Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:

A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department The approved action plan was implemented and all actions described in the plan were documented.

Based on scenario 9. did the ISMS project manager complete the corrective action process appropriately?
* Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions
* No, the corrective action did not address the root cause of the nonconformity
* No, the corrective action process should also include the review of the implementation of the selected actions
According to ISO/IEC 27001:2022, the corrective action process consists of the following steps12:

* Reacting to the nonconformity and, as applicable, taking action to control and correct it and deal with the consequences

* Evaluating the need for action to eliminate the root cause(s) of the nonconformity, in order that it does not recur or occur elsewhere

* Implementing the action needed

* Reviewing the effectiveness of the corrective action taken

* Making changes to the information security management system, if necessary In scenario 9, the ISMS project manager did not complete the last step of reviewing the effectiveness of the corrective action taken. This step is important to verify that the corrective action has achieved the intended results and that no adverse effects have been introduced. The review can be done by using various methods, such as audits,tests, inspections, or performance indicators3. Therefore, the ISMS project manager did not complete the corrective action process appropriately.

References:

1: ISO/IEC 27001:2022, clause 10.2 2: Procedure for Corrective Action [ISO 27001 templates] 3: ISO 27001 Clause 10.2 Nonconformity and corrective action

Q72. How can Invalid Electric’s ensure that Us employees are prepared for the audit?
* By conducting practice Interviews with the employees
* By allowing the employees to observe the technologies used
* By showing the employees the internal audit reports so they can anticipate the questions asked by the auditor

Q73. Which of the following is the information security committee responsible for?
* Ensure smooth running of the ISMS
* Set annual objectives and the ISMS strategy
* Treat the nonconformities

Q74. Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management

system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company’s best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security- related controls. The session included topics such as Skyver’s information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver’s information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on scenario 6. Lisa found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. What does this indicate?

* Lisa did not take actions to acquire the necessary competence
* The effectiveness of the training and awareness session was not evaluated
* Skyver did not determine differing team needs in accordance to the activities they perform and the intended results

According to the ISO/IEC 27001:2022 Lead Implementer Training Course Guide1, one of the requirements of ISO/IEC 27001 is to ensure that all persons doing work under the organization’s control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. To achieve this, the organization should determine the necessary competence of persons doing work under its control that affects its information security performance, provide training or take other actions to acquire the necessary competence, evaluate the effectiveness of the actions taken, and retain appropriate documented information as evidence of competence. The organization should also determine differing team needsin accordance to the activities they perform and the intended results, and provide appropriate training and awareness programs to meet those needs.

Therefore, the scenario indicates that Skyver did not determine differing team needs in accordance to the activities they perform and the intended results, since Lisa, who works in the HR Department, found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. This implies that the session was not tailored to the specific needs and roles of the HR personnel, and that the information security expert did not consider the level of technical knowledge and skills required for them to perform their work effectively and securely.

References:

* ISO/IEC 27001:2022 Lead Implementer Training Course Guide1

* ISO/IEC 27001:2022 Lead Implementer Info Kit2

Q75. Which of the following practices Indicates that Company A has Implemented clock synchronization?

* Logs that record activities and other relevant events are stored and analyzed
* Information processing systems are coordinated according to an approved time source
* Suspected information security events are reported in a timely manner through an appropriate channel