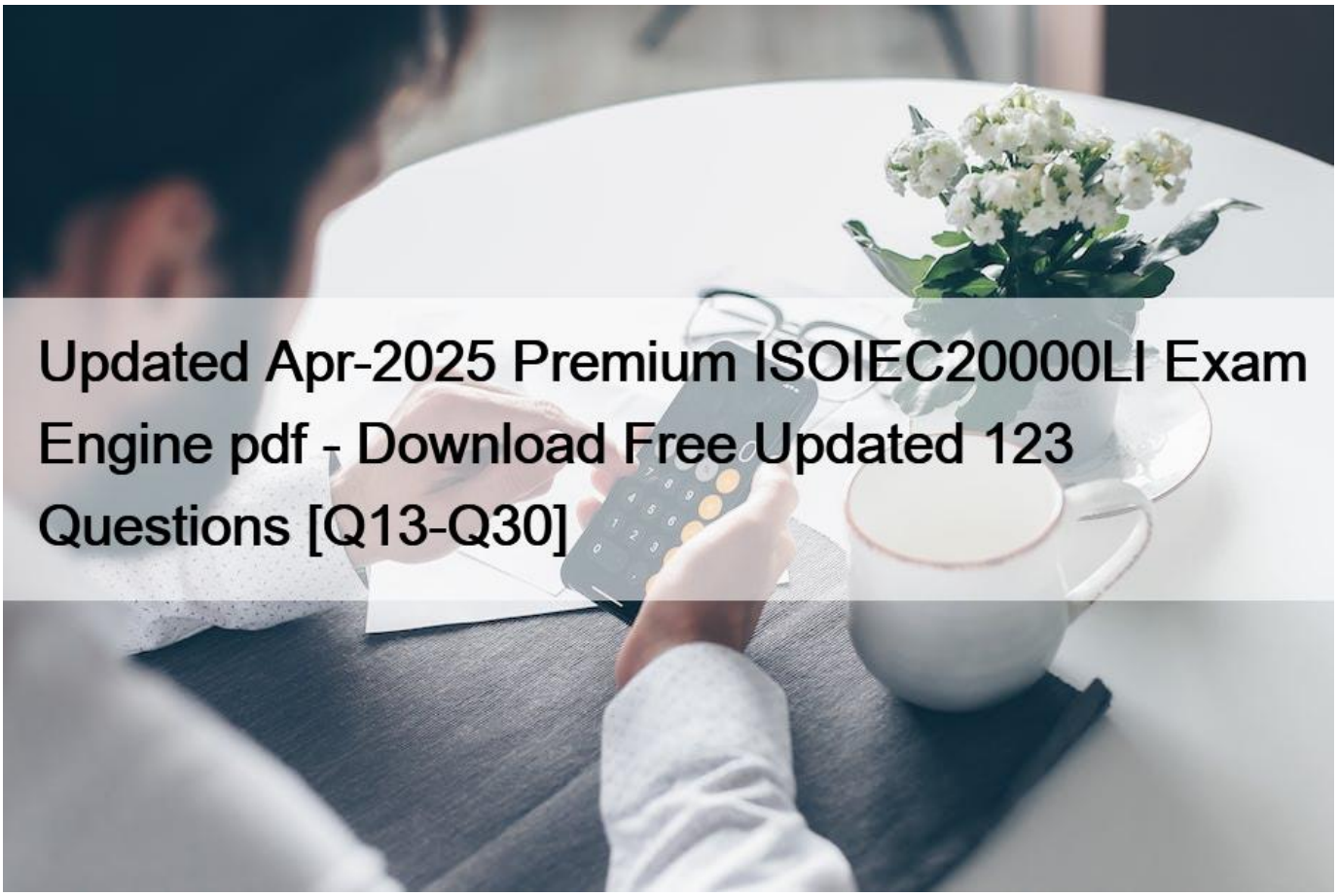
Updated Apr-2025 Premium ISOIEC20000LI Exam Engine pdf - Download Free Updated 123 Questions [Q13-Q30



Updated Apr-2025 Premium ISOIEC20000LI Exam Engine pdf - Download Free Updated 123 Questions
Authentic ISOIEC20000LI Dumps With 100% Passing Rate Practice Tests Dumps

QUESTION 13

Which of the following statements regarding information security risk is NOT correct?
* Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats
* Information security risk cannot be accepted without being treated or during the process of risk treatment
* Information security risk can be expressed as the effect of uncertainty on information security objectives
According to ISO/IEC 27001:2022, information security risk can be accepted as one of the four possible options for risk treatment, along with avoiding, modifying, or sharing the risk12. Risk acceptance means that the organization decides to tolerate the level of risk without taking any further action to reduce it3. Risk acceptance can be done before, during, or after the risk treatment process, depending on the organization’s risk criteria and the residual risk level4.

References: 1: ISO 27001 Risk Assessments | IT Governance UK 2: ISO 27001 Risk Assessment: 7 Step Guide – IT Governance UK Blog 3: ISO 27001 Clause 6.1.2 Information security risk assessment process 4:

ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide – Advisera

QUESTION 14

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company’s departments within the ISMS scope.

The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top management determinedthat this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze’s top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze’s top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.

Based on scenario 5. which committee should Operaze create to ensure the smooth running of the ISMS?
* Information security committee
* Management committee
* Operational committee

According to ISO/IEC 27001:2022, clause 5.1, the top management of an organization is responsible for ensuring the leadership and commitment for the ISMS. However, the top management may delegate some of its responsibilities to an information security committee, which is a group of people who oversee the ISMS and provide guidance and support for its implementation and operation. The information security committee may include representatives from different departments, functions, or levels of the organization, as well as external experts or consultants. The information security committee may have various roles and responsibilities, such as:

* Establishing the information security policy and objectives

* Approving the risk assessment and risk treatment methodology and criteria

* Reviewing and approving the risk assessment and risk treatment results and plans

* Monitoring and evaluating the performance and effectiveness of the ISMS

* Reviewing and approving the internal and external audit plans and reports

* Initiating and approving corrective and preventive actions

* Communicating and promoting the ISMS to all interested parties

* Ensuring the alignment of the ISMS with the strategic direction and objectives of the organization

* Ensuring the availability of resources and competencies for the ISMS

* Ensuring the continual improvement of the ISMS

Therefore, in scenario 5, Operaze should create an information security committee to ensure the smooth running of the ISMS, as this committee would provide the necessary leadership, guidance, and support for the ISMS implementation and operation.

References: ISO/IEC 27001:2022, clause 5.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 9.

QUESTION 15

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, what type of assets were identified during risk assessment?
* Supporting assets
* Primary assets
* Business assets
According to ISO/IEC 27005:2021, there are three types of assets in information security risk management:

primary assets, supporting assets, and business assets. Primary assets are the information and business processes that support the organization’s objectives and operations. Supporting assets are the resources that enable the primary assets to function, such as hardware, software, networks, people, facilities, etc. Business assets are the outcomes or benefits that the organization expects from the primary assets, such as reputation, market share, customer satisfaction, etc. (Must be taken from ISO/IEC 27001 : 2022 Lead Implementer resources) In scenario 4, the assets that were identified during risk assessment are hardware, software, and networks, which are examples of supporting assets. These assets are necessary for the information and business processes of TradeB to operate, but they are not the main focus of the risk assessment. The risk assessment should also consider the primary assets and the business assets, as well as the threats and vulnerabilities that affect them, and the potential impacts and likelihood of information

security incidents.

References: ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, specifically:

* ISO/IEC 27001:2022, clause 6.1.2 Information security risk assessment

* ISO/IEC 27005:2021, clause 5.2 Asset identification and valuation

* PECB ISO/IEC 27001 Lead Implementer Course, Module 6: Risk Management

QUESTION 16

Why is the power/interest matrix used for?
* Define the information security and physical boundaries
* identify business requirements
* Determine and manage interested parties

QUESTION 17

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

QUESTION 18

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

QUESTION 19

Which tool is used to identify, analyze, and manage interested parties?
* The probability/impact matrix
* The power/interest matrix
* The likelihood/severity matrix

The power/interest matrix is a tool that can be used to identify, analyze, and manage interested parties according to ISO/IEC 27001:2022. The power/interest matrix is a two-dimensional diagram that plots the level of power and interest of each interested party in relation to the organization’s information security objectives. The power/interest matrix can help the organization to prioritize the interested parties, understand their expectations and needs, and develop appropriate communication and engagement strategies. The power

/interest matrix can also help the organization to identify potential risks and opportunities related to the interested parties.

References: ISO/IEC 27001:2022, clause 4.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 12.

QUESTION 20

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 Based on scenario 8. does SunDee comply with ISO/IEC 27001 requirements regarding the monitoring and measurement process?
* Yes. because the standard does not Indicate when the monitoring and measurement phase should be performed
* Yes, because the standard requires that the monitoring and measurement phase be conducted every two years
* No, because even though the standard does not imply when such a process should be performed, the company must have a monitoring and measurement process in place

According to ISO/IEC 27001:2022, clause 9.1, the organization shall determine:

* what needs to be monitored and measured, including information security processes and controls, as well as information security performance and the effectiveness of the ISMS;

* the methods for monitoring, measurement, analysis and evaluation, to ensure valid and reliable results;

* when the monitoring and measurement shall be performed;

* who shall monitor and measure;

* who shall analyze and evaluate the monitoring and measurement results; and

* how the results shall be communicated and used for decision making and improvement.

The organization shall retain documented information as evidence of the monitoring and measurement results.

The standard does not prescribe a specific frequency or method for monitoring and measurement, but it requires the organization to have a defined and documented process that is appropriate to its context, objectives, risks, and opportunities. The organization should also ensure that the monitoring and measurement results are analyzed and evaluated to determine the performance and effectiveness of the ISMS, and to identify any nonconformities, gaps, or improvement opportunities.

In the scenario, SunDee did not comply with these requirements, as it did not have a monitoring and measurement process in place, and did not monitor or measure the performance and effectiveness of its ISMS regularly. It also did not use valid and reliable methods, or communicate and use the results for improvement.

Therefore, SunDee’s negligence of ISMS performance evaluation was a major nonconformity, as Tessa correctly identified.

References: ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, clause 9.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 9: Monitoring, Measurement, Analysis and Evaluation.

QUESTION 21

Kyte. a company that has an online shopping website, has added a Q&A section to its website; however, its Customer Service Department almost never provides answers to users’ questions. Which principle of an effective communication strategy has Kyte not followed?
* Clarity
* Appropriateness
* Responsiveness

In the scenario described, Kyte’s failure to provide answers to users’ questions in the Q&A section of its online shopping website demonstrates a lack of responsiveness. Responsiveness is a key principle of an effective communication strategy, especially in customer service. It involves timely and appropriate reactions to inquiries and feedback, ensuring that customers’ concerns and queries are addressed promptly. By not responding, Kyte is not adhering to this principle, potentially affecting customer satisfaction and trust.

QUESTION 22

Org Y. a well-known bank, uses an online banking platform that enables clients to easily and securely access their bank accounts.

To log in. clients are required to enter the one-time authorization code sent to their smartphone.

What can be concluded from this scenario?
* Org Y has implemented an integrity control that avoids the involuntary corruption of data
* Org Y has incorrectly implemented a security control that could become a vulnerability
* Org Y has implemented a security control that ensures the confidentiality of information

QUESTION 23

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 NetworkFuse should_____to ensure that employees are prepared for the audit. Refer to scenario 10.
* Conduct practice interviews
* Observe the technologies used
* Select a certification body that provides combined audits

One of the ways to prepare employees for an ISO/IEC 27001 audit is to conduct practice interviews with them. This can help them to familiarize themselves with the audit process, the types of questions they might be asked, and the evidence they need to provide to demonstrate compliance with the standard. Practice interviews can also help employees to identify any gaps or weaknesses in their knowledge or performance, and to address them before the actual audit. Practice interviews can be conducted by internal auditors, managers, or consultants, and should cover the relevant scope, objectives, and criteria of the audit. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113) References:

* PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113

* PECB ISO/IEC 27001 Lead Implementer Info Kit, page 10

* 5 Step Plan: How to Prepare for an ISO 27001 Certification Audit

QUESTION 24

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 relevantagreements, 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 scenario 3. which information security control of Annex A of ISO/IEC 27001 did Socket Inc.

implement by establishing a new system to maintain, collect, and analyze information related to information security threats?
* Annex A 5.5 Contact with authorities
* Annex A 5 7 Threat Intelligence
* Annex A 5.13 Labeling of information

Annex A 5.7 Threat Intelligence is a new control in ISO 27001:2022 that aims to provide the organisation with relevant information regarding the threats and vulnerabilities of its information systems and the potential impacts of information security incidents. By establishing a new system to maintain, collect, and analyze information related to information security threats, Socket Inc. implemented this control and improved its ability to prevent, detect, and respond to information security incidents.

References:

* ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements, Annex A 5.7 Threat Intelligence

* ISO/IEC 27002:2022 Information technology – Security techniques – Information security, cybersecurity and privacy protection controls, Clause 5.7 Threat Intelligence

* PECB ISO/IEC 27001:2022 Lead Implementer Course, Module 6: Implementation of Information Security Controls Based on ISO/IEC 27002:2022, Slide 18: A.5.7 Threat Intelligence

QUESTION 25

Based on scenario 5. Socket Inc. decided to use cloud storage to store customers’ personal data considering that the identified risks have low likelihood and high impact, is this acceptable?
* Yes. because the calculated level of risk is below the acceptable threshold
* No, because the impact of the identified risks is considered in he high
* No. because the identified risks fall above the risk acceptable criteria threshold

QUESTION 26

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

QUESTION 27

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 According to scenario 10, NetworkFuse requested from the certification body to review all the documentation only on-site. Is this acceptable?
* Yes, the auditee may request that the review of the documentation takes place on-site
* Yes, only if a confidentiality agreement is formerly signed by the audit team
* No, the certification body decides whether the documentation review takes place on-site or off-site
According to the ISO/IEC 27001:2022 standard, the certification body is responsible for planning and conducting the audit, including the review of the documented information. The certification body may decide to review the documentation on-site or off-site, depending on the audit objectives, scope, criteria, and risks.

The auditee may not impose any restrictions on the access to the documentation, unless there are valid reasons for confidentiality or security. However, such restrictions should be agreed upon before the audit and should not compromise the effectiveness and impartiality of the audit.

References:

* ISO/IEC 27001:2022, clause 9.2.2

* ISO/IEC 27006:2021, clause 7.1.4

QUESTION 28

Which statement is an example of risk retention?
* An organization has decided to release the software even though some minor bugs have not been fixed yet
* An organization has implemented a data loss protection software
* An organization terminates work in the construction site during a severe storm
According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, either because the bugs are not critical or because the cost of fixing them would outweigh the benefits.

References:

* ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment

* ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process

* 3, ISO 27001: Top risk treatment options and controls explained

QUESTION 29

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 the scenario above, answer the following question:

The decision to treat only risks that were classified as high indicates that Trade B has:
* Evaluated other risk categories based on risk treatment criteria
* Accepted other risk categories based on risk acceptance criteria
* Modified other risk categories based on risk evaluation criteria

According to ISO/IEC 27001 : 2022, risk acceptance criteria are the criteria used to decide whether a risk can be accepted or not1. Risk acceptance criteria are often based on a maximum level of acceptable risks, on cost- benefits considerations, or on consequences for the organization2. In the scenario, TradeB decided to treat only the high risk category, which implies that

QUESTION 30

Employees of the Finance Department did not fully understand the awareness sessions. What should TradeB do to avoid similar situations in the future? Refer to scenario 6.
* Extend the duration of the training and awareness session
* Adjust awareness sessions to the target audience based on the activities they perform within the company
* Consider self-studies as the type of activities needed to address the competence gaps