LEAD-IMPLEMENTER Q&As

PECB Certified ISO/IEC 27001 Lead Implementer

Pass PECB LEAD-IMPLEMENTER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/lead-implementer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by PECB Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 j^ombined 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?

A. Yes, the auditee may request that the review of the documentation takes place on-site

B. Yes, only if a confidentiality agreement is formerly signed by the audit team

C. No, the certification body decides whether the documentation review takes place on-site or off-site

Correct Answer: C

Explanation: 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 2

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. when should Colin deliver the next training and awareness session?

A. After he ensures that the group of employees targeted have satisfied the organization\\'s needs

B. After he conducts a competence needs analysis and records the competence related issues

C. After he determines the employees\\' availability and motivation

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 7.2.3, the organization shall conduct a competence needs analysis to determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization shall also evaluate the effectiveness of the actions taken to acquire the necessary competence and retain appropriate documented information as evidence of competence. Therefore, Colin should deliver the next training and awareness session after he conducts a competence needs analysis and records the competence related issues, such as the level of understanding, the gaps in knowledge, and the feedback from the participants. References: ISO/IEC 27001:2022, clause 7.2.3; PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 8.

QUESTION 3

What is the main purpose of Annex A 7.1 Physical security perimeters of ISO/IEC 27001?

A. To prevent unauthorized physical access, damage, and interference to the organization\\'s information and other associated assets

B. To maintain the confidentiality of information that is accessible by personnel or external parties

C. To ensure access to information and other associated assets is defined and authorized

Correct Answer: A

Explanation: Annex A 7.1 of ISO/IEC 27001 : 2022 is a control that requires an organization to define and implement security perimeters and use them to protect areas that contain information and other associated assets. Information and information security assets can include data, infrastructure, software, hardware, and personnel. The main purpose of this control is to prevent unauthorized physical access, damage, and interference to these assets, which could compromise the confidentiality, integrity, and availability of the information. Physical security perimeters can include fences, walls, gates, locks, alarms, cameras, and other barriers or devices that restrict or monitor access to the facility or area. The organization should also consider the environmental and fire protection of the assets, as well as the disposal of any waste or media that could contain sensitive information. References: ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Section 5.3.1.7, page 101 ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 17 ISO/IEC 27002 : 2022, Control 7.1 ?Physical Security Perimeters123

QUESTION 4

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?

A. Yes. because the standard does not Indicate when the monitoring and measurement phase should be performed

B. Yes, because the standard requires that the monitoring and measurement phase be conducted every two years

C. 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

Correct Answer: C

Explanation: 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 5

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 determined that 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?

A. Information security committee

B. Management committee

C. Operational committee

Correct Answer: A

Explanation: 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.