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

QUESTION 1

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 2

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?

A. Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions

B. No, the corrective action did not address the root cause of the nonconformity

C. No, the corrective action process should also include the review of the implementation of the selected actions

Correct Answer: C

Explanation: 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 3

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.

QUESTION 4

Which of the following statements regarding information security risk is NOT correct?

A. Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats

B. Information security risk cannot be accepted without being treated or during the process of risk treatment

C. Information security risk can be expressed as the effect of uncertainty on information security objectives

Correct Answer: B

Explanation: 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 and Risk Treatment: The Complete Guide - Advisera

QUESTION 5

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 this scenario, answer the following question:

OpenTech has decided to establish a new version of its access control policy. What should the company do when such changes occur?

A. Identify the change factors to be monitored

B. Update the information security objectives

C. Include the changes in the scope

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 6.2, the organization shall establish information security objectives at relevant functions and levels. The information security objectives shall be consistent with the information security policy and relevant to the information security risks. The organization shall update the information security objectives as changes occur. Therefore, when OpenTech decides to establish a new version of its access control policy, it should update its information security objectives accordingly to reflect the changes and ensure alignment with the policy. References: ISO/IEC 27001:2022, clause 6.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 10, slide 8.