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 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.

What is the next step that Operaze\\'s ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.

A. Implement the information security policy

B. Obtain top management\\'s approval for the information security policy

C. Communicate the information security policy to all employees

Correct Answer: B

Explanation: According to ISO/IEC 27001 : 2022 Lead Implementer, the information security policy is a high-level document that defines the organization\\'s objectives, principles, and commitments regarding information security. The policy should be aligned with the organization\\'s strategic direction and context, and should provide a framework for setting information security objectives and establishing the ISMS. The policy should also be approved by top management, who are ultimately responsible for the ISMS and its performance. Therefore, after drafting the information security policy, the next step that Operaze\\'s ISMS implementation team should take is to obtain top management\\'s approval for the policy. This will ensure that the policy is consistent with the organization\\'s vision and values, and that it has the necessary support and resources for its implementation and maintenance. References: ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 5.2 Policy ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 12, Information security policy

QUESTION 2

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

Based on the scenario above, answer the following question:

Does NetworkFuse fulfill the prerequisites for a certification audit?

A. Yes, because the certification body has been selected

B. Yes, because internal audits and management reviews have been performed

C. Yes, because the ISMS must be operational for at least one year prior to the certification audit

Correct Answer: B

Explanation: According to ISO/IEC 27006:2015, the prerequisites for a certification audit are:

The ISMS must be operational for a period of time that is sufficient to demonstrate its effectiveness and performance.

The organization must have conducted at least one internal audit and one management review of the ISMS prior to the certification audit. The organization must provide the certification body with access to all the relevant documented

information, records, personnel, and facilities related to the ISMS. In the scenario, NetworkFuse has fulfilled these prerequisites, as it has had an operational ISMS for approximately two years, and it has performed internal audits and

management reviews. Therefore, the correct answer is B.

References: ISO/IEC 27006:2015, clauses 9.1.1, 9.1.2, and 9.2.1.

QUESTION 3

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

How does SunDee\\'s negligence affect the ISMS certificate? Refer to scenario 8.

A. SunDee will renew the ISMS certificate, because it has conducted an Internal audit to evaluate the ISMS effectiveness

B. SunDee might not be able to renew the ISMS certificate, because it has not conducted management reviews at planned intervals

C. SunDee might not be able to renew the ISMS certificate, because the internal audit lasted longer than planned

Correct Answer: B

Explanation: According to ISO/IEC 27001:2013, clause 9.3, the top management of an organization must review the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review must consider the status of actions from previous management reviews, changes in external and internal issues, the performance and effectiveness of the ISMS, feedback from interested parties, results of risk assessment and treatment, and opportunities for continual improvement. The management review must also result in decisions and actions related to the ISMS policy and objectives, resources, risks and opportunities, and improvement. The management review is a critical process that demonstrates the commitment and involvement of the top management in the ISMS and its alignment with the strategic direction of the organization. The management review also provides input for the internal audit and the certification audit. SunDee has neglected to conduct management reviews regularly, which means that it has not fulfilled the requirement of clause 9.3. This is a major nonconformity that could jeopardize the renewal of the ISMS certificate. The certification body will verify whether SunDee has conducted management reviews and whether they have been effective and documented. If SunDee cannot provide evidence of management reviews, it will have to take corrective actions and undergo a follow-up audit before the certificate can be renewed. Alternatively, the certification body may decide to suspend or withdraw the certificate if SunDee fails to address the nonconformity within a specified time frame. References: ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements, clause 9.3 PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001 PECB, ISO/IEC 27001 Lead Implementer Exam Preparation Guide, Section 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001

QUESTION 4

An organization uses Platform as a Services (PaaS) to host its cloud-based services As such, the cloud provider manages most off the services to the organization. However, the organization still manages_____

A. Operating system and visualization

B. Servers and storage

C. Application and data

Correct Answer: C

QUESTION 5

An employee of the organization accidentally deleted customers\\' data stored in the database. What is the impact of

this action?

A. Information is not accessible when required

B. Information is modified in transit

C. Information is not available to only authorized users

Correct Answer: A

Explanation: According to ISO/IEC 27001:2022, availability is one of the three principles of information security, along with confidentiality and integrity1. Availability means that information is accessible and usable by authorized persons

whenever it is needed2. If an employee of the organization accidentally deleted customers\\' data stored in the database, this would affect the availability of the information, as it would not be accessible when required by the authorized persons,

such as the customers themselves, the organization\\'s staff, or other stakeholders. This could result in loss of trust, reputation, or business opportunities for the organization, as well as dissatisfaction or inconvenience for the customers.

References:

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements What is ISO 27001? A detailed and straightforward guide - Advisera