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

An organization has justified the exclusion of control 5.18 Access rights of ISO/IEC 27001 in the Statement of Applicability (SoA) as follows: "An access control reader is already installed at the main entrance of the building." Which statement is correct\\'

A. The justification for the exclusion of a control is not required to be included in the SoA

B. The justification is not acceptable, because it does not reflect the purpose of control 5.18

C. The justification is not acceptable because it does not indicate that it has been selected based on the risk assessment results

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 6.1.3, the Statement of Applicability (SoA) is a document that identifies the controls that are applicable to the organization\\'s ISMS and explains why they are selected or not. The SoA is based on the results of the risk assessment and risk treatment, which are the previous steps in the risk management process. Therefore, the justification for the exclusion of a control should be based on the risk assessment results and the risk treatment plan, and should reflect the purpose and objective of the control. Control 5.18 of ISO/IEC 27001:2022 is about access rights to information and other associated assets, which should be provisioned, reviewed, modified and removed in accordance with the organization\\'s topic-specific policy on and rules for access control. The purpose of this control is to prevent unauthorized access to, modification of, and destruction of information assets. Therefore, the justification for the exclusion of this control should explain why the organization does not need to implement this control to protect its information assets from unauthorized access. The justification given by the organization in the question is not acceptable, because it does not reflect the purpose of control 5.18. An access control reader at the main entrance of the building is a physical security measure, which is related to control 5.15 of ISO/IEC 27001:2022, not control 5.18. Control 5.18 is about logical access rights to information systems and services, which are not addressed by the access control reader. Therefore, the organization should either provide a valid justification for the exclusion of control 5.18, or include it in the SoA and implement it according to the risk assessment and risk treatment results. References: ISO/IEC 27001:2022, clause 6.1.3, control 5.18; PECB ISO/IEC 27001 Lead Implementer Course, Module 5, slide 18, Module 6, slide 10.

QUESTION 2

An organization has implemented a control that enables the company to manage storage media through their life cycle of use. acquisition, transportation and disposal. Which control category does this control belong to?

A. Organizational

B. Physical

C. Technological

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, the control that enables the organization to manage storage media through their life cycle of use, acquisition, transportation and disposal belongs to the category of physical and environmental security. This category covers the controls that prevent unauthorized physical access, damage and interference to the organization\\'s information and information processing facilities. The specific control objective for this control is A.11.2.7 Secure disposal or reuse of equipment1, which states that "equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse."2 References: ISO/IEC 27001:2022, Annex A ISO/IEC 27002:2022, clause 11.2.7

QUESTION 3

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 4

An organization documented each security control that it Implemented by describing their functions in detail. Is this compliant with ISO/IEC 27001?

A. No, the standard requires to document only the operation of processes and controls, so no description of each security control is needed

B. No, because the documented information should have a strict format, including the date, version number and author identification

C. Yes, but documenting each security control and not the process in general will make it difficult to review the documented information

Correct Answer: C

Explanation: According to ISO/IEC 27001:2022, clause 7.5, an organization is required to maintain documented information to support the operation of its processes and to have confidence that the processes are being carried out as planned. This includes documenting the information security policy, the scope of the ISMS, the risk assessment and treatment methodology, the statement of applicability, the risk treatment plan, the information security objectives, and the results of monitoring, measurement, analysis, evaluation, internal audit, and management review. However, the standard does not specify the level of detail or the format of the documented information, as long as it is suitable for the organization\\'s needs and context. Therefore, documenting each security control that is implemented by describing their functions in detail is not a violation of the standard, but it may not be the most efficient or effective way to document the ISMS. Documenting each security control separately may make it harder to review, update, and communicate the documented information, and may also create unnecessary duplication or inconsistency. A better approach would be to document the processes and activities that involve the use of security controls, and to reference the relevant controls from Annex A or other sources. This way, the documented information would be more aligned with the process approach and the Plan-DoCheck-Act cycle that the standard promotes. References: ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements, clauses 4.3, 5.2, 6.1, 6.2, 7.5, 8.2, 8.3, 9.1, 9.2, 9.3, and Annex A ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

QUESTION 5

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.

Latest LEAD-IMPLEMENTER Dumps | LEAD-IMPLEMENTER VCE Dumps | LEAD-IMPLEMENTER Study Guide