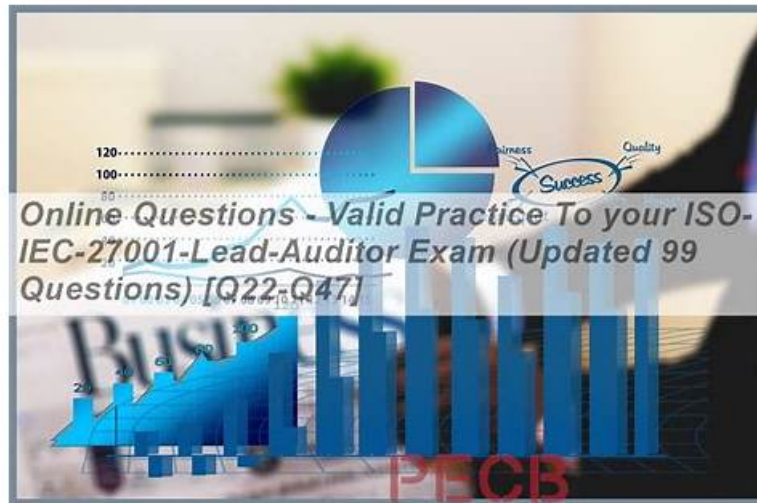


New ISO-IEC-27001-Lead-Auditor Exam Review & ISO-IEC-27001-Lead-Auditor Reliable Test Cram



BTW, DOWNLOAD part of TestPDF ISO-IEC-27001-Lead-Auditor dumps from Cloud Storage: <https://drive.google.com/open?id=1MExUHZoC1kWc4H95NaZkNUOcT2yo6g8b>

The high quality and high efficiency of our ISO-IEC-27001-Lead-Auditor exam materials has helped many people pass exams quickly. And we can proudly claim that if you study with our ISO-IEC-27001-Lead-Auditor study questions for 20 to 30 hours, then you can confidently pass the exam for sure. After our worthy customers get a ISO-IEC-27001-Lead-Auditor certificate, they now have more job opportunities. The current situation is very serious. Selecting ISO-IEC-27001-Lead-Auditor training guide is your best decision.

You can use this PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) practice exam software to test and enhance your PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam preparation. Your practice will be made easier by having the option to customize the PECB in ISO-IEC-27001-Lead-Auditor exam dumps. Only Windows-based computers can run this PECB ISO-IEC-27001-Lead-Auditor Exam simulation software. The fact that it runs without an active internet connection is an incredible comfort for users who don't have access to the internet all the time.

>> New ISO-IEC-27001-Lead-Auditor Exam Review <<

Free PDF PECB - ISO-IEC-27001-Lead-Auditor –Reliable New Exam Review

The PECB ISO-IEC-27001-Lead-Auditor certificate stands out among the numerous certificates because its practicability and role to improve the clients stocks of knowledge and practical ability. Owning a test PECB Certified ISO/IEC 27001 Lead Auditor exam ISO-IEC-27001-Lead-Auditor certificate equals owning a weighty calling card when the clients find jobs and the proof that the clients are the competent people.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q257-Q262):

NEW QUESTION # 257

Scenario 3: Rebuildy is a construction company located in Bangkok.. Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below

- * Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.
- * Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.
- * All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

* The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

* Information security roles and responsibilities have been clearly stated in every employee's job description.

* Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member Electra, a key client of Rebuildy, who also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001. The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

* An instance of improper user access control settings was detected within the company's financial reporting system.

* A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings.

The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Based on the scenario above, answer the following question:

Which action described in Scenario 3 indicates that the audit team leader violated the independence principle?

- A. The audit team leader revealed confidential information about Rebuildy to the former employee
- B. The audit team included the former employee's evidence in the audit report without revealing the source
- **C. The audit team leader sent a favorable report after discussing the audit conclusions with the top management**

Answer: C

Explanation:

Comprehensive and Detailed In-Depth

A . Correct Answer:

Independence is compromised when an auditor alters audit findings under pressure.

The audit team leader misrepresented compliance, violating ISO 19011's principles of objectivity and integrity.

B . Incorrect:

Including anonymous evidence in an audit report is acceptable as long as it is verified.

C . Incorrect:

While revealing confidential information would be unethical, it was not mentioned in the scenario.

Relevant Standard Reference:

NEW QUESTION # 258

The scope of an organization certified against ISO/IEC 27001 states that they provide editing and web hosting services. However, due to some changes in the organization, the technical support related to the web hosting services has been outsourced. Should a change in the scope be initiated in this case?

- A. No, because the organization is already certified for its editing and web hosting services
- B. No, because the change does not require implementation of new security controls
- **C. Yes, because any change in the external environment initiates a change in the scope**

Answer: C

Explanation:

Yes, a change in the scope should be initiated because outsourcing a significant part of the service, such as technical support related to web hosting, could impact the risk landscape and the controls needed to manage those risks. This change affects the external environment and how the ISMS operates, necessitating a scope review and possible adjustment.

NEW QUESTION # 259

Please match the roles to the following descriptions:

Answer:

Explanation:

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable test from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Reference:

[ISO 19011:2022 Guidelines for auditing management systems]

[ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements]

NEW QUESTION # 260

You are the audit team leader conducting a third-party audit of an online insurance organisation. During Stage 1, you found that the organisation took a very cautious risk approach and included all the information security controls in ISO/IEC 27001:2022 Appendix A in their Statement of Applicability.

During the Stage 2 audit, your audit team found that there was no evidence of the implementation of the three controls (5.3 Segregation of duties, 6.1 Screening, 7.12 Cabling security) shown in the extract from the Statement of Applicability. No risk treatment plan was found.

Select three options for the actions you would expect the auditee to take in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:2022.

- A. Revisit the risk assessment process relating to the three controls.
- B. Revise the relevant content in the Statement of Applicability to justify their exclusion.
- C. Undertake a survey of customers to find out if the controls are needed by them.
- D. Remove the three controls from the Statement of Applicability.
- E. Allocate responsibility for producing evidence to prove to auditors that the controls are implemented.
- F. Compile plans for the periodic assessment of the risks associated with the controls.
- G. Incorporate written procedures for the controls into the organisation's Security Manual.
- H. Implement the appropriate risk treatment for each of the applicable controls.

Answer: A,B,H

Explanation:

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the auditee should take the following actions in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:20221:

Implement the appropriate risk treatment for each of the applicable controls, as this is the main requirement of clause 6.1.3.e and the objective of the risk treatment process2.

Revise the relevant content in the Statement of Applicability to justify their exclusion, as this is the expected output of the risk treatment process and the evidence of the risk-based decisions3.

Revisit the risk assessment process relating to the three controls, as this is the input for the risk treatment process and the source of identifying the risks and the controls4.

The other options are not correct because:

Allocating responsibility for producing evidence to prove to auditors that the controls are implemented is not a valid action, as the audit team already found that there was no evidence of the implementation of the three controls.

Compiling plans for the periodic assessment of the risks associated with the controls is not a valid action, as this is part of the risk monitoring and review process, not the risk treatment process5.

Incorporating written procedures for the controls into the organisation's Security Manual is not a valid action, as this is part of the documentation and operation of the ISMS, not the risk treatment process.

Removing the three controls from the Statement of Applicability is not a valid action, as this is not a sufficient justification for their exclusion and does not reflect the risk treatment process.

Undertaking a survey of customers to find out if the controls are needed by them is not a valid action, as this is not a relevant criterion for the risk assessment and treatment process, which should be based on the organisation's own context and objectives.

NEW QUESTION # 261

Select two options that describe an advantage of using a checklist.

- A. Ensuring relevant audit trails are followed
- B. Not varying from the checklist when necessary
- C. Using the same checklist for every audit without review
- D. Restricting interviews to nominated parties
- E. Reducing audit duration
- F. Ensuring the audit plan is implemented

Answer: A,F

Explanation:

A checklist is a tool that helps auditors to collect and verify information relevant to the audit objectives and scope. It can provide the following advantages:

* Ensuring relevant audit trails are followed: A checklist can help auditors to identify and trace the sources of evidence that support the conformity or nonconformity of the audited criteria. It can also help auditors to avoid missing or overlooking any important aspects of the audit.

* Ensuring the audit plan is implemented: A checklist can help auditors to follow and fulfil the audit plan,

* which describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. It can also help auditors to manage their time and resources effectively and efficiently.

The other options are not advantages of using a checklist, but rather:

* Using the same checklist for every audit without review: This is a disadvantage of using a checklist, as it can lead to a rigid and ineffective audit approach. A checklist should be tailored and adapted to each specific audit, taking into account the context, risks, and changes of the auditee and the audit criteria. A checklist should also be reviewed and updated periodically to ensure its validity and relevance.

* Restricting interviews to nominated parties: This is a disadvantage of using a checklist, as it can limit the scope and depth of the audit. A checklist should not prevent auditors from interviewing other relevant parties or sources of information that may provide valuable evidence or insights for the audit. A checklist should be used as a guide, not as a constraint.

* Reducing audit duration: This is not necessarily an advantage of using a checklist, as it depends on various factors, such as the complexity, size, and maturity of the auditee's ISMS, the availability and quality of evidence, the competence and experience of the auditors, and the level of cooperation and communication between the auditors and the auditee. A checklist may help reduce audit duration by improving efficiency and organization, but it may also increase audit duration by requiring more evidence or verification.

* Not varying from the checklist when necessary: This is a disadvantage of using a checklist, as it can result in a superficial or incomplete audit. A checklist should not prevent auditors from exploring or investigating any issues or concerns that arise during the audit, even if they are not included in the checklist. A checklist should be used as a support, not as a substitute.

References:

* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB

* ISO 19011:2018 Guidelines for auditing management systems [Section 6.2.2]

NEW QUESTION # 262

.....

The evergreen field of PECB is so attractive that it provides non-stop possibilities for the one who passes the PECB ISO-IEC-27001-Lead-Auditor exam. So, to be there on top of the PECB sector, earning the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) certification is essential. Because of using outdated ISO-IEC-27001-Lead-Auditor study material, many candidates don't get success in the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam and lose their resources.

ISO-IEC-27001-Lead-Auditor Reliable Test Cram: <https://www.testpdf.com/ISO-IEC-27001-Lead-Auditor-exam-braindumps.html>

PECB New ISO-IEC-27001-Lead-Auditor Exam Review The soft test engine can just be installed in personal computers, And you can get the according ISO-IEC-27001-Lead-Auditor certification as well, The web-based ISO-IEC-27001-Lead-Auditor practice exam can be taken via the internet from any browser like Firefox, Safari, Opera, MS Edge, Internet Explorer, and Chrome, The ISO-IEC-27001-Lead-Auditor certificate you have obtained can really prove your ability to work.

Preferring Internal Documentation, He has led both product development ISO-IEC-27001-Lead-Auditor and consulting organizations for multi-national organizations, The soft test engine can just be installed in personal computers.

PECB ISO-IEC-27001-Lead-Auditor Dumps [2026] - Try Free ISO-IEC-27001-Lead-Auditor Exam Questions Demo

And you can get the according ISO-IEC-27001-Lead-Auditor Certification as well, The web-based ISO-IEC-27001-Lead-Auditor practice exam can be taken via the internet from any browser like Firefox, Safari, Opera, MS Edge, Internet Explorer, and Chrome.

- [illegible]