2026 Valid ISO-IEC-27001-Lead-Auditor Test Simulator 100% Pass | Trustable PECB PECB Certified ISO/IEC 27001 Lead Auditor exam Test Questions Vce Pass for sure

DOWNLOAD the newest Test4Sure ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13chGFTeYHqD3_VfYyVrjJypkzfW_FyGr

The PECB is committed to making the PECB ISO-IEC-27001-Lead-Auditor certification exam journey simple, smart, and easiest. The mock PECB Certified ISO/IEC 27001 Lead Auditor exam exams that will give you real-time environment for PECB ISO-IEC-27001-Lead-Auditor exam preparation. To keep you updated with latest changes in the ISO-IEC-27001-Lead-Auditor Test Questions, we offer one-year free updates in the form of new questions according to the requirement of ISO-IEC-27001-Lead-Auditor real exam. Updated ISO-IEC-27001-Lead-Auditor PDF dumps ensure the accuracy of learning materials and guarantee success of in your first attempt.

The ISO/IEC 27001 standard is a globally recognized framework for managing and securing information assets. PECB Certified ISO/IEC 27001 Lead Auditor exam certification ensures that the candidate has a thorough understanding of the standard and can assess an organization's information security management system (ISMS) against it. The PECB ISO-IEC-27001-Lead-Auditor Exam covers all the necessary topics and skills required to plan, conduct, report, and follow up on an ISMS audit.

The PECB ISO-IEC-27001-Lead-Auditor Exam is based on the ISO/IEC 27001 standard, which is an internationally recognized framework for information security management. The standard provides a systematic approach to managing sensitive information so that it remains secure. By taking ISO-IEC-27001-Lead-Auditor exam, you will gain a thorough understanding of the standard and its requirements, enabling you to effectively audit an ISMS based on the standard.

>> Valid ISO-IEC-27001-Lead-Auditor Test Simulator <<

ISO-IEC-27001-Lead-Auditor Test Questions Vce | ISO-IEC-27001-Lead-Auditor Test Duration

Are you still staying up for the ISO-IEC-27001-Lead-Auditor exam day and night? If your answer is yes, then you may wish to try our ISO-IEC-27001-Lead-Auditor exam materials. We are professional not only on the content that contains the most accurate and useful information, but also on the after-sales services that provide the quickest and most efficient assistants. With our ISO-IEC-27001-Lead-Auditor practice torrent for 20 to 30 hours, we can claim that you are ready to take part in your ISO-IEC-27001-Lead-Auditor exam and will achieve your expected scores.

PECB ISO-IEC-27001-Lead-Auditor Certification Exam is a rigorous exam that requires candidates to demonstrate their knowledge and skills through a written exam and a practical audit. The written exam consists of multiple-choice questions and is designed to test the candidate's knowledge and understanding of the ISO 27001 standard and the auditing process. The practical audit is designed to test the candidate's ability to apply the principles and techniques learned during the training to a real-world scenario.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q88-Q93):

NEW QUESTION # 88
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?

- A. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
- B. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
- C. Verification should focus on whether any action undertaken taken has been undertaken efficiently
- D. Verification should focus on whether any action undertaken is complete
- E. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
- F. Verification should focus on whether any action undertaken has been undertaken effectively

Answer: D,F

Explanation:
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence.
The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12 Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12 Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1
2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION # 89
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?

- A. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement

- B. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
- C. Verification should focus on whether any action undertaken taken has been undertaken efficiently
- D. Verification should focus on whether any action undertaken is complete
- E. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
- F. Verification should focus on whether any action undertaken has been undertaken effectively

Answer: D,F

Explanation:
Explanation
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence.
The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12
* Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes,
* but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12
* Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1
2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION # 90
You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including mis-addressed labels and, in 15% of company cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).
You: Are items checked before being dispatched?
SH: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.
You: What action is taken when items are returned?
SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.

You raise a nonconformity. Referencing the scenario, which six of the following Appendix A controls would you expect the auditee to have implemented when you conduct the follow-up audit?

- A. 5.32 Intellectual property rights
- B. 5.13 Labelling of information
- C. 7.4 Physical security monitoring
- D. 6.3 Information security awareness, education, and training
- E. 6.4 Disciplinary process
- F. 5.3 Segregation of duties
- G. 8.12 Data leakage protection
- H. 5.11 Return of assets
- I. 7.10 Storage media
- J. 8.3 Information access restriction
- K. 5.6 Contact with special interest groups

Answer: B,C,D,G,I,J

Explanation:
Explanation
* B. 8.12 Data leakage protection. This is true because the auditee should have implemented measures to prevent unauthorized disclosure of sensitive information, such as personal data, medical records, or official documents, that are contained in the parcels. Data leakage protection could include encryption, authentication, access control, logging, and monitoring of data transfers12.
* D. 6.3 Information security awareness, education, and training. This is true because the auditee should have ensured that all employees and contractors involved in the shipping process are aware of the information security policies and procedures, and have received appropriate training on how to handle and protect the information assets in their custody. Information security awareness, education, and training could include induction programmes, periodic refreshers, awareness campaigns, e-learning modules, and feedback mechanisms13.
* E. 7.10 Storage media. This is true because the auditee should have implemented controls to protect the storage media that contain information assets from unauthorized access, misuse, theft, loss, or damage. Storage media could include paper documents, optical disks, magnetic tapes, flash drives, or hard disks14. Storage media controls could include physical locks, encryption, backup, disposal, or destruction14.
* F. 8.3 Information access restriction. This is true because the auditee should have implemented controls to restrict access to information assets based on the principle of least privilege and the need-to-know basis. Information access restriction could include identification, authentication, authorization, accountability, and auditability of users and systems that access information assets15.
* I. 7.4 Physical security monitoring. This is true because the auditee should have implemented controls to monitor the physical security of the premises where information assets are stored or processed. Physical security monitoring could include CCTV cameras, alarms, sensors, guards, or patrols16. Physical security monitoring could help detect and deter unauthorized physical access or intrusion attempts16.
* J. 5.13 Labelling of information. This is true because the auditee should have implemented controls to label information assets according to their classification level and handling instructions. Labelling of information could include markings, tags, stamps, stickers, or barcodes1 . Labelling of information could help identify and protect information assets from unauthorized disclosure or misuse1 .
References :=
* ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* ISO/IEC 27004:2022 Information technology - Security techniques - Information security management systems - Monitoring measurement analysis and evaluation
* ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management
* ISO/IEC 27006:2022 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
* [ISO/IEC 27007:2022 Information technology - Security techniques - Guidelines for information security management systems auditing]

NEW QUESTION # 91
Scenario 5: Cobt. an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organizations internal control mechanisms.

The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification Sarah, an experienced auditor, was assigned to the audit Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes Therefore, her initial focus was to gather information on how the company manages its information security risks Sarah contacted Cobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence Moreover, Cobt raised concerns about the audit schedule, stating that it does not properly reflect the recent changes the company made It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the scenario above, answer the following question:
Based on Scenario 5, Cobt stated that the audit schedule did not properly reflect the recent changes they made in the audit scope. What should Sarah do in this case?

- A. Change the audit schedule only if Cobt, Sarah, and the certification body agree on the changes in the audit scope
- B. Change the audit schedule as requested by Cobt as the scope should reflect the status and importance of the activities to be audited
- C. Continue the audit with the initial scope since Cobt can request a change in the audit scope only if there are recent changes in technologies in place

Answer: A

Explanation:
Comprehensive and Detailed In-Depth
C . Correct Answer: Changes to the audit scope must be approved by the auditee, the A . Incorrect: The audit schedule cannot be changed solely at Cobt's request-approval is required.
B . Incorrect: Audit scope is not limited to technological changes but includes organizational and procedural changes as well.
Relevant Standard Reference:
ISO 19011:2018 Clause 5.5.2 (Determining the Audit Scope and Schedule)

NEW QUESTION # 92
An audit team leader is planning a follow-up audit after the completion of a third-party surveillance audit earlier in the year. They have decided they will verify the nonconformities that require corrections before they move on to consider corrective actions. Based on the descriptions below, which four of the following are corrections for nonconformities identified at the surveillance?

- A. Data centre staff not carrying out backups in accordance with specified procedures were retrained
- B. Hard drive HD302 which had been colour-coded green (available for use) instead of red (to be destroyed) was removed from the system
- C. The organisation, having failed to maintain its Schedule of Applicability, re-allocated responsibility for its updating to the Technical Director
- D. Scheduled management reviews, having been missed, were prioritised by the General Manager for holding on a specific date twice each following year
- E. A signature missing from a client's contract for the supply of data services was added
- F. A software installation guide which had not been sent to the client along with their new system was posted out
- G. An incorrectly dated purchase order for a new network switch was rectified
- H. The documented process for product shipment, which did not reflect how this activity was conducted by the despatch team, was re-written and the team trained accordingly

Answer: B,E,F,G

Explanation:
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, a correction is an action to eliminate a detected

nonconformity, such as rework, repair, or replacement1. The examples of A, B, C, and E are corrections because they fix the errors or defects that caused the nonconformities, such as a missing signature, a missing guide, a wrong date, or a wrong colour code. The other examples (D, F, G, and H) are not corrections, but corrective actions, because they address the root causes of the nonconformities, such as inadequate training, poor planning, ineffective documentation, or unclear responsibility2. References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 35, section 4.5.12: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 36, section 4.5.2.

NEW QUESTION # 93

.....