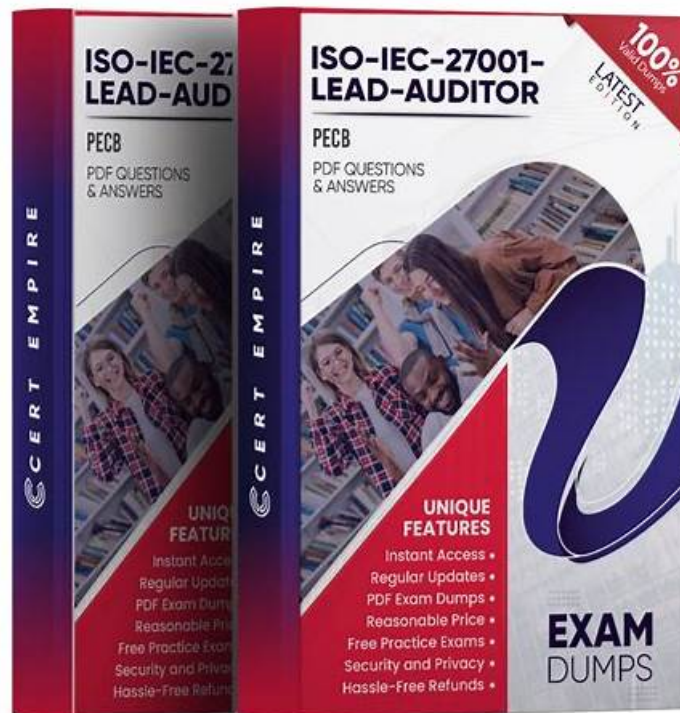


Exam ISO-IEC-27001-Lead-Auditor Guide - Valid ISO-IEC-27001-Lead-Auditor Exam Format



DOWNLOAD the newest TestPDF ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1A-j7hCjdR4NKpDfjRGvL6LfVIZAAALrq->

If you prepare well in advance, you'll be stress-free on the PECB Certified ISO/IEC 27001 Lead Auditor exam ISO-IEC-27001-Lead-Auditor exam day and thus perform well. Candidates can know where they stand by attempting the PECB ISO-IEC-27001-Lead-Auditor practice test. It can save you lots of time and money. The question on the PECB ISO-IEC-27001-Lead-Auditor Practice Test is quite similar to the PECB ISO-IEC-27001-Lead-Auditor questions that get asked on the ISO-IEC-27001-Lead-Auditor exam day.

PECB ISO-IEC-27001-Lead-Auditor Exam is ideal for individuals who work in the information security field, such as information security managers, IT managers, consultants, and auditors. PECB Certified ISO/IEC 27001 Lead Auditor exam certification provides a comprehensive understanding of the ISO/IEC 27001 standard and the auditing process, making it an essential credential for those who want to ensure that their organization's information assets are protected. PECB Certified ISO/IEC 27001 Lead Auditor exam certification also demonstrates to clients and stakeholders that the organization is committed to maintaining the highest standards of information security management.

PECB ISO-IEC-27001-Lead-Auditor certification exam tests the candidates on various aspects of information security management, including the planning and conducting of audits, the evaluation and reporting of audit findings, and the follow-up and monitoring of corrective actions. ISO-IEC-27001-Lead-Auditor Exam also covers topics such as risk management, information security controls, and the legal and regulatory framework for information security. PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam is intended for professionals who are responsible for ensuring the effectiveness of an organization's information security management system and its compliance with the ISO/IEC 27001 standard. Successful completion of the certification exam demonstrates that the candidate has the knowledge and skills necessary to lead an information security audit and provide guidance on the implementation and maintenance of an ISMS.

>> Exam ISO-IEC-27001-Lead-Auditor Guide <<

Valid ISO-IEC-27001-Lead-Auditor Exam Format - Reliable ISO-IEC-27001-Lead-Auditor Test Book

Your opportunity to survey the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam questions before buying it will relax your nerves. TestPDF proudly declares that it will not disappoint you in providing the best quality PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) study material. The guarantee to give you the money back according to terms and conditions is one of the remarkable facilities of the TestPDF.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q50-Q55):

NEW QUESTION # 50

You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.

You are currently in a large room that is subdivided into several smaller rooms, each of which has a numeric combination lock and swipe card reader on the door. You notice two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorised electrical repairs.

You go to reception and ask to see the door access record for the client's suite. This indicates only one card was swiped. You ask the receptionist and they reply, 'yes it's a common problem. We ask everyone to swipe their cards but with contractors especially, one tends to swipe and the rest simply 'tailgate' their way in' but we know who they are from the reception sign-in.

Based on the scenario above which one of the following actions would you now take?

- A. Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities
- B. Raise a nonconformity against control A.7.1 'security perimeters' as a secure area is not adequately protected
- C. Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV
- D. Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier
- E. Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined
- F. Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times

Answer: C

Explanation:

Explanation

The best action to take in this scenario is to determine whether any additional effective arrangements are in place to verify individual access to secure areas, such as CCTV. This action is consistent with the audit principle of evidence-based approach, which requires the auditor to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions¹. By verifying the existence and effectiveness of other security controls, the auditor can assess the extent and impact of the nonconformity observed, and determine the appropriate audit finding and recommendation.

The other options are not the best actions to take in this scenario, because they are either premature or inappropriate. For example:

*Option A is inappropriate, because it is not the auditor's role to suggest specific solutions or improvements to the auditee, but rather to report the audit findings and recommendations based on the audit criteria and objectives². A large sign in reception may not be an effective or feasible solution to address the issue of tailgating, and it may not reflect the root cause of the problem.

*Option C is premature, because it assumes that the control A.7.1 'security perimeters' is not adequately implemented, without verifying the existence and effectiveness of other security controls that may compensate for the observed nonconformity. The auditor should not jump to conclusions based on a single observation, but rather gather sufficient and appropriate audit evidence to support the audit finding³.

*Option D is premature, because it assumes that the control A.7.6 'working in secure areas' is not adequately implemented, without verifying the existence and effectiveness of other security controls that may compensate for the observed nonconformity. The auditor should not jump to conclusions based on a single observation, but rather gather sufficient and appropriate audit evidence to support the audit finding³.

*Option E is inappropriate, because it is not related to the observed nonconformity, which is about the access control to secure areas, not the information security requirements agreed upon with the supplier. The auditor should not raise a nonconformity based on irrelevant or incorrect audit criteria⁴.

*Option F is inappropriate, because it is not the auditor's role to suggest specific solutions or improvements to the auditee, but rather to report the audit findings and recommendations based on the audit criteria and objectives². Requiring contractors to be accompanied at all times when accessing secure facilities may not be an effective or feasible solution to address the issue of tailgating, and it may not reflect the root cause of the problem.

References: 1: ISO 19011:2018, 5.2; 2: ISO 19011:2018, 6.6; 3: ISO 19011:2018, 6.2; 4: ISO 19011:2018, 6.3; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018

NEW QUESTION # 51

You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.

You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.

To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.

Select three options for the audit evidence you need to find to verify the scope of the ISMS.

- A. The auditee has ISO 9001 certification
- B. The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment
- C. The auditee is considering the purchase of a healthcare monitoring app from an external software company
- **D. The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling**
- E. The auditee has identified the resident's needs and expectations on the facility and environmental safety
- **F. The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located**
- **G. The auditee has identified the resident's needs and expectations on how they should protect the resident's personal data**
- H. The auditee has identified the resident's needs and expectations on healthcare medical treatment services

Answer: D,F,G

Explanation:

Explanation

According to ISO 27001:2022 clause 4.3, the organisation shall determine the scope of the information security management system (ISMS) by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organisations¹² In this case, the ISMS scope covers an outsourced data center that hosts the artificial intelligence (AI) cloud server for healthcare monitoring and analysis of the residents' data. Therefore, the audit evidence you need to find to verify the scope of the ISMS should include:

The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to comply with the relevant laws and regulations regarding the quality, safety, and privacy of healthcare services and patient data¹² The auditee has identified the resident's needs and expectations on how they should protect the resident's personal data. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to ensure the confidentiality, integrity, and availability of the resident's personal data that is collected, processed, and stored by the electronic wristband and the AI cloud server¹² The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located. This is an interface and dependency with another organisation that affects the ISMS scope, as the auditee has to control the externally provided processes, products, and services that are relevant to the ISMS, and to implement appropriate contractual requirements related to information security¹² The following options are not relevant or sufficient for verifying the scope of the ISMS:

The auditee has identified the resident's needs and expectations on the facility and environmental safety.

This is an external issue and an interested party requirement, but it does not affect the ISMS scope, as it is not related to information security¹² The auditee has ISO 9001 certification. This is an indication of the auditee's quality management system, but it does not verify the scope of the ISMS, as it is not related to information security¹² The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment. These are external issues and interested party requirements, but they do not affect the ISMS scope, as they are not related to information security¹² The auditee has identified the resident's needs and expectations on healthcare medical treatment services. These are external issues and interested party requirements, but they do not verify the scope of the ISMS, as they are not specific to information security¹² The auditee is considering the purchase of a healthcare monitoring app from an external software company. This is a potential change that may affect the ISMS scope in the future, but it does not verify the current scope of the ISMS, as it is not yet implemented or controlled¹²

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 # 52

The following options are key actions involved in a first-party audit. Order the stages to show the sequence in which the actions should take place.

Appoint an audit team leader

Issue the report

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

Prepare the audit checklist Gather objective evidence Review audit evidence Document findings

Answer:

Explanation:

Appoint an audit team leader

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

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

Prepare the audit checklist Gather objective evidence Review audit evidence Document findings

Explanation:

Appoint an audit team leader

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

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

Prepare the audit checklist Gather objective evidence Review audit evidence Document findings

The correct order of the stages is:

- * Prepare the audit checklist
- * Gather objective evidence
- * Review audit evidence
- * Document findings

* **Audit preparation:** This stage involves defining the audit objectives, scope, criteria, and plan. The auditor also prepares the audit checklist, which is a list of questions or topics that will be covered during the audit. The audit checklist helps the auditor to ensure that all relevant aspects of the ISMS are addressed and that the audit evidence is collected in a systematic and consistent manner¹².

* **Audit execution:** This stage involves conducting the audit activities, such as opening meeting, interviews, observations, document review, and closing meeting. The auditor gathers objective evidence, which is any information that supports the audit findings and conclusions. Objective evidence can be qualitative or quantitative, and can be obtained from various sources, such as records, statements, physical objects, or observations¹²³.

* **Audit reporting:** This stage involves reviewing the audit evidence, evaluating the audit findings, and documenting the audit results. The auditor reviews the audit evidence to determine whether it is sufficient, reliable, and relevant to support the audit findings. The auditor evaluates the audit findings to determine the degree of conformity or nonconformity of the ISMS with the audit criteria. The auditor

* documents the audit results in an audit report, which is a formal record of the audit process and outcomes. The audit report typically includes the following elements¹²³:

- * An introduction clarifying the scope, objectives, timing and extent of the work performed
- * An executive summary indicating the key findings, a brief analysis and a conclusion
- * The intended report recipients and, where appropriate, guidelines on classification and circulation
- * Detailed findings and analysis
- * Recommendations for improvement, where applicable
- * A statement of conformity or nonconformity with the audit criteria
- * Any limitations or exclusions of the audit scope or evidence
- * Any deviations from the audit plan or procedures
- * Any unresolved issues or disagreements between the auditor and the auditee
- * A list of references, abbreviations, and definitions used in the report
- * A list of appendices, such as audit plan, audit checklist, audit evidence, audit team members, etc.
- * Audit follow-up: This stage involves verifying the implementation and effectiveness of the corrective actions taken by the auditee to address the audit findings. The auditor monitors the progress and completion of the corrective actions, and evaluates their impact on the ISMS performance and conformity. The auditor may conduct a follow-up audit to verify the corrective actions on-site, or may rely on other methods, such as document review, remote interviews, or self-assessment by the auditee. The auditor documents the follow-up results and updates the audit report accordingly¹²³.

References:

- * PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
- * ISO 19011:2018 - Guidelines for auditing management systems
- * The ISO 27001 audit process | ISMS.online

NEW QUESTION # 53

A couple of years ago you started your company which has now grown from 1 to 20 employees. Your company's information is worth more and more and gone are the days when you could keep control yourself.

You are aware that you have to take measures, but what should they be? You hire a consultant who advises you to start with a qualitative risk analysis.

What is a qualitative risk analysis?

- A. This analysis is based on scenarios and situations and produces a subjective view of the possible threats.
- B. This analysis follows a precise statistical probability calculation in order to calculate exact loss caused by damage.

Answer: A

NEW QUESTION # 54

You are an ISMS audit team leader assigned by your certification body to carry out a follow-up audit of a Data Centre client. According to ISO 19011:2018, the purpose of a follow-up audit is to verify which one of the following?

- A. Completion and effectiveness of corrective actions
- B. The effectiveness of the management system
- C. Implementation of ISMS objectives
- D. Implementation of risk treatment plans

Answer: A

Explanation:

The purpose of a follow-up audit is to verify the completion and effectiveness of corrective actions taken by the auditee in response to the nonconformities identified in a previous audit¹. A follow-up audit is a type of audit that is conducted after an initial audit, and it focuses on the specific areas where nonconformities were found and corrective actions were agreed upon². A follow-up audit can be conducted as a separate audit or as part of a scheduled audit, depending on the nature and severity of the nonconformities and the audit programme objectives³.

The other options are not the purpose of a follow-up audit, but rather the purpose of other types of audits. For example:

*Option A is the purpose of a performance audit, which is a type of audit that evaluates the effectiveness of the management system in achieving its intended results⁴.

*Option B is the purpose of a compliance audit, which is a type of audit that verifies the conformity of the management system with the specified requirements, such as the ISMS objectives⁵.

*Option C is the purpose of a process audit, which is a type of audit that examines the inputs, activities, outputs, and interactions of a specific process within the management system, such as the risk treatment process.

References: 1: ISO 19011:2018, 6.7; 2: ISO 19011:2018, 3.7; 3: ISO 19011:2018, 5.5.2; 4: ISO 19011:2018, 3.6; 5: ISO 19011:2018, 3.5; : ISO 19011:2018, 3.4; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018;

: ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]

NEW QUESTION # 55

• • • • •

TestPDF ISO-IEC-27001-Lead-Auditor exam dumps have been developed with a conscious effort to abridge information into fewer questions and answers that any candidate can learn easily. Now you don't need to go through the hassle of studying lengthy manuals for ISO-IEC-27001-Lead-Auditor Exam Questions preparation. What you actually required is packed into easy to grasp content. Fix your attention on these ISO-IEC-27001-Lead-Auditor questions and answers and your success is guaranteed.

Valid ISO-IEC-27001-Lead-Auditor Exam Format: <https://www.testpdf.com/ISO-IEC-27001-Lead-Auditor-exam-braindumps.html>

- [illegible]

DOWNLOAD the newest TestPDF ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1A-j7hCjdR4NKpDfjRGvL6LfVZAALRq->