Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

ISO-IEC-27001-Lead-Auditor Practice Questions
ISO-IEC-27001-Lead-Auditor Practice Test
ISO-IEC-27001-Lead-Auditor Practice Exam
ISO-IEC-27001-Lead-Auditor Exam Questions
ISO-IEC-27001-Lead-Auditor Study Guide

killexams.com

PECB

ISO-IEC-27001-Lead-Auditor

PECB Certified ISO/IEC 27001 Lead Auditor

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ISO-IEC-27001-Lead-Auditor

Question: 559

In the context of security incident management, what does the term "escalation" refer to?

A. The initial reporting of a security incident
B. The documentation of security incidents
C. The process of increasing the urgency of a response
D. The analysis of the root cause of an incident

Answer: C

Explanation: Escalation in security incident management refers to increasing the urgency of a response, often involving notifying higher levels of management or specialized teams when a security incident occurs.

Question: 560

While reviewing audit documentation, you realize that the evidence collected does not adequately substantiate the conclusions drawn in the audit report. What is the best course of action?

A. Revise the audit conclusions to fit the available evidence
B. Present the findings as they are without modification
C. Ignore the discrepancies as they do not affect the overall audit
D. Document the inadequacies and suggest further investigation

Answer: D

Explanation: Documenting inadequacies and suggesting further investigation ensures that the audit report is accurate, reliable, and reflective of the true state of the ISMS.

Question: 561

As you conduct a stage 2 audit, you find that the organization has not implemented some of the controls as stated in their ISMS documentation. Which action should you take first?

A. Verify with relevant personnel why the controls were not implemented
B. Discuss your findings with the audit team
C. Prepare a non-conformity report immediately
D. Suggest additional controls to mitigate the risks

Answer: A

Explanation: It is crucial to understand why the controls were not implemented before concluding they are non-conformities. This step ensures that you gather adequate evidence and context regarding the organization's practices.

Question: 562

In an ISMS audit, which type of evidence is most valuable when assessing the effectiveness of the risk treatment plan, and what characteristics make this evidence preferable?

A. Testimonial evidence from management due to its authority.
B. Physical evidence, as it is tangible and verifiable.
C. Circumstantial evidence, as it supports the overall context.
D. Documentary evidence, which provides a clear trail of actions taken.

Answer: D

Explanation: Documentary evidence is crucial in assessing the effectiveness of a risk treatment plan since it provides a clear, verifiable record of actions taken and decisions made, ensuring transparency and accountability.

Question: 563

Which document serves as the foundation for developing an ISMS in compliance with ISO/IEC 27001?

A. Risk assessment report
B. Business continuity plan
C. Incident management plan
D. Information security policy

Answer: D

Explanation: The information security policy serves as the foundation for developing an ISMS, outlining the organization’s approach to managing information security.

Question: 564

What is the primary challenge an auditor faces when determining the amount of evidence required for an ISMS audit, particularly in relation to varying organizational contexts?

A. There is a standard amount of evidence that applies to all organizations.
B. The auditor must account for the specific risks and complexities of the organization.
C. Evidence requirements are solely based on the auditor's preferences.
D. Organizations typically provide an excessive amount of evidence.

Answer: B

Explanation: The auditor must consider the specific risks, complexities, and unique context of the organization to determine the appropriate amount of evidence needed, as there is no one-size-fits-all approach.

Question: 565
What is a primary reason for implementing a security awareness training program?

A. To comply with industry regulations
B. To educate employees about security risks and best practices
C. To improve employee morale
D. To reduce IT support costs

Answer: B
Explanation: A security awareness training program educates employees about security risks and best practices, helping to mitigate human-related security incidents.

Question: 566

When evaluating the value of data, which of the following factors is MOST critical in determining its potential impact on the organization if compromised?

A. The encryption strength used to protect the data.
B. The existence of backups for the data.
C. The sensitivity and confidentiality of the data.
D. The physical location of the data storage.

Answer: C

Explanation: The sensitivity and confidentiality of the data are crucial in assessing its value and the potential impact on the organization if it is compromised.

Question: 567

What is the primary purpose of conducting a "Context of the Organization" analysis before establishing an ISMS?

A. To identify resources available for information security
B. To evaluate the organization's current risk management practices
C. To understand external and internal factors affecting information security
D. To define the scope of the ISMS

Answer: C

Explanation: Understanding the context of the organization involves analyzing external and internal factors that can impact information security, which is essential for effective ISMS establishment.

Question: 568

When evaluating ethical dilemmas in an ISMS audit, which of the following obligations must the auditor prioritize to maintain integrity and compliance with the PECB Code of Ethics?

A. The auditor should prioritize the interests of the audit client over the requirements of regulatory authorities.
B. The auditor must balance the interests of the auditee while ensuring compliance with legal and regulatory obligations.
C. The auditor should focus solely on the auditee's perspective, disregarding any external regulations.
D. The auditor's primary responsibility is to the certification body, regardless of the auditee's compliance status.

Answer: B

Explanation: The auditor must balance the interests of the auditee with the legal and regulatory obligations to maintain integrity, ensuring that all parties are treated fairly and ethically.

Question: 569

Which of the following is NOT a recommended practice for ensuring data integrity in electronic records?

A. Regular audits of data access logs
B. Use of unverified third-party software
C. Implementing strict access controls
D. Maintaining a comprehensive backup strategy

Answer: B

Explanation: Using unverified third-party software can introduce vulnerabilities and risks that compromise data integrity, making it a practice to avoid.

Question: 570

Which of the following is a key benefit of implementing a formal ISMS based on ISO/IEC 27001 standards?

A. Elimination of all security risks
B. Improved stakeholder confidence and trust in the organization
C. Automatic compliance with all regulatory requirements
D. Guaranteed protection against data breaches

Answer: B

Explanation: Implementing a formal ISMS enhances stakeholder confidence and trust by demonstrating the organization's commitment to managing information security effectively.

Question: 571

During an ISMS audit, the assessment of audit findings should primarily aim to:

A. Identify root causes and opportunities for improvement
B. Determine compliance with ISO/IEC 27001 only
C. Highlight areas where the organization has failed
D. Provide suggestions for immediate corrective actions

Answer: A

Explanation: Assessing findings with the aim of identifying root causes and improvement opportunities fosters a constructive audit environment that supports organizational growth.

Question: 572

In managing the audit program, you need to ensure that all auditors maintain a high level of professional integrity. What is the best way to promote this among your audit team?

A. Provide ongoing training on ethical standards and practices
B. Implement strict penalties for unethical behavior
C. Conduct audits of auditors to monitor their performance
D. Encourage auditors to work independently without supervision

Answer: A

Explanation: Ongoing training on ethical standards reinforces the importance of integrity and equips auditors with the knowledge to uphold these principles in their work.

Question: 573

In the context of evidence collection during an ISMS audit, how does the concept of triangulation enhance the reliability of the findings?

A. Triangulation is irrelevant to evidence collection.
B. It combines evidence from multiple sources to confirm findings, enhancing reliability.
C. Triangulation only applies to quantitative evidence.
D. It focuses solely on subjective evidence to support findings.

Answer: B

Explanation: Triangulation enhances the reliability of findings by combining evidence from multiple sources, allowing auditors to confirm results and reduce the risk of errors or biases in the audit process.

Question: 574

During an ISMS audit, an auditor discovers that a member of the audit team has a personal relationship with a key stakeholder of the organization being audited. What is the most appropriate course of action for the lead auditor?

A. Ignore the relationship as it does not directly affect the audit results.
B. Conduct the audit as planned, but document the relationship in the audit findings.
C. Allow the team member to proceed with the audit since their expertise is crucial.
D. Reassign the team member to another role within the audit team to maintain impartiality.

Answer: D

Explanation: To maintain the integrity and impartiality of the audit, the lead auditor should reassign the team member to another role, ensuring that no conflicts of interest influence the audit process.

Question: 575

Which of the following is a common consequence of data integrity breaches in organizations?

A. Enhanced user experience
B. Legal penalties and fines
C. Improved data analytics
D. Increased customer trust

Answer: B

Explanation: Data integrity breaches can lead to legal penalties and fines, as organizations may fail to comply with regulations governing data protection and integrity.

Question: 576

In a situation where you discover that an organization's audit records have been tampered with after an audit, what is your immediate course of action as the lead auditor?

A. Ignore the tampering if the overall audit results are positive
B. Conclude the audit process without mentioning the tampering to avoid complications
C. Document the tampering, report it to senior management, and recommend a thorough investigation
D. Inform only the IT department, as it falls under their jurisdiction

Answer: C

Explanation: Documenting and reporting tampering is critical to maintaining the integrity of the audit

process and addressing potential compliance issues.

Question: 577

In the context of auditing practices, what challenges do auditors face when adapting to rapidly changing technology trends, particularly in relation to evidence collection?

A. Auditors typically have sufficient training to handle all technological changes.
B. Rapid changes can lead to outdated audit techniques that may not effectively evaluate current risks.
C. Technology trends are irrelevant to auditing practices.
D. Auditors should avoid using technology altogether to maintain traditional practices.

Answer: B

Explanation: Rapid technological changes can render traditional audit techniques ineffective, creating challenges for auditors in evaluating current risks and necessitating adaptations in their evidence collection methods.

Question: 578

During an ISO/IEC 27001 audit, you encounter significant discrepancies between the documented information and the actual practices observed. After the initial audit, what is the most effective approach for conducting follow-up activities to ensure that the discrepancies are addressed in a timely manner?

A. Immediately escalate the discrepancies to senior management without further investigation
B. Ignore the discrepancies if they are minor, as they do not impact the overall audit outcome
C. Document the discrepancies and wait for the next scheduled audit cycle
D. Schedule a follow-up audit to verify corrective actions after a predefined period

Answer: D

Explanation: A follow-up audit allows for the verification of corrective actions taken to address discrepancies, ensuring compliance and continuous improvement.

Question: 579

In the context of preparing for an ISO/IEC 27001 audit, which of the following actions is most critical for determining the level of materiality and applying a risk-based approach during the audit stages?

A. Conducting a comprehensive review of the organization’s financial statements
B. Mapping the organization's information assets and their associated risks
C. Analyzing historical audit findings to identify recurring issues
D. Engaging in stakeholder interviews to assess their perception of risk

Answer: B

Explanation: Mapping information assets and their risks is essential for understanding the potential impact of different audit findings and prioritizing audit activities based on risk levels.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.