

Certificate ISO-IEC-27001-Lead-Auditor Exam, ISO-IEC-27001-Lead-Auditor Reliable Exam Tutorial



DOWNLOAD the newest PassTestking ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1G8E6JR9jB8Xx2KL-bKyEEHvxxwNJJaM9B>

Our ISO-IEC-27001-Lead-Auditor study question is compiled and verified by the first-rate experts in the industry domestically and they are linked closely with the real exam. Our test bank provides all the questions which may appear in the real exam and all the important information about the exam. You can use the practice test software to test whether you have mastered the ISO-IEC-27001-Lead-Auditor Test Practice materials and the function of stimulating the exam to be familiar with the real exam's pace. So our ISO-IEC-27001-Lead-Auditor exam questions are real-exam-based and convenient for the clients to prepare for the ISO-IEC-27001-Lead-Auditor exam.

To become certified, individuals must pass the PECB ISO-IEC-27001-Lead-Auditor exam, which is a rigorous and comprehensive assessment of their knowledge and skills. ISO-IEC-27001-Lead-Auditor exam is designed to test the individual's ability to apply information security management principles and techniques to real-world situations.

PECB ISO-IEC-27001-Lead-Auditor exam covers a range of topics related to information security management, including risk management, security policies and procedures, security controls, and security auditing. ISO-IEC-27001-Lead-Auditor Exam also tests knowledge of the ISO/IEC 27001 standard and its implementation. Candidates who pass the exam demonstrate their ability to conduct effective information security audits and to manage an organization's information security management system in accordance with the ISO/IEC 27001 standard.

>> **Certificate ISO-IEC-27001-Lead-Auditor Exam** <<

ISO-IEC-27001-Lead-Auditor Reliable Exam Tutorial & ISO-IEC-27001-Lead-Auditor Exam Testking

You can download a free demo of PECB exam study material at PassTestking. The free demo of ISO-IEC-27001-Lead-Auditor exam product will eliminate doubts about our ISO-IEC-27001-Lead-Auditor PDF and practice exams. You should avail this opportunity of PECB Certified ISO/IEC 27001 Lead Auditor exam ISO-IEC-27001-Lead-Auditor exam dumps free demo. It will help you pay money without any doubt in mind. We ensure that our ISO-IEC-27001-Lead-Auditor Exam Questions will meet your ISO-IEC-27001-Lead-Auditor test preparation needs. If you remain unsuccessful in the ISO-IEC-27001-Lead-Auditor test after using our ISO-IEC-27001-Lead-Auditor product, you can ask for a full refund. PassTestking will refund you as per the terms and conditions.

The PECB ISO-IEC-27001-Lead-Auditor Exam consists of multiple-choice questions, and candidates are required to achieve a passing score of 70% or higher. ISO-IEC-27001-Lead-Auditor exam covers a range of topics, including the principles and concepts of information security, the ISO/IEC 27001 standard, and the auditing process. It also covers the skills and competencies required for conducting audits, managing audit teams, and communicating effectively with stakeholders.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q241-Q246):

NEW QUESTION # 241

A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives. What is not one of the four main objectives of a risk analysis?

- A. Establishing a balance between the costs of an incident and the costs of a security measure
- **B. Implementing counter measures**
- C. Determining relevant vulnerabilities and threats
- D. Identifying assets and their value

Answer: B

Explanation:

Implementing countermeasures is not one of the four main objectives of a risk analysis. A risk analysis is a systematic process that involves identifying, assessing, and evaluating potential risks to understand their likelihood and impact. Its objective is to develop strategies to manage or mitigate those risks effectively. The four main objectives of a risk analysis are:

Identifying assets and their value: This involves determining what are the information assets that need to be protected and how valuable they are for the organization.

Determining relevant vulnerabilities and threats: This involves identifying what are the weaknesses or flaws in the information assets or systems that could be exploited by malicious actors or events and what are the sources or causes of those potential attacks or incidents.

Establishing a balance between the costs of an incident and the costs of a security measure: This involves estimating what are the potential consequences or impacts of a risk occurrence in terms of financial, operational, reputational, or legal losses and comparing them with what are the costs or benefits of implementing a security measure to prevent or reduce that risk.

Providing a basis for risk treatment decisions: This involves prioritizing the risks based on their likelihood and impact and selecting the most appropriate risk treatment options such as avoiding, transferring, reducing, or accepting the risk.

Implementing countermeasures is not an objective but an outcome of a risk analysis. Countermeasures are specific actions or controls that are designed to prevent or mitigate a risk occurrence or impact. Countermeasures are selected based on the results of a risk analysis and aligned with the organization's risk appetite and objectives. Therefore, the correct answer is B. Reference: [ISO/IEC 27005:2018], clauses 6-9; Risk Analysis - What Is It, Benefits, Example, Methods - WallStreetMojo.

NEW QUESTION # 242

You are conducting an Information Security Management System 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 misaddressed labels and, in 15% of 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?

SM: 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 non-conformity against clause 8.1 of ISO 27001:2022.

Which one option below that best describes the non-conformity you have identified?

- A. The organisation does not have an efficient process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have detailed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational procedures to meet information security requirements.
- B. The organisation does not have an efficient process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have protected information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational processes to meet information security requirements.
- **C. The organisation does not have an effective process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have disclosed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without**

adequate operational controls to meet information security requirements.

- D. The organisation does not have an approved process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have corrected information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational methods to meet information security requirements.
- E. The organisation does not have an audited process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have inaccurate information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational rules to meet information security requirements.

Answer: C

Explanation:

The non-conformity you have identified relates to the organization's failure to implement adequate operational controls to ensure that service and regulatory requirements for data protection are met. This situation is particularly critical given the nature of the items being shipped, which include sensitive medical information and government documents. The fact that 15% of returned parcels have labels for different addresses, potentially exposing sensitive information to incorrect recipients, underscores the lack of effective information security practices.

The best description of the non-conformity, based on the details provided and the requirements of ISO/IEC 27001:2022, particularly clause 8.1 which deals with operational planning and control, would be:

C . The organisation does not have an effective process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have disclosed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational controls to meet information security requirements.

This option accurately captures the essence of the non-conformity by highlighting the lack of effective operational controls to protect sensitive information, leading to potential unauthorized disclosure of information intended for another party. This is a direct violation of information security management principles, particularly those related to the protection of confidentiality and integrity of information as mandated by ISO/IEC 27001:2022.

NEW QUESTION # 243

CMM stands for?

- A. Capacity Maturity Matrix
- B. Capable Mature Model
- **C. Capability Maturity Model**
- D. Capability Maturity Matrix

Answer: C

NEW QUESTION # 244

A planning process that introduced the concept of planning as a cycle that forms the basis for continuous improvement is called:

- A. time based planning.
- B. RACI Matrix
- C. planning for continuous improvement.
- **D. plan, do, check, act.**

Answer: D

NEW QUESTION # 245

You are performing an ISO 27001 ISMS surveillance audit at a residential nursing home, ABC Healthcare Services. ABC uses a healthcare mobile app designed and maintained by a supplier, WeCare, to monitor residents' well-being. During the audit, you learn that 90% of the residents' family members regularly receive medical device advertisements from WeCare, by email and SMS once a week. The service agreement between ABC and WeCare prohibits the supplier from using residents' personal data. ABC has received many complaints from residents and their family members.

The Service Manager says that the complaints were investigated as an information security incident which found that they were justified. Corrective actions have been planned and implemented according to the nonconformity and corrective action management

procedure.

You write a nonconformity "ABC failed to comply with information security control A.5.34 (Privacy and protection of PII) relating to the personal data of residents' and their family members. A supplier, WeCare, used residents' personal information to send advertisements to family members" Select three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity

- A. ABC confirms that information security control A.5.34 is contained in the Statement of Applicability (SoA)
- B. ABC needs to collect more evidence on how information security risk assessment relates to the identified nonconformities before concluding actions on the nonconformity
- C. ABC instructs all staff to follow the signed healthcare service agreement with residents' family members
- D. ABC conducts a management review to take the feedback from residents' family members into consideration
- E. The Service Manager implements the corrective actions and Customer Service Representatives evaluate the effectiveness of implemented corrective actions
- F. ABC needs to collect more evidence on how the organisation defines the management system scope and find out if they covered WeCare the medical device manufacturer
- G. The Service Manager provides evidence of analysis of the cause of nonconformity and how the ABC evaluates the effectiveness of implemented corrective actions
- H. ABC identifies and checks compliance with all applicable legislation and contractual requirements involving third parties

Answer: E,G,H

Explanation:

According to the ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, the following corrections and corrective actions are expected from ABC in response to the nonconformity:

* B. The Service Manager provides evidence of analysis of the cause of nonconformity and how the ABC evaluates the effectiveness of implemented corrective actions. This is part of the requirement of clause 10.1 of ISO/IEC 27001:2022, which states that the organization shall determine the causes of nonconformities and evaluate the need for action to ensure that they do not recur or occur elsewhere¹².

The organization shall also evaluate the effectiveness of any corrective actions taken¹².

* F. ABC identifies and checks compliance with all applicable legislation and contractual requirements involving third parties. This is part of the requirement of clause 4.2 of ISO/IEC 27001:2022, which states that the organization shall determine the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system¹². This includes the legal and contractual requirements related to the information security aspects of the organization's activities, products and services¹².

* G. The Service Manager implements the corrective actions and Customer Service Representatives evaluate the effectiveness of implemented corrective actions. This is part of the requirement of clause 10.1 of ISO/IEC 27001:2022, which states that the organization shall implement any action needed and retain documented information as evidence of the results of any action taken¹². The organization shall also monitor, measure, analyze and evaluate the information security performance and the effectiveness of the information security management system¹².

References:

- * 1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, CQI and IRCA Certified Training, 1
- * 2: ISO/IEC 27001 Lead Auditor Training Course, PECB, 2

NEW QUESTION # 246

.....

ISO-IEC-27001-Lead-Auditor Reliable Exam Tutorial: <https://www.passtestking.com/PECB/ISO-IEC-27001-Lead-Auditor-practice-exam-dumps.html>

- New ISO-IEC-27001-Lead-Auditor Test Tips Valid ISO-IEC-27001-Lead-Auditor Test Syllabus Valid ISO-IEC-27001-Lead-Auditor Test Blueprint Open website 「 www.examcollectionpass.com 」 and search for ➡ ISO-IEC-27001-Lead-Auditor for free download ISO-IEC-27001-Lead-Auditor Valid Exam Vce
- Vce ISO-IEC-27001-Lead-Auditor Test Simulator Sample ISO-IEC-27001-Lead-Auditor Questions Answers Valid ISO-IEC-27001-Lead-Auditor Test Syllabus Download “ ISO-IEC-27001-Lead-Auditor ” for free by simply entering 【 www.pdfvce.com 】 website Vce ISO-IEC-27001-Lead-Auditor Test Simulator
- Pass Guaranteed PECB - ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam–Efficient Certificate Exam Search for ✓ ISO-IEC-27001-Lead-Auditor ✓ and obtain a free download on “ www.prepawayete.com ” ISO-IEC-27001-Lead-Auditor Vce Torrent
- ISO-IEC-27001-Lead-Auditor Relevant Questions ISO-IEC-27001-Lead-Auditor Reliable Study Plan ISO-IEC-27001-Lead-Auditor Practice Exam Pdf ~ Search for { ISO-IEC-27001-Lead-Auditor } and obtain a free download on

