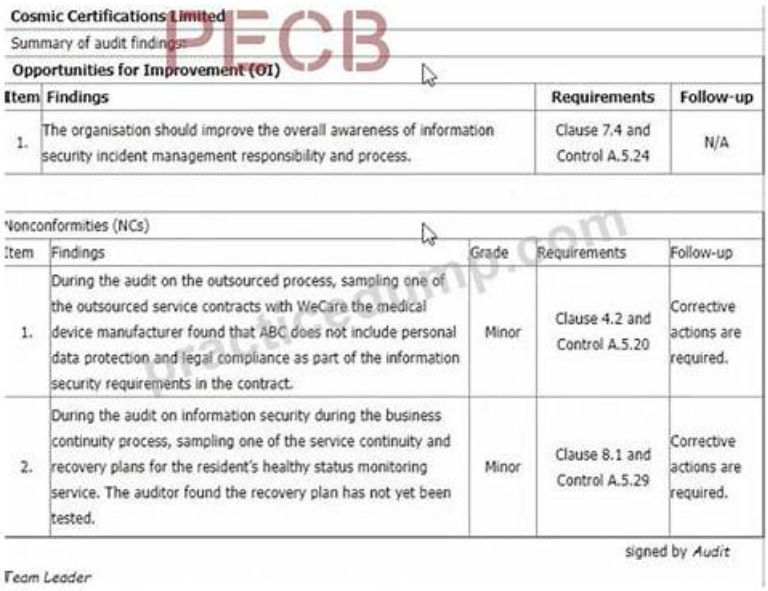
Dump ISO-IEC-27001-Lead-Auditor File - ISO-IEC-27001-Lead-Auditor Practice Mock



Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

Item	Findings	Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.	Clause 7.4 and Control A.5.24	N/A

Nonconformities (NCs)

Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.

signed by Audit

Team Leader

P.S. Free 2026 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by Exam-Killer: https://drive.google.com/open?id=1ydJ7g8Blk_uHh3sytE4f5viFEQ24hA9L

You can absolutely assure about the high quality of our products, because the contents of ISO-IEC-27001-Lead-Auditor training materials have not only been recognized by hundreds of industry experts, but also provides you with high-quality after-sales service. Before purchasing ISO-IEC-27001-Lead-Auditor exam torrent, you can log in to our website for free download. During your installation, ISO-IEC-27001-Lead-Auditor exam questions hired dedicated experts to provide you with free remote online guidance. During your studies, ISO-IEC-27001-Lead-Auditor Exam Torrent also provides you with free online services for 24 hours, regardless of where and when you are, as long as an email, we will solve all the problems for you. At the same time, if you fail to pass the exam after you have purchased ISO-IEC-27001-Lead-Auditor training materials, you just need to submit your transcript to our customer service staff and you will receive a full refund.

PECB ISO-IEC-27001-Lead-Auditor Certification is a globally recognized credential that confirms your expertise in information security management systems auditing. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is ideal for professionals who wish to enhance their career prospects and credibility in the industry. It is also beneficial for those who are responsible for conducting ISMS audits in their organizations or for those who wish to become independent auditors.

>> Dump ISO-IEC-27001-Lead-Auditor File <<

ISO-IEC-27001-Lead-Auditor Practice Mock, ISO-IEC-27001-Lead-Auditor New Learning Materials

It doesn't matter if it's your first time to attend ISO-IEC-27001-Lead-Auditor practice test or if you are freshman in the IT certification test, our latest ISO-IEC-27001-Lead-Auditor dumps guide will boost you confidence to face the challenge. Our dumps collection will save you much time and ensure you get high mark in ISO-IEC-27001-Lead-Auditor Actual Test with less effort. Come and check the free demo in our website you won't regret it.

The ISO-IEC-27001-Lead-Auditor Certification Exam is intended for professionals who have experience in information security management and auditing. It is designed to help individuals acquire the skills and knowledge required to conduct an effective and efficient ISMS audit. PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam covers various topics, including the principles of information security management, the ISO 27001 standard, auditing techniques, and the certification process.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q201-Q206):

NEW QUESTION # 201
Scenario 2:
Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and proprietary technologies.
Clinic established the scope of its ISMS by solely considering internal issues, interfaces, dependencies between internal and outsourced activities, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.
Despite initial challenges, Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001 while incorporating additional sector-specific controls to enhance security. The team evaluated the applicability of these controls against internal and external factors, culminating in the development of a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.
As preparations for certification progressed, Brian, appointed as the team leader, adopted a self-directed risk assessment methodology to identify and evaluate the company's strategic issues and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and mission.
Does the Clinic's SoA document meet the ISO/IEC 27001 requirements for the SoA?

- A. No, because it does not contain the justification for the exclusion of controls from Annex A of ISO/IEC 27001
- B. No, because security controls selected from sources other than Annex A of ISO/IEC 27001 are included
- C. Yes, because it comprises an exhaustive list of controls considered applicable from Annex A of ISO/IEC 27001 and the other sources

Answer: A

Explanation:
Comprehensive and Detailed In-Depth
The Statement of Applicability (SoA) is a mandatory document in ISO/IEC 27001:2022 that lists all Annex A controls, their applicability, and justifications for inclusion or exclusion.
C . Correct Answer: The SoA must include justifications for excluding Annex A controls. The A . Incorrect: While the SoA should include an exhaustive list of controls, simply listing applicable controls from Annex A and other sources does not meet the requirement if exclusions are not justified.
B . Incorrect: Including security controls from other sources is allowed and does not invalidate the SoA, as organizations can define additional controls beyond Annex A based on their risk assessment.

NEW QUESTION # 202
Scenario 8: EsBank provides banking and financial solutions to the Estonian banking sector since September
2010. The company has a network of 30 branches with over 100 ATMs across the country.
Operating in a highly regulated industry, EsBank must comply with many laws and regulations regarding the security and privacy of data. They need to manage information security across their operations by implementing technical and nontechnical controls. EsBank decided to implement an ISMS based on ISO/IEC
27001 because it provided better security, more risk control, and compliance with key requirements of laws and regulations.
Nine months after the successful implementation of the ISMS, EsBank decided to pursue certification of their ISMS by an independent certification body against ISO/IEC 27001 .The certification audit included all of EsBank's systems, processes, and technologies.
The stage 1 and stage 2 audits were conducted jointly and several nonconformities were detected. The first nonconformity was related to EsBank's labeling of information. The company had an information classification scheme but there was no information labeling procedure. As a result, documents requiring the same level of protection would be labeled differently (sometimes as confidential, other times sensitive).
Considering that all the documents were also stored electronically, the nonconformity also impacted media handling. The audit team used sampling and concluded that 50 of 200 removable media stored sensitive information mistakenly classified as confidential. According to the information classification scheme, confidential information is allowed to be stored in removable media, whereas storing sensitive information is strictly prohibited. This marked the other nonconformity.
They drafted the nonconformity report and discussed the audit conclusions with EsBank's representatives, who agreed to submit an action plan for the detected nonconformities within two months.
EsBank accepted the audit team leader's proposed solution. They resolved the nonconformities by drafting a procedure for information labeling based on the classification scheme for both physical and electronic formats. The removable media procedure

was also updated based on this procedure.
Two weeks after the audit completion, EsBank submitted a general action plan. There, they addressed the detected nonconformities and the corrective actions taken, but did not include any details on systems, controls, or operations impacted. The audit team evaluated the action plan and concluded that it would resolve the nonconformities. Yet, EsBank received an unfavorable recommendation for certification.
Based on the scenario above, answer the following question:
Which option justifies the unfavorable recommendation for certification? Refer to scenario 8.

- A. The major nonconformity related to storing sensitive information in removable media
- B. The minor nonconformity related to the lack of information labeling procedure
- C. The unrealistic date of the submitted action plan (two weeks)

Answer: A

Explanation:
The major nonconformity related to storing sensitive information in removable media justifies the unfavorable recommendation for certification. This issue directly contradicts the information classification scheme's stipulations, indicating a significant oversight in enforcing the ISMS policies.

NEW QUESTION # 203
Which one of the following options best describes the main purpose of a Stage 1 third-party audit?

- A. To determine redness for a stage 2 audit
- B. To learn about the organisation's procurement
- C. To get to know the organisation's customers
- D. To prepare an independent audit report
- E. To introduce the audit team to the client
- F. To check for legal compliance by the organisation

Answer: A

Explanation:
Explanation
The main purpose of a Stage 1 third-party audit is to determine readiness for a Stage 2 audit. A Stage 1 audit is a preliminary assessment that evaluates the organization's ISMS documentation, scope, context, and objectives, and identifies any major gaps or nonconformities that need to be addressed before the Stage 2 audit. A Stage 1 audit does not introduce the audit team to the client, as this is done during the audit planning phase. A Stage 1 audit does not check for legal compliance by the organization, as this is done during the Stage 2 audit. A Stage 1 audit does not prepare an independent audit report, as this is done after the Stage 2 audit.
References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 70. : ISO/IEC 27001 LEAD AUDITOR - PECB, page 23.

NEW QUESTION # 204
You are conducting a third-party surveillance audit when another member of the audit team approaches you seeking clarification. They have been asked to assess the organisation's application of control 5.7 - Threat Intelligence. They are aware that this is one of the new controls introduced in the 2022 edition of ISO/IEC 27001, and they want to make sure they audit the control correctly. They have prepared a checklist to assist them with their audit and want you to confirm that their planned activities are aligned with the control's requirements.
Which three of the following options represent valid audit trails?

- A. I will ensure that the task of producing threat intelligence is assigned to the organisation's internal audit team
- B. I will check that the organisation has a fully documented threat intelligence process
- C. I will ensure that the organisation's risk assessment process begins with effective threat intelligence
- D. I will speak to top management to make sure all staff are aware of the importance of reporting threats
- E. I will check that threat intelligence is actively used to protect the confidentiality, integrity and availability of the organisation's information assets
- F. I will determine whether internal and external sources of information are used in the production of threat intelligence
- G. I will review how information relating to information security threats is collected and evaluated to produce threat intelligence
- H. I will ensure that appropriate measures have been introduced to inform top management as to the effectiveness of current

threat intelligence arrangements

Answer: E,G,H

Explanation:
These three options represent valid audit trails for control 5.7, as they are aligned with the control's requirements and objectives. According to the web search results from my predefined tool, control 5.7 requires organisations to collect and analyse information relating to information security threats and use that information to take mitigation actions12. The control also specifies that threat intelligence should be relevant, perceptive, contextual, and actionable, and that it should be used to prevent, detect, or respond to threats34. Therefore, the auditor should verify how the organisation collects, analyses, and produces threat intelligence, how it uses threat intelligence to protect its information assets, and how it monitors and evaluates the effectiveness of its threat intelligence arrangements. The other options are not valid audit trails, as they are either irrelevant, incorrect, or incomplete. For example:
* The task of producing threat intelligence is not assigned to the organisation's internal audit team, but to the person or team responsible for the ISMS, such as the information security manager or the information security committee5 .
* The organisation's risk assessment process does not begin with effective threat intelligence, but with the identification of the context, scope, and objectives of the ISMS . Threat intelligence is an input for the risk identification and analysis, but not the starting point of the risk assessment process.
* Speaking to top management to make sure all staff are aware of the importance of reporting threats is not sufficient to audit the control, as it does not address how the organisation collects, analyses, and produces threat intelligence, nor how it uses it to take mitigation actions. The auditor should also speak to the staff involved in the threat intelligence process, and review the relevant documents and records.
* Checking that the organisation has a fully documented threat intelligence process is not enough to audit the control, as it does not verify the implementation and effectiveness of the process. The auditor should also observe the process in action, and examine the outputs and outcomes of the process.
* Determining whether internal and external sources of information are used in the production of threat intelligence is a partial audit trail, as it only covers one aspect of the control. The auditor should also assess the quality, reliability, and relevance of the sources, and how the information is analysed and used.

NEW QUESTION # 205
All are prohibited in acceptable use of information assets, except:

- A. Company-wide e-mails with supervisor/TL permission.
- B. Messages with very large attachments or to a large number ofrecipients.
- C. E-mail copies to non-essential readers
- D. Electronic chain letters

Answer: A

Explanation:
The only option that is not prohibited in acceptable use of information assets is C: company-wide e-mails with supervisor/TL permission. This option implies that the sender has obtained the necessary authorization from their supervisor or team leader to send an e-mail to all employees in the organization. This could be done for legitimate business purposes, such as announcing important news, events or updates that are relevant to everyone. However, this option should still be used sparingly and responsibly, as it could cause unnecessary disruption or annoyance to the recipients if abused or misused. The other options are prohibited in acceptable use of information assets, as they could violate the information security policies and procedures of the organization, as well as waste resources and bandwidth. Electronic chain letters (A) are messages that urge recipients to forward them to multiple other people, often with false or misleading claims or promises. They are considered spam and could contain malicious links or attachments that could compromise information security. E-mail copies to non-essential readers (B) are messages that are sent to recipients who do not need to receive them or have no interest in them. They are considered unnecessary and could clutter the inbox and distract the recipients from more important messages. Messages with very large attachments or to a large number of recipients (D) are messages that consume a lot of network resources and could affect the performance or availability of the information systems. They could also exceed the storage capacity or quota limits of the recipients' mailboxes and cause problems for them. ISO/IEC 27001:2022 requires the organization to implement rules for acceptable use of assets (see clause A.8.1.3). Reference: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Acceptable Use?

NEW QUESTION # 206
.....

ISO-IEC-27001-Lead-Auditor Practice Mock: https://www.exam-killer.com/ISO-IEC-27001-Lead-Auditor-valid-questions.html

- Practice ISO-IEC-27001-Lead-Auditor Test Engine □ ISO-IEC-27001-Lead-Auditor Reliable Test Practice □ New ISO-IEC-27001-Lead-Auditor Real Exam □ Easily obtain ➽ ISO-IEC-27001-Lead-Auditor □ for free download through ➤ www.examcollectionpass.com □ □New ISO-IEC-27001-Lead-Auditor Real Exam
- Pass Guaranteed High Pass-Rate ISO-IEC-27001-Lead-Auditor - Dump PECB Certified ISO/IEC 27001 Lead Auditor exam File □ Search for □ ISO-IEC-27001-Lead-Auditor □ and download it for free on ➡ www.pdfvce.com □□□ website □ISO-IEC-27001-Lead-Auditor Vce Download
- Top Dump ISO-IEC-27001-Lead-Auditor File Pass Certify | Valid ISO-IEC-27001-Lead-Auditor Practice Mock: PECB Certified ISO/IEC 27001 Lead Auditor exam □ Open website ➡ www.pass4test.com □□□ and search for ⇛ ISO-IEC-27001-Lead-Auditor ⇚ for free download □Flexible ISO-IEC-27001-Lead-Auditor Learning Mode
- ISO-IEC-27001-Lead-Auditor Reliable Exam Blueprint □ Latest ISO-IEC-27001-Lead-Auditor Test Preparation □ ISO-IEC-27001-Lead-Auditor Valid Mock Test □ Search for ⇛ ISO-IEC-27001-Lead-Auditor ⇚ and download it for free on （ www.pdfvce.com ） website □New Exam ISO-IEC-27001-Lead-Auditor Materials
- Top Dump ISO-IEC-27001-Lead-Auditor File Pass Certify | Valid ISO-IEC-27001-Lead-Auditor Practice Mock: PECB Certified ISO/IEC 27001 Lead Auditor exam↴ Go to website ➥ www.vceengine.com □ open and search for 【 ISO-IEC-27001-Lead-Auditor 】 to download for free □ISO-IEC-27001-Lead-Auditor Valid Test Braindumps
- ISO-IEC-27001-Lead-Auditor Reliable Test Preparation □ Books ISO-IEC-27001-Lead-Auditor PDF □ ISO-IEC-27001-Lead-Auditor Trustworthy Pdf □ Search for □ ISO-IEC-27001-Lead-Auditor □ and download it for free on □ www.pdfvce.com □ website □ISO-IEC-27001-Lead-Auditor Reliable Test Practice
- ISO-IEC-27001-Lead-Auditor Valid Test Braindumps □ ISO-IEC-27001-Lead-Auditor Valid Exam Notes □ ISO-IEC-27001-Lead-Auditor Reliable Test Practice □ Search for 「 ISO-IEC-27001-Lead-Auditor 」 and download it for free on ➡ www.pass4test.com □□□ website ☮ISO-IEC-27001-Lead-Auditor Trustworthy Pdf
- 100% Pass PECB ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam Marvelous Dump File □ Search for ➽ ISO-IEC-27001-Lead-Auditor □ and download it for free on ➤ www.pdfvce.com □ website □ □ISO-IEC-27001-Lead-Auditor Exam Price
- Top Dump ISO-IEC-27001-Lead-Auditor File Pass Certify | Valid ISO-IEC-27001-Lead-Auditor Practice Mock: PECB Certified ISO/IEC 27001 Lead Auditor exam □ Easily obtain （ ISO-IEC-27001-Lead-Auditor ） for free download through 《 www.vce4dumps.com 》 □ISO-IEC-27001-Lead-Auditor Reliable Test Preparation
- Pass Guaranteed Quiz ISO-IEC-27001-Lead-Auditor - Accurate Dump PECB Certified ISO/IEC 27001 Lead Auditor exam File □ Open [www.pdfvce.com] enter 《 ISO-IEC-27001-Lead-Auditor 》 and obtain a free download □New ISO-IEC-27001-Lead-Auditor Real Exam
- ISO-IEC-27001-Lead-Auditor Actual Tests □ ISO-IEC-27001-Lead-Auditor Examcollection Questions Answers □ ISO-IEC-27001-Lead-Auditor Vce Download □ □ www.validtorrent.com □ is best website to obtain 「 ISO-IEC-27001-Lead-Auditor 」 for free download □ISO-IEC-27001-Lead-Auditor Reliable Test Preparation
- www.stes.tyc.edu.tw, www.competize.com, www.stes.tyc.edu.tw, lms.ait.edu.za, app.parler.com, www.stes.tyc.edu.tw, ncon.edu.sa, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, pct.edu.pk, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Exam-Killer ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1ydJ7g8Blk_uHh3sytE4f5viFEQ24hA9L