Pass Guaranteed 2025 PECB ISO-IEC-27001-Lead-Auditor: The Best Pass PECB Certified ISO/IEC 27001 Lead Auditor exam Test Guide

P.S. Free 2025 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by ITExamDownload: https://drive.google.com/open?id=1SblE0vjCiPfyYm1ntfR0ymk2iEwAJU8k

We promise you that if you fail to pass the exam after using ISO-IEC-27001-Lead-Auditor training materials of us, we will give you full refund. We are pass guarantee and money back guarantee if you fail to pass the exam. Besides, ISO-IEC-27001-Lead-Auditor exam dumps are high-quality, you can pass the exam just one time if you choose us. We offer you free update for one year for ISO-IEC-27001-Lead-Auditor Training Materials, and our system will send the update version to your email automatically. We have online and offline service, the staff possess the professional knowledge for ISO-IEC-27001-Lead-Auditor exam dumps, if you have any questions, don't hesitate to contact us.

PECB ISO-IEC-27001-Lead-Auditor is a certification exam that tests the knowledge and skills of individuals seeking to become certified ISO/IEC 27001 lead auditors. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is offered by the Professional Evaluation and Certification Board (PECB) and is highly regarded in the field of information security management.

>> Pass ISO-IEC-27001-Lead-Auditor Test Guide <<

2025 ISO-IEC-27001-Lead-Auditor: Valid Pass PECB Certified ISO/IEC 27001 Lead Auditor exam Test Guide

OurISO-IEC-27001-Lead-Auditor practice engine has collected the frequent-tested knowledge into the content for your reference according to our experts' years of diligent work. So our ISO-IEC-27001-Lead-Auditor exam materials are triumph of their endeavor. By resorting to our ISO-IEC-27001-Lead-Auditor practice materials, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our training engine, the passing rate is 98-100 percent. So your chance of getting success will be increased greatly by our ISO-IEC-27001-Lead-Auditor Exam Questions.

PECB ISO-IEC-27001-Lead-Auditor Certification Exam is a challenging and rewarding certification that requires dedication and commitment to study and prepare for the exam. ISO-IEC-27001-Lead-Auditor exam covers a range of topics, including ISMS, risk management, auditing principles, and compliance with regulatory requirements. By passing the certification exam, individuals gain recognition for their knowledge and skills in the field of information security management and open up opportunities for career advancement.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q306-Q311):

NEW QUESTION # 306
You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymization tests failed. Also, whether the Service Manager is authorized to approve the test.
The IT Manager explains the test results should be approved by him according to the software security management procedure. The

reason why the encryption and pseudonymization functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You sample one of the medical staff's mobile and found that ABC's healthcare mobile app, version 1.01 is installed. You found that version 1.01 has no test record.
The IT Manager explains that because of frequent ransomware attacks, the outsourced mobile app development company gave a free minor update on the tested software, performed an emergency release of the updated software, and gave a verbal guarantee that there will be no impact on any security functions. Based on his 20 years of information security experience, there is no need to re-test.
You are preparing the audit findings Select two options that are correct.

- A. There is NO nonconformity (NC). The IT Manager demonstrates good leadership. (Relevant to clause 5.1, control 5.4)
- B. There is NO nonconformity (NC). The IT Manager demonstrates he is fully competent. (Relevant to clause 7.2)
- C. There is an opportunity for improvement (OI). The organisation selects an external service provider based on the extent of free services it will provide. (Relevant to clause 8.1, control A.5.21)
- D. There is a nonconformity (NC). The IT Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
- E. There is a nonconformity (NC). The organisation does not control planned changes and review the consequences of unintended changes. (Relevant to clause 8.1)
- F. There is an opportunity for improvement (OI). The IT Manager should make the decision to continue the service based on appropriate testing. (Relevant to clause 8.1, control A.8.30)

Answer: D,E

Explanation:
Explanation
According to ISO 27001:2022 Annex A Control 8.30, the organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This includes developing and entering into licensing agreements that cover code ownership and intellectual property rights, and implementing appropriate contractual requirements related to secure design and coding in accordance with Annex A 8.25 and 8.2912 In this case, the organisation and the developer have performed security tests that failed, which indicates that the secure design and coding requirements of Annex A 8.29 were not met. The IT Manager explains that the encryption and pseudonymization functions failed because they slowed down the system and service performance, and that an extra 150% of resources are needed to cover this. However, this does not justify the acceptance of the test results by the Service Manager, who is not authorised to approve the test according to the software security management procedure. The Service Manager should have consulted with the IT Manager, who is the owner of the process, and followed the procedure for handling nonconformities and corrective actions. The Service Manager's decision to continue the service based on access control alone exposes the organisation to the risk of compromising the confidentiality, integrity, and availability of personal data processed by the mobile app. Therefore, there is a nonconformity (NC) with clause 8.1, control A.8.30.
According to ISO 27001:2022 Clause 8.1, the organisation shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in Clause 6.1. The organisation shall also control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary12 In this case, the organisation has not controlled the planned change of the mobile app from version 1.0 to version 1.01, which was a minor update provided by the outsourced developer in response to frequent ransomware attacks. The IT Manager explains that the developer performed an emergency release of the updated software, and gave a verbal guarantee that there will be no impact on any security functions.
However, this is not sufficient to ensure that the change is properly assessed, tested, documented, and approved before deployment. The IT Manager should have followed the change management process and procedure, and verified that the updated software meets the security requirements and does not introduce any new vulnerabilities or risks. The IT Manager's reliance on his 20 years of information security experience and the developer's verbal guarantee is not a valid basis for skipping the re-testing of the software. Therefore, there is a nonconformity (NC) with clause 8.1.
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 # 307
Scenario 4: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs. Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology. equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its

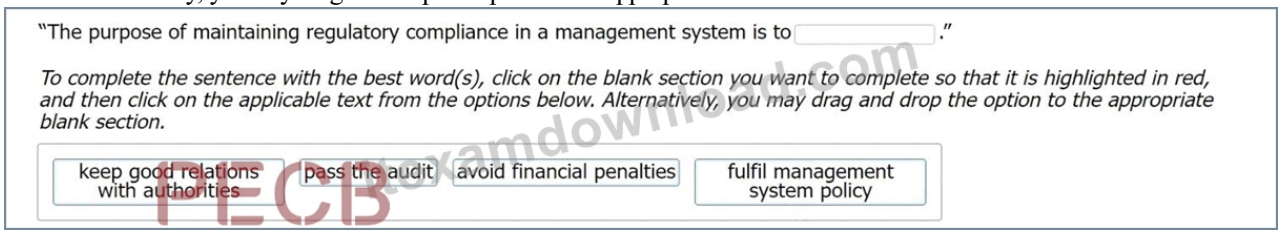
commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit. Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence based approach, particularly in light of two information security incidents reported by Techvology in the past year The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards The auditors also verified whether Techvology complied with the contractual requirements established between the two entities This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to. Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
Based on the scenario above, answer the following question:
Were the auditors diligent in adhering to the auditing process for outsourced operations?

- A. Yes, they demonstrated diligence and judgment in their auditing practices
- B. No, the auditors did not interview any of Techvology's top management during the audit
- C. No, the auditors did not request a sample of employment contracts until the end of the audit

Answer: A

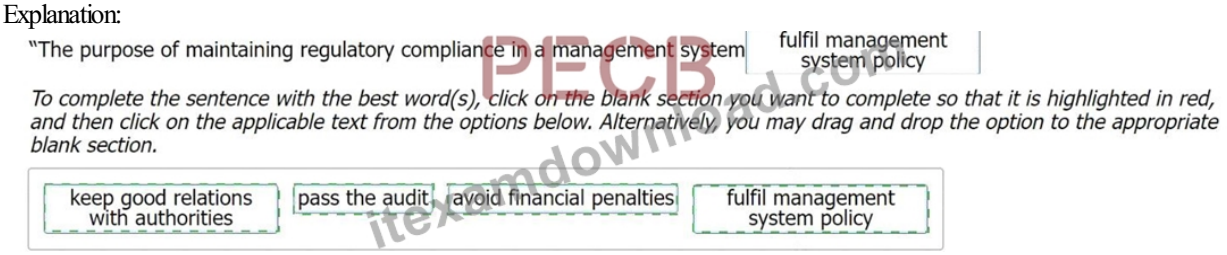
Explanation:
Comprehensive and Detailed In-Depth
A . Correct Answer:
ISO 19011:2018 (Guidelines for Auditing Management Systems) outlines diligent audit practices, including evidence-based assessment and professional skepticism.
The auditors critically reviewed records, interviewed staff, and validated incident response effectiveness.
They did not rely solely on verbal statements but sought concrete evidence, demonstrating due diligence and judgment.
B . Incorrect:
Employment contracts are not primary audit evidence for competence; training and certification records hold greater significance.
C . Incorrect:
The scenario does not mention that top management was excluded from interviews. However, their involvement is not mandatory for evaluating incident handling.
Relevant Standard Reference:

NEW QUESTION # 308
Select the words that best complete the sentence:
"The purpose of maintaining regulatory compliance in a management system is to To complete the sentence with the best word(s), 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 option to the appropriate blank section.



Answer:

Explanation:



Explanation

According to ISO 27001:2013, clause 5.2, the top management of an organization must establish, implement and maintain an information security policy that is appropriate to the purpose of the organization and provides a framework for setting information security objectives. The information security policy must also include a commitment to comply with the applicable legal, regulatory and contractual requirements, as well as any other requirements that the organization subscribes to. Therefore, maintaining regulatory compliance is part of fulfilling the management system policy and ensuring its effectiveness and suitability. References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 5.2
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* ISO 27001 Policy: How to write it according to ISO 27001

NEW QUESTION # 309
Scenario 6: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.
Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles This phase was crucial for aligning the team with the audit's objectives and scope However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber Acrypt's policies This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.
The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.
The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.
The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert s objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.
Based on the scenario above, answer the following question:
Based on Scenario 6, is the audit team leader's decision regarding the technical expert's behavior acceptable?

- A. No, questioning the expert's objectivity is not a valid reason for the audit team leader to discuss the matter with the certification body

- B. No, the audit team leader should have reported the issue directly to the top management instead
- C. Yes, if the auditor is skeptical about the technical expert's objectivity, he must discuss his concerns with the certification body

Answer: C

Explanation:
Comprehensive and Detailed In-Depth
C . Correct Answer:
ISO 17021-1:2015 Clause 5.2.4 requires auditors to report impartiality concerns.
The technical expert received consultancy fees from Cyber ACrypt, creating a conflict of interest.
The certification body must be informed to ensure audit integrity.
A . Incorrect:
Reporting to top management does not resolve certification body independence concerns.
B . Incorrect:
Impartiality is a critical concern in ISO/IEC 27001 certification.
Relevant Standard Reference:
ISO/IEC 17021-1:2015 Clause 5.2.4 (Ensuring Impartiality in Audits)

NEW QUESTION # 310
Information or data that are classified as _____ do not require labeling.

- A. Internal
- B. Confidential
- C. Highly Confidential
- D. Public

Answer: D

Explanation:
Explanation
Information or data that are classified as public do not require labeling. Public information or data are those that are intended for general disclosure and have no impact on the organization's operations or reputation if disclosed. Labeling is a method of implementing classification, which is a process of structuring information according to its sensitivity and value for the organization. Labeling helps to identify the level of protection and handling required for each type of information. Information or data that are classified as internal, confidential, or highly confidential require labeling, as they contain information that is not suitable for public disclosure and may cause harm or loss to the organization if disclosed. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page
37. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 14.

NEW QUESTION # 311
.....

www.examcollectionpass.com open and search for ✔ ISO-IEC-27001-Lead-Auditor ✔ to download for free Reliable ISO-IEC-27001-Lead-Auditor Dumps Free

- PECB Certified ISO/IEC 27001 Lead Auditor exam dumps torrent - ISO-IEC-27001-Lead-Auditor exam pdf - PECB Certified ISO/IEC 27001 Lead Auditor exam study practice Search for ▶ ISO-IEC-27001-Lead-Auditor ◀ and download exam materials for free through ➠ www.pdfvce.com ISO-IEC-27001-Lead-Auditor Valid Test Blueprint
- Questions ISO-IEC-27001-Lead-Auditor Exam Study Guide ISO-IEC-27001-Lead-Auditor Pdf Valid ISO-IEC-27001-Lead-Auditor Exam Questions Search for 《 ISO-IEC-27001-Lead-Auditor 》 on { www.pass4leader.com } immediately to obtain a free download Reliable ISO-IEC-27001-Lead-Auditor Dumps Free
- First-grade Pass ISO-IEC-27001-Lead-Auditor Test Guide – Pass ISO-IEC-27001-Lead-Auditor First Attempt The page for free download of [ISO-IEC-27001-Lead-Auditor] on www.pdfvce.com will open immediately Questions ISO-IEC-27001-Lead-Auditor Exam
- ISO-IEC-27001-Lead-Auditor Authorized Pdf Exam ISO-IEC-27001-Lead-Auditor Tutorial ISO-IEC-27001-Lead-Auditor Test Labs Open ➡ www.pass4leader.com enter ➡ ISO-IEC-27001-Lead-Auditor and obtain a free download ISO-IEC-27001-Lead-Auditor New Exam Camp
- PECB ISO-IEC-27001-Lead-Auditor Unparalleled Pass Test Guide Pass Guaranteed Immediately open www.pdfvce.com and search for ➡ ISO-IEC-27001-Lead-Auditor to obtain a free download Questions ISO-IEC-27001-Lead-Auditor Exam
- ISO-IEC-27001-Lead-Auditor Real Brain Dumps Exam ISO-IEC-27001-Lead-Auditor Tutorial 🏵 ISO-IEC-27001-Lead-Auditor Valid Test Objectives Download 《 ISO-IEC-27001-Lead-Auditor 》 for free by simply entering www.prep4away.com website ISO-IEC-27001-Lead-Auditor Test Simulator Online
- secureedges.com, 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, 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, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, myportal.utt.edu.tt, lifepass.site, lms.ait.edu.za, study.stcs.edu.np, www.eabook.cn, Disposable vapes

What's more, part of that ITExamDownload ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1SblE0vjCiPfyYm1ntfR0ymk2iEwAJU8k