

Latest ISO-IEC-27001-Lead-Auditor Exam Dumps Quiz Prep and preparation materials - DumpsKing



P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by DumpsKing:
https://drive.google.com/open?id=1k65KBMAhViD_zIDN3qOYZ6e_5Xwal8ht

Our website takes the lead in launching a set of test plan aiming at those office workers to get the ISO-IEC-27001-Lead-Auditor exam certification. We have organized a team to research and study question patterns pointing towards various learners. Our company keeps pace with contemporary talent development and makes every learners fit in the needs of the society. Based on advanced technological capabilities, our ISO-IEC-27001-Lead-Auditor Study Materials are beneficial for the masses of customers. Our experts have plenty of experience in meeting the requirement of our customers and try to deliver satisfied ISO-IEC-27001-Lead-Auditor exam guides to them.

PECB ISO-IEC-27001-Lead-Auditor (PECB Certified ISO/IEC 27001 Lead Auditor) Exam is an internationally recognized certification that attests to the competence of individuals in performing audits of information security management systems (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is issued by the Professional Evaluation and Certification Board (PECB), a global provider of training, examination, and certification services in various fields, including information security.

PECB ISO-IEC-27001-Lead-Auditor Exam is a rigorous and comprehensive assessment of a candidate's knowledge and skills in leading an ISMS audit team and conducting an audit according to the requirements of ISO/IEC 27001:2013 standard. It is a valuable certification for professionals who wish to advance their careers in information security management and auditing and demonstrate their expertise in the field.

>> **ISO-IEC-27001-Lead-Auditor Latest Exam Preparation** <<

Excellent PECB ISO-IEC-27001-Lead-Auditor Practice Material's 3 formats

With the high pass rate as 98% to 100%, we are confident to claim that our high quality and high efficiency of our ISO-IEC-27001-Lead-Auditor exam guide is unparalleled in the market. We provide the latest and exact ISO-IEC-27001-Lead-Auditor practice quiz to our customers and you will be grateful if you choose our ISO-IEC-27001-Lead-Auditor Study Materials and gain what you are expecting in the shortest time. Besides, you have the chance to experience the real exam in advance with the Software version of our ISO-IEC-27001-Lead-Auditor practice materials.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q215-Q220):

NEW QUESTION # 215

You are an experienced audit team leader guiding an auditor in training. Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site. Select four controls from the following that would you expect the auditor in training to review.

- A. How the organisation evaluates its exposure to technical vulnerabilities
- B. The organisation's arrangements for maintaining equipment
- C. How information security has been addressed within supplier agreements
- D. Confidentiality and nondisclosure agreements
- E. How access to source code and development tools are managed
- F. The organisation's arrangements for information deletion
- G. The development and maintenance of an information asset inventory
- H. The conducting of verification checks on personnel
- I. How power and data cables enter the building
- J. Rules for transferring information within the organisation and to other organisations
- K. The organisation's business continuity arrangements
- L. The operation of the site CCTV and door control systems
- M. Information security awareness, education and training
- N. Access to and from the loading bay
- O. How protection against malware is implemented
- P. Remote working arrangements

Answer: A,E,L,O

Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), an organization should select and implement appropriate controls to achieve its information security objectives¹. The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS¹. The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls². Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:

How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems². This control is related to control A.12.2.1 of ISO/IEC 27002:2013².

How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures². This control is related to control A.12.6.1 of ISO/IEC 27002:2013².

How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or systems that are developed or maintained by the organization or its external providers². This control is related to control A.14.2.5 of ISO/IEC 27002:2013².

The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed². This control is related to control A.11.1.4 of ISO/IEC 27002:2013².

The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance of an information asset inventory (related to control A.8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. Reference: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION # 216

In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is [b]not[/b] important for determining the value of data for an organization?

- A. The importance of the business processes that make use of the data.
- B. The degree to which missing, incomplete or incorrect data can be recovered.
- C. The indispensability of data for the business processes.

- D. The content of data.

Answer: D

NEW QUESTION # 217

You are an audit team leader who has just completed a third-party audit of a mobile telecommunication provider. You are preparing your audit report and are just about to complete a section headed 'confidentiality'.

An auditor in training on your team asks you if there are any circumstances under which the confidential report can be released to third parties.

Which four of the following responses are false?

- A. Our duty of confidentiality is not something that lasts forever. As a certification body, we can decide how long we wish to keep reports confidential. After this, they can be accessed by third parties making a subject access request
- B. Any auditor employed by the auditing organisation can access the audit report
- C. There are no circumstances under which the report can be released to a third party. Confidential means confidential and releasing the document would be a breach of trust
- D. The starting position is always that third parties have no automatic right to access an audit report
- E. If the third party has gained a legal notice for us to disclose the report then we must do so. In all such cases we would advise the audit client and, as appropriate, the auditee
- F. Although we advise the client the report is confidential we can decide to release it to third parties if we feel this is justified. We would always tell the client afterwards
- G. The report can be released to third parties but only with the explicit, prior approval of the audit client
- H. Subcontracted auditors are considered to be third parties regarding confidentiality and are therefore typically bound by confidentiality agreements

Answer: A,B,F,H

Explanation:

Explanation

The audit report is a confidential document that contains sensitive information about the auditee's ISMS and its performance. The audit team has a duty to protect the confidentiality of the audit report and only disclose it to authorized parties, such as the audit client, the certification body, and the accreditation body. Therefore, the following responses are false:

A: The audit team cannot decide to release the report to third parties without the consent of the audit client, as this would breach the confidentiality agreement and the audit code of conduct. The audit team should always inform the audit client before disclosing the report to any third party, and obtain their explicit, prior approval.

F: Not every auditor employed by the auditing organization can access the audit report, as this would violate the principle of need-to-know. Only auditors who are involved in the audit process, such as the audit team leader, the audit team members, the audit programme manager, and the certification decision maker, can access the audit report. Other auditors who are not related to the audit have no legitimate reason to access the report, and should be prevented from doing so by appropriate security measures.

G: The duty of confidentiality does not expire after a certain period of time, as this would compromise the trust and integrity of the audit process. The audit report remains confidential indefinitely, unless there is a legal or contractual obligation to disclose it, or the audit client agrees to release it. Third parties cannot access the audit report by making a subject access request, as this would infringe the privacy and data protection rights of the audit client and the auditee.

H: Subcontracted auditors are not considered to be third parties regarding confidentiality, as they are part of the audit team and have a contractual relationship with the auditing organization. Subcontracted auditors are typically bound by the same confidentiality agreement and audit code of conduct as the employed auditors, and have the same rights and responsibilities to access and protect the audit report.

References: =

ISO/IEC 27001:2022, clause 9.2, Internal audit

ISO/IEC 27006:2015, clause 7.2.3, Confidentiality

PECB Candidate Handbook ISO 27001 Lead Auditor, page 22, Audit Report

PECB Candidate Handbook ISO 27001 Lead Auditor, page 24, Audit Code of Conduct

NEW QUESTION # 218

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:

According to Scenario 6, Cyber ACrypt modified the SoA and the ISMS policy after the Stage 1 audit report. How do you define this situation?

- A. Unacceptable, once the external audit passes Stage 1, the SoA and the ISMS policy cannot be modified
- **B. Acceptable, situations that lead to major nonconformities during the Stage 2 audit should be corrected**
- C. Acceptable, minor modifications to the SoA and ISMS policy can be made until the submission of the final audit report

Answer: B

Explanation:

Comprehensive and Detailed In-Depth

B . Correct Answer:

Stage 1 audits identify gaps and allow the organization to correct major nonconformities before Stage 2 certification.

ISO/IEC 27006 requires organizations to address major nonconformities before proceeding to Stage 2.

A . Incorrect:

Organizations are allowed to correct nonconformities identified in Stage 1.

C . Incorrect:

Major changes must be addressed, not just minor modifications.

Relevant Standard Reference:

ISO/IEC 27006:2020 Clause 9.2.3 (Stage 1 and Stage 2 Audit Process)

NEW QUESTION # 219

OrgXY is an ISO/IEC 27001-certified software development company. A year after being certified, OrgXY's top management informed the certification body that the company was not ready for conducting the surveillance audit. What happens in this case?

- A. OrgXY transfers its registration to another certification body
- B. The current certification is used until the next surveillance audit
- **C. The certification is suspended**

Answer: C

Explanation:

If an organization like OrgXY informs the certification body that it is not ready to conduct the surveillance audit as scheduled, the certification may be suspended. This is because the surveillance audit is a critical part of the ongoing certification maintenance, required to ensure continued compliance with the standard.

NEW QUESTION # 220

.....

Cracking the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam brings high-paying jobs, promotions, and validation of talent. Dozens of PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam applicants don't get passing scores in the real ISO-IEC-27001-Lead-Auditor exam because of using invalid PECB ISO-IEC-27001-Lead-Auditor exam dumps. Failure in the ISO-IEC-27001-Lead-Auditor Exam leads to a loss of time, money, and confidence. If you are an applicant for the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam, you can prevent these losses by using the latest real ISO-IEC-27001-Lead-Auditor exam questions of DumpsKing.

ISO-IEC-27001-Lead-Auditor Real Sheets: <https://www.dumpsking.com/ISO-IEC-27001-Lead-Auditor-testking-dumps.html>

- 2026 PECB Efficient ISO-IEC-27001-Lead-Auditor Latest Exam Preparation □ Search for ▷ ISO-IEC-27001-Lead-Auditor ◁ and download exam materials for free through ⇒ www.testkingpass.com ⇐ □ Latest ISO-IEC-27001-Lead-Auditor Test Online
- 2026 PECB Efficient ISO-IEC-27001-Lead-Auditor Latest Exam Preparation □ Search for ▶ ISO-IEC-27001-Lead-Auditor ◀ and download exam materials for free through ➡ www.pdfvce.com □ □ Valid ISO-IEC-27001-Lead-Auditor Test Pdf
- 2026 ISO-IEC-27001-Lead-Auditor Latest Exam Preparation 100% Pass | High Pass-Rate PECB PECB Certified ISO/IEC 27001 Lead Auditor exam Real Sheets Pass for sure □ The page for free download of ▷ ISO-IEC-27001-Lead-Auditor ◁ on ➡ www.exam4labs.com □ will open immediately □ ISO-IEC-27001-Lead-Auditor Regular Update
- Prepare for ISO-IEC-27001-Lead-Auditor with PECB's Realistic Exam Questions and Get Accurate Answers □ Open ➡ www.pdfvce.com □ and search for (ISO-IEC-27001-Lead-Auditor) to download exam materials for free □ □ Latest Braindumps ISO-IEC-27001-Lead-Auditor Ppt
- PECB ISO-IEC-27001-Lead-Auditor Online Practice Test (PECB-ISO-IEC-27001-Lead-Auditor-Practice-Test) □ Go to website ▶ www.vceengine.com ◀ open and search for (ISO-IEC-27001-Lead-Auditor) to download for free □ □ Latest ISO-IEC-27001-Lead-Auditor Exam Pattern
- Valid ISO-IEC-27001-Lead-Auditor Exam Question □ ISO-IEC-27001-Lead-Auditor Regular Update □ New Study ISO-IEC-27001-Lead-Auditor Questions □ Enter ☀ www.pdfvce.com □ ☀ □ and search for ➡ ISO-IEC-27001-Lead-Auditor □ to download for free □ New ISO-IEC-27001-Lead-Auditor Test Syllabus
- ISO-IEC-27001-Lead-Auditor Valid Exam Materials □ Valid ISO-IEC-27001-Lead-Auditor Test Pdf □ ISO-IEC-27001-Lead-Auditor Valid Exam Materials □ Easily obtain free download of □ ISO-IEC-27001-Lead-Auditor □ by searching on ☀ www.testkingpass.com □ ☀ □ □ ISO-IEC-27001-Lead-Auditor Latest Exam Forum
- Help You in PECB ISO-IEC-27001-Lead-Auditor Exam Preparation [2026] ♥ Open { www.pdfvce.com } and search for □ ISO-IEC-27001-Lead-Auditor □ to download exam materials for free □ Associate ISO-IEC-27001-Lead-Auditor Level Exam
- Prepare for ISO-IEC-27001-Lead-Auditor with PECB's Realistic Exam Questions and Get Accurate Answers □ Enter ➡ www.practicevce.com □ and search for 「 ISO-IEC-27001-Lead-Auditor 」 to download for free □ ISO-IEC-27001-Lead-Auditor Latest Exam Forum
- Associate ISO-IEC-27001-Lead-Auditor Level Exam □ ISO-IEC-27001-Lead-Auditor Dump Torrent □ Certification ISO-IEC-27001-Lead-Auditor Torrent □ Search on 「 www.pdfvce.com 」 for ➡ ISO-IEC-27001-Lead-Auditor □ to obtain exam materials for free download □ ISO-IEC-27001-Lead-Auditor Valid Braindumps Files
- PECB ISO-IEC-27001-Lead-Auditor Online Practice Test (PECB-ISO-IEC-27001-Lead-Auditor-Practice-Test) □ Simply search for ➡ ISO-IEC-27001-Lead-Auditor □ □ for free download on ➡ www.vce4dumps.com □ □ Valid ISO-IEC-27001-Lead-Auditor Exam Question
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.hggz.com, writeablog.net, sahuwebgrowmaster.online, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, sconline.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that DumpsKing ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1k65KBMAhViD_zlDN3qOYZ6e_5Xwal8ht