Pass Guaranteed 2026 PECB Marvelous ISO-IEC-27001-Lead-Auditor: Exam PECB Certified ISO/IEC 27001 Lead Auditor exam Study Guide

P.S. Free 2026 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1BeWTaSByM3ZUL-IwpBhCVhtvKxejwdyr

You can conveniently test your performance by checking your score each time you use our PECB ISO-IEC-27001-Lead-Auditor practice exam software (desktop and web-based). It is heartening to announce that all Dumpkiller users will be allowed to capitalize on a free PECB ISO-IEC-27001-Lead-Auditor Exam Questions demo of all three formats of the PECB ISO-IEC-27001-Lead-Auditor practice test.

The PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam assesses the candidate's understanding of the ISO/IEC 27001 standard, its requirements, and the best practices for implementing and maintaining an ISMS. It also evaluates the candidate's ability to plan, conduct, report, and follow-up on an audit. ISO-IEC-27001-Lead-Auditor Exam covers topics such as risk management, incident management, asset management, and compliance with legal and regulatory requirements.

>> Exam ISO-IEC-27001-Lead-Auditor Study Guide <<

ISO-IEC-27001-Lead-Auditor Brain Exam - ISO-IEC-27001-Lead-Auditor Test Simulator Free

Our company is your ally in achieving your targeted certification, providing you easy and interactive ISO-IEC-27001-Lead-Auditor exam braindumps. You can totally count on us as we are good at help you get the success on your coming exam. We will always stand by your on your way for the certification as we work as 24/7 online. If you have any question, you can find help from us on the ISO-IEC-27001-Lead-Auditor Study Guide. And our ISO-IEC-27001-Lead-Auditor learning questions are well-written to be understood by the customers all over the world.

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.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q137-Q142):

NEW QUESTION # 137

Which two of the following actions are the individual(s) managing the audit programme responsible for?

- A. Defining the plan of an individual audit
- B. Keping informed the accreditation body on the progress of the audit programme
- C. Determining the resources necessary for the audit programme
- D. Communicating with the auditee during the audit
- E. Defining the objectives, scope and criteria for an individual audit
- F. Determining the legal requirements applicable to each audit

Answer: B,C

Explanation:
Establishing the audit programme objectives, scope and criteria
Determining the resources necessary for the audit programme, such as the audit team members, the budget, the time, the tools, etc.
Selecting and appointing the audit team leaders and auditors
Reviewing and approving the audit plans and arrangements
Ensuring the effective communication and coordination among the audit programme stakeholders, such as the auditors, the auditees, the certification bodies, the accreditation bodies, etc.
Keeping informed the accreditation body on the progress of the audit programme, especially in case of any significant changes, issues, or nonconformities Monitoring and reviewing the performance and results of the audit programme and the audit teams Evaluating the feedback and satisfaction of the auditees and other interested parties Identifying and implementing the opportunities for improvement of the audit programme The individual(s) managing the audit programme are not responsible for the following tasks, which are delegated to the audit team leaders or the auditors12:
Communicating with the auditee during the audit, such as conducting the opening and closing meetings, resolving any audit-related problems, reporting any audit findings, etc.
Determining the legal requirements applicable to each audit, such as the confidentiality, the impartiality, the consent, the liability, etc.
Defining the objectives, scope and criteria for an individual audit, which are derived from the audit programme and agreed with the auditee Defining the plan of an individual audit, which includes the audit schedule, the audit activities, the audit methods, the audit documents, etc.
References:
ISO 19011:2018 - Guidelines for auditing management systems
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-20

NEW QUESTION # 138
You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.
You are currently in a large room that is subdivided into several smaller rooms, each of which has a numeric combination lock and swipe card reader on the door. You notice two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorised electrical repairs.
You go to reception and ask to see the door access record for the client's suite. This indicates only one card was swiped. You ask the receptionist and they reply, "yes it's a common problem. We ask everyone to swipe their cards but with contractors especially, one tends to swipe and the rest simply 'tailgate' their way in" but we know who they are from the reception sign-in.
Based on the scenario above which one of the following actions would you now take?

- A. Tell the organisation they must write to their contractors, reminding them of the need to use access cards appropriately
- B. Raise a nonconformity against control A.7.2 'physical entry' as a secure area is not adequately protected
- C. Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier
- D. Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times
- E. Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities
- F. Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV
- G. Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined
- H. Take no action. Irrespective of any recommendations, contractors will always act in this way

Answer: B

Explanation:
Explanation

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), control A.7.2 requires an organization to implement appropriate physical entry controls to prevent unauthorized access to secure areas1. The organization should define and document the criteria for granting and revoking access rights to secure areas, and should monitor and record the use of such access rights1. Therefore, when auditing the organization's application of control A.7.2, an ISMS auditor should verify that these aspects are met in accordance with the audit criteria.

Based on the scenario above, the auditor should raise a nonconformity against control A.7.2, as the secure area is not adequately protected from unauthorized access. The auditor should provide the following evidence and justification for the nonconformity:

* Evidence: The auditor observed two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorized electrical repairs. The auditor checked the door access record for the client's suite and found that only one card was swiped. The auditor asked the receptionist and was told that it was a common problem that contractors tend to swipe one card and tailgate their way in, but they were known from the reception sign-in.
* Justification: This evidence indicates that the organization has not implemented appropriate physical entry controls to prevent unauthorized access to secure areas, as required by control A.7.2. The organization has not defined and documented the criteria for granting and revoking access rights to secure areas, as there is no verification or authorization process for providing swipe cards and combination numbers to external contractors. The organization has not monitored and recorded the use of access rights to secure areas, as there is no mechanism to ensure that each individual swipes their card and enters their combination number before entering a secure area. The organization has relied on the reception sign-in as a means of identification, which is not sufficient or reliable for ensuring information security.

The other options are not valid actions for auditing control A.7.2, as they are not related to the control or its requirements, or they are not appropriate or effective for addressing the nonconformity. For example:

* Take no action: This option is not valid because it implies that the auditor ignores or accepts the nonconformity, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems.
* Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not supplier relationships. Control A.5.20 requires an organization to agree on information security requirements with suppliers that may access, process, store, communicate or provide IT infrastructure components for its information assets1. While this control may be relevant for ensuring information security in supplier relationships, it does not address the issue of unauthorized access to secure areas by external contractors.
* Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not working in secure areas. Control A.7.6 requires an organization to define and apply security measures for working in secure areas1.
* While this control may be relevant for ensuring information security when working in secure areas, it does not address the issue of unauthorized access to secure areas by external contractors.
* Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV: This option is not valid because it does not address or resolve the nonconformity, but rather attempts to find alternative or compensating controls that may mitigate its impact or likelihood. While additional arrangements such as CCTV may be useful for verifying individual access to secure areas, they do not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may prevent or reduce its recurrence or severity.

While accompanying contractors at all times when accessing secure facilities may be a good practice for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.

* Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may increase awareness or compliance with the existing controls. While having a large sign in reception reminding everyone requiring access must use their swipe card at all times may be a helpful reminder for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Tell the organisation they must write to their contractors, reminding them of the need to use access cards appropriately: This option is not valid because it does not address or resolve the nonconformity, but rather instructs the organization to take a corrective action that may not be effective or sufficient for ensuring information security. While writing to contractors, reminding them of the need to use access cards appropriately may be a communication measure for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.

References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION # 139

Which one of the following options is the definition of an interested party?

- A. An individual or organisation that can control, be controlled by, or perceive itself to be controlled by a decision or activity
- B. A person or organisation that can affect, be affected by or perceive itself to be affected by a decision or activity
- C. A group or organisation that can interfere in or perceive itself to be interfered with by a management decision
- D. A third party can appeal to an organisation when it perceives itself to be affected by a decision or activity

Answer: B

Explanation:
This is the definition of an interested party according to ISO 27001:2013, clause 3.16. An interested party is essentially a stakeholder, i.e., a person or organization that can influence or be influenced by the information security management system (ISMS) or its activities. Interested parties can have different needs and expectations regarding the ISMS, and these should be identified and addressed by the organization.
References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.16
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* Identifying interested parties and their expectations for an ISO 27001 ISMS
* Examples of ISO 27001 interested parties

NEW QUESTION # 140
You receive the following mail from the IT support team: Dear User,Starting next week, we will be deleting all inactive email accounts in order to create spaceshare the below details in order to continue using your account. In case of no response, Name:
Email ID:
Password:
DOB:
Kindly contact the webmail team for any further support. Thanks for your attention.
Which of the following is the best response?

- A. One should not respond to these mails and report such email to your supervisor
- B. Ignore the email
- C. Respond it by saying that one should not share the password with anyone

Answer: A

Explanation:
The best response to the email from the IT support team asking for personal details is to not respond to the email and report it to your supervisor. The email is likely a phishing attempt, which is a form of social engineering that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information.
The IT support team should never ask for your password or other personal details via email, as this is a violation of information security policies and best practices. Ignoring the email or responding to it by saying that one should not share the password with anyone are not sufficient responses, as they do not alert the IT support team or your supervisor about the phishing attempt, which could affect other users as well. Reporting the email to your supervisor is a responsible action that could help prevent further damage or compromise of information. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2).
References: 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 Phishing?

NEW QUESTION # 141
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:
According to scenario 8, the audit team evaluated the action plan and concluded that it would resolve the detected nonconformities. Is this acceptable?

- A. Yes. the audit team must evaluate the action plan and verify if it is appropriate for correcting the detected nonconformities
- B. Yes, only if EsBank has previously verified the effectiveness of the action plan and informed the audit team that the action plan allows the correction of nonconformities
- C. No, the auditee should verify if the action plan allows the correction of nonconformities and elimination of the root causes

Answer: A

Explanation:
Yes, the audit team must evaluate the action plan and verify if it is appropriate for correcting the detected nonconformities. This is part of the auditor's responsibilities to ensure that the proposed actions adequately address the issues identified during the audit.

NEW QUESTION # 142
.....

download for free □Latest ISO-IEC-27001-Lead-Auditor Exam Topics

- ISO-IEC-27001-Lead-Auditor Updated Torrent - ISO-IEC-27001-Lead-Auditor Valid Practice - ISO-IEC-27001-Lead-Auditor Test Engine □ Simply search for ⇛ ISO-IEC-27001-Lead-Auditor ⇚ for free download on 「 www.pdfvce.com 」 □ISO-IEC-27001-Lead-Auditor Vce Torrent
- Free PDF Authoritative PECB - Exam ISO-IEC-27001-Lead-Auditor Study Guide □ Open □ www.pass4test.com □ and search for { ISO-IEC-27001-Lead-Auditor } to download exam materials for free □New Study ISO-IEC-27001-Lead-Auditor Questions
- Composite Test ISO-IEC-27001-Lead-Auditor Price □ Valid ISO-IEC-27001-Lead-Auditor Learning Materials □ Latest ISO-IEC-27001-Lead-Auditor Exam Topics □ Copy URL □ www.pdfvce.com □ open and search for ➠ ISO-IEC-27001-Lead-Auditor □ to download for free □ISO-IEC-27001-Lead-Auditor Latest Exam Simulator
- Valid ISO-IEC-27001-Lead-Auditor Learning Materials □ Passing ISO-IEC-27001-Lead-Auditor Score ✔□ Latest ISO-IEC-27001-Lead-Auditor Braindumps Questions □ Search for □ ISO-IEC-27001-Lead-Auditor □ on [www.verifieddumps.com] immediately to obtain a free download □ISO-IEC-27001-Lead-Auditor Vce Torrent
- www.stes.tyc.edu.tw, cpfcordoba.com, www.stes.tyc.edu.tw, www.klemminghundar.se, bbs.t-firefly.com, www.stes.tyc.edu.tw, english101.site, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest Dumpkiller ISO-IEC-27001-Lead-Auditor PDF Dumps and ISO-IEC-27001-Lead-Auditor Exam Engine Free Share: https://drive.google.com/open?id=1BeWTaSByM3ZUL-IwpBhCVhtvKxejwdyr