PECB ISO-IEC-27001-Lead-Auditor Books PDF, New ISO-IEC-27001-Lead-Auditor Mock Test

What's more, part of that VCEPrep ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1AINM4rq5SCmk8dJloOXf4RvuSwrgCdzs

To provide our users with the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) latest questions based on the sections of the actual exam quesions, we regularly update our ISO-IEC-27001-Lead-Auditor study material. Also, VCEPrep provides free updates of PECB ISO-IEC-27001-Lead-Auditor Exam Questions for up to 365 days. For customers who don't crack the PECB ISO-IEC-27001-Lead-Auditor test after using our product, VCEPrep will provides them a refund guarantee according to terms and conditions.

PECB ISO-IEC-27001-Lead-Auditor certification exam is designed for professionals who wish to become certified as ISO/IEC 27001 Lead Auditors. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is globally recognized and demonstrates an individual's expertise in auditing information security management systems (ISMS) based on the ISO/IEC 27001 standard. ISO-IEC-27001-Lead-Auditor Exam covers various topics such as auditing principles, techniques, and best practices, as well as risk management and information security controls.

>> PECB ISO-IEC-27001-Lead-Auditor Books PDF <<

PECB ISO-IEC-27001-Lead-Auditor Books PDF Spend Your Little Time and Energy to Pass ISO-IEC-27001-Lead-Auditor exam

The ISO-IEC-27001-Lead-Auditor exam questions are being offered in three different formats. The names of these formats are PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) desktop practice test software, web-based practice test software, and PDF dumps file. The PECB desktop practice test software and web-based practice test software both give you real-time PECB ISO-IEC-27001-Lead-Auditor Exam environment for quick and complete exam preparation.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q270-Q275):

NEW QUESTION # 270
Scenario 3: NightCore is a multinational technology company based in the United States that focuses on e-commerce, cloud computing, digital streaming, and artificial intelligence. After having an information security management system (ISMS) implemented for over 8 months, they contracted a certification body to conduct a third party audit in order to get certified against ISO/IEC 27001.
The certification body set up a team of seven auditors. Jack, the most experienced auditor, was assigned as the audit team leader. Over the years, he received many well known certifications, such as the ISO/IEC 27001 Lead Auditor, CISA, CISSP, and CISM. Jack conducted thorough analyses on each phase of the ISMS audit, by studying and evaluating every information security requirement and control that was implemented by NightCore. During stage 2 audit. Jack detected several nonconformities. After

comparing the number of purchased invoices for software licenses with the software inventory, Jack found out that the company has been using the illegal versions of a software for many computers. He decided to ask for an explanation from the top management about this nonconformity and see whether they were aware about this. His next step was to audit NightCore's IT Department. The top management assigned Tom, NightCore's system administrator, to act as a guide and accompany Jack and the audit team toward the inner workings of their system and their digital assets infrastructure.
While interviewing a member of the Department of Finance, the auditors discovered that the company had recently made some unusual large transactions to one of their consultants. After gathering all the necessary details regarding the transactions. Jack decided to directly interview the top management.
When discussing about the first nonconformity, the top management told Jack that they willingly decided to use a copied software over the original one since it was cheaper. Jack explained to the top management of NightCore that using illegal versions of software is against the requirements of ISO/IEC 27001 and the national laws and regulations. However, they seemed to be fine with it.
Several months after the audit, Jack sold some of NightCore's information that he collected during the audit for a huge amount of money to competitors of NightCore.
Based on this scenario, answer the following question:
Does ISO/IEC 27001 require organizations to comply with national laws and regulations?

- A. Yes, complying with the applicable legislation is a requirement of ISO/IEC 27001
- B. Yes, but relevant legal and contractual requirements do not need to be explicitly identified
- C. No, there is no clear indication in the standard as to whether the organization should comply with the national laws and regulations

Answer: A

Explanation:
ISO/IEC 27001 requires organizations to comply with applicable legal, statutory, regulatory, and contractual requirements, including those pertaining to information security. These requirements must be identified, documented, and kept up to date as part of the organization's ISMS.

NEW QUESTION # 271
You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

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*

Select one option of the recommendation to the audit programme manager you are going to advise to the auditee at the closing meeting.

- A. Recommend that an unannounced audit is carried out at a future date
- B. Recommend certification after your approval of the proposed corrective action plan Recommend that the findings can be closed out at a surveillance audit in 1 year
- C. Recommend that a partial audit is required within 3 months
- D. Recommend certification immediately
- E. Recommend that a full scope re-audit is required within 6 months

Answer: B

Explanation:
According to ISO/IEC 17021-1:2015, which specifies the requirements for bodies providing audit and certification of management systems, clause 9.4.9 requires the certification body to make a certification decision based on the information obtained during the audit and any other relevant information1. The certification body should also consider the effectiveness of the corrective actions taken by the auditee to address any nonconformities identified during the audit1. Therefore, when making a recommendation to the audit programme manager, an ISMS auditor should consider the nature and severity of the nonconformities and the proposed corrective actions.
Based on the scenario above, the auditor should recommend certification after their approval of the proposed corrective action plan and recommend that the findings can be closed out at a surveillance audit in 1 year. The auditor should provide the following justification for their recommendation:
* Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:
* Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.
* Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.
* Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.
* Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.
References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION # 272
The data center at which you work is currently seeking ISO/IEC27001:2022 certification. In preparation for your initial certification visit a number of internal audits have been carried out by a colleague working at another data centre within your Group. They secured their ISO/IEC 27001:2022 certificate earlier in the year.
You have just qualified as an Internal ISMS auditor and your manager has asked you to review the audit process and audit findings as a final check before the external Certrfication Body arrives.
Which six of the following would cause you concern in respect of conformity to ISO/IEC 27001:2022 requirements?

- A. The audit programme does not reference audit methods or audit responsibilities
- B. The audit programme shows management reviews taking place at irregular intervals during the year
- C. The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022
- D. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet
- E. Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme
- F. The audit programme does not take into account the results of previous audits
- G. Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes
- H. The audit programme does not take into account the relative importance of information security processes
- I. Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date
- J. The audit process states the results of audits will be made available to 'relevant' managers, not top management

Answer: B,E,F,G,H,I

Explanation:
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 9.3 requires top management to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness1. Clause 9.2 requires the organization to conduct internal audits at planned intervals to provide information on whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022, and is effectively implemented and maintained1. Therefore, when reviewing the audit process and audit findings as a final check before the external certification body arrives, an internal ISMS auditor should verify that these clauses are met in accordance with the audit criteria.

Six of the following statements would cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
The audit programme shows management reviews taking place at irregular intervals during the year: This statement would cause concern because it implies that the organization is not conducting management reviews at planned intervals, as required by clause 9.3. This may affect the ability of top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS.
The audit programme does not take into account the relative importance of information security processes: This statement would cause concern because it implies that the organization is not applying a risk-based approach to determine the audit frequency, methods, scope and criteria, as recommended by ISO 19011:2018, which provides guidelines for auditing management systems2. This may affect the ability of the organization to identify and address the most significant risks and opportunities for its ISMS.
Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date: This statement would cause concern because it implies that the organization is not establishing audit criteria for each internal audit, as required by clause 9.2. Audit criteria are the set of policies, procedures or requirements used as a reference against which audit evidence is compared2. Without audit criteria, it is not possible to determine whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022.
Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes: This statement would cause concern because it implies that the organization is not evaluating the effectiveness of ISMS processes, as required by clause 9.1. Effectiveness is the extent to which planned activities are realized and planned results achieved2. Efficiency is the relationship between the result achieved and the resources used2. Both aspects are important for measuring and evaluating ISMS performance and improvement.
The audit programme does not take into account the results of previous audits: This statement would cause concern because it implies that the organization is not using the results of previous audits as an input for planning and conducting subsequent audits, as recommended by ISO 19011:20182. This may affect the ability of the organization to identify and address any recurring or unresolved issues or nonconformities related to its ISMS.
Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme: This statement would cause concern because it implies that the organization is not verifying that top management demonstrates leadership and commitment with respect to its ISMS, as required by clause 5.1. This may affect the ability of top management to ensure that the ISMS policy and objectives are established and compatible with the strategic direction of the organization; that roles, responsibilities and authorities for relevant roles are assigned and communicated; that resources needed for the ISMS are available; that communication about information security matters is established; that continual improvement of the ISMS is promoted; that other relevant management reviews are aligned with those of information security; and that support is provided to other relevant roles1.
The other statements would not cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific format or media for documenting or storing audit reports, as long as they are controlled according to clause 7.5.
The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for auditor independence, as long as the audit is conducted objectively and impartially, in accordance with ISO 19011:20182.
The audit programme does not reference audit methods or audit responsibilities: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for referencing audit methods or audit responsibilities in the audit programme, as long as they are defined and documented according to ISO 19011:20182.
The audit process states the results of audits will be made available to 'relevant' managers, not top management: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for communicating the results of audits to top management, as long as they are reported to the relevant parties and used as an input for management review, according to clause 9.3.

NEW QUESTION # 273
Which two of the following phrases would apply to "plan" in relation to the Plan-Do-Check-Act cycle for a business process?

- A. Retaining documentation
- B. Setting objectives
- C. Training staff
- D. Organising changes
- E. Providing ICT assets
- F. Retaining documentation

Answer: B,C

Explanation:

The Plan-Do-Check-Act (PDCA) cycle is a four-step method for implementing and improving processes, products, or services. The "plan" phase involves establishing the objectives and processes necessary to deliver the desired results. This may include setting SMART goals, identifying resources, defining roles and responsibilities, conducting risk assessments, and developing plans for training, communication, and monitoring.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION # 274
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?

- A. Verification should focus on whether any action undertaken is complete
- B. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
- C. Verification should focus on whether any action undertaken taken has been undertaken efficiently
- D. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
- E. Verification should focus on whether any action undertaken has been undertaken effectively
- F. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions

Answer: A,E

Explanation:
Explanation
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence.
The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12 Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12 Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 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 # 275

......

Our ISO-IEC-27001-Lead-Auditor exam torrent is compiled by first-rank experts with a good command of professional knowledge, and our experts adept at this exam practice materials area over ten years' long, so they are terrible clever about this thing. They exert great effort to boost the quality and accuracy of our ISO-IEC-27001-Lead-Auditor study tools and is willing to work hard as well as willing to do their part in this area. The wording is fully approved in our ISO-IEC-27001-Lead-Auditor Exam Guide. They handpicked what the ISO-IEC-27001-Lead-Auditor exam torrent usually tests in exam recent years and devoted their knowledge accumulated into these ISO-IEC-27001-Lead-Auditor study tools. Besides, they keep the quality and content according to the trend of the ISO-IEC-27001-Lead-Auditor practice exam. As approved ISO-IEC-27001-Lead-Auditor exam guide from professional experts their quality is unquestionable.

New ISO-IEC-27001-Lead-Auditor Mock Test: https://www.vceprep.com/ISO-IEC-27001-Lead-Auditor-latest-vce-prep.html

P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by VCEPrep: https://drive.google.com/open?id=1AINM4rq5SCmk8dJloOXf4RvuSwrgCdzs