Reliable ISO-IEC-27001-Lead-Auditor Exam Registration - Latest Braindumps ISO-IEC-27001-Lead-Auditor Book

P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by Exam4Tests: https://drive.google.com/open?id=1bHs9qMOH9np1ZVu8kkRoIlzXh9C4pccy

Exam4Tests is a trusted and reliable platform that has been helping ISO-IEC-27001-Lead-Auditor exam candidates for many years. Over this long time period countless PECB ISO-IEC-27001-Lead-Auditor exam questions candidates have passed their dream ISO-IEC-27001-Lead-Auditor certification exam. They all got help from PECB Exam Questions and easily passed their challenging ISO-IEC-27001-Lead-Auditor PDF exam. You can also trust top-notch PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam questions and start preparation with complete peace of mind and satisfaction.

Our company Exam4Tests is glad to provide customers with authoritative study platform. Our ISO-IEC-27001-Lead-Auditor quiz torrent was designed by a lot of experts and professors in different area in the rapid development world. At the same time, if you have any question on our ISO-IEC-27001-Lead-Auditor exam questions, we can be sure that your question will be answered by our professional personal in a short time. In a word, if you choose to buy our ISO-IEC-27001-Lead-Auditor Quiz torrent, you will have the chance to enjoy the authoritative study platform provided by our company.

>> Reliable ISO-IEC-27001-Lead-Auditor Exam Registration <<

Pass Guaranteed ISO-IEC-27001-Lead-Auditor - Perfect Reliable PECB Certified ISO/IEC 27001 Lead Auditor exam Exam Registration

The second format of PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) is the web-based practice exam that can be taken online through browsers like Firefox, Chrome, Safari, MS Edge, Internet Explorer, and Microsoft Edge. You don't need to install any excessive plugins or Software to attempt the web-based Practice ISO-IEC-27001-Lead-Auditor Exam. All operating systems also support the web-based practice exam.

PECB ISO-IEC-27001-Lead-Auditor Exam is intended for individuals who have already completed a lead auditor training program, or who have significant experience in the field of information security management. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is recognized worldwide and is highly valued by employers in the information security industry.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q128-Q133):

NEW QUESTION # 128

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. Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes
- C. The audit programme does not take into account the results of previous audits
- D. The audit process states the results of audits will be made available to 'relevant' managers, not top management
- E. The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022
- F. The audit programme does not take into account the relative importance of information security processes
- G. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet
- H. The audit programme shows management reviews taking place at irregular intervals during the year
- 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. Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme

Answer: B,C,F,H,I,J

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

NEW QUESTION # 129
Which of the following statements regarding documented information in an organization's ISMS is incorrect?

- A. The collection of documented information should be a target in itself
- B. Documented information should not be detailed and complex to ensure thoroughness
- C. The purpose of documented information is to guide the ISMS operation and provide evidence of process effectiveness

Answer: A

Explanation:
Comprehensive and Detailed In-Depth
ISO/IEC 27001:2022 Clause 7.5 (Documented Information) defines the role of documentation in an ISMS.
A . Correct Statement:
Documented information serves as a guideline for ISMS operations and provides audit evidence.
B . Incorrect Statement:
Collecting documented information is not a goal in itself.
The purpose of documentation is to support the ISMS and ensure compliance, not just to generate paperwork.
C . Correct Statement:
Documents should be clear and concise, avoiding unnecessary complexity while still being detailed enough to be useful.
Thus, documentation should be purposeful and functional, not just a bureaucratic requirement.
Relevant Standard Reference:

NEW QUESTION # 130
You are an experienced ISMS audit team leader conducting a third-party surveillance audit of an internet services provider. You are reviewing the organization's risk assessment processes for conformity with ISO/IEC 27001:2022.
Which three of the following audit findings would prompt you to raise a nonconformity report?

- A. The organisation has not used RAG (Red, Amber, Green) to classify its' information security risks. Instead, it has used a smiling emoji, a neutral face emoji and a sad face emoji
- B. The organisation is treating information security risks in the order in which they are identified
- C. The organisation's risk assessment criteria have not been reviewed and approved by top management
- D. Both systems contain additional information security risks which are not associated with preserving the confidentiality, integrity and accessibility of information
- E. There is a different system in place for assessing operational information security risks and for assessing strategic information security risks

- F. The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
- G. The organisation's information security risk assessment process suggests each risk is allocated a risk owner
- H. The organisation has assessed the probability of all of its information security risks as either 0%, 25%, 50%, 75% or 100%

Answer: B,C,F

Explanation:
The three audit findings that would prompt you to raise a nonconformity report are:
* The organisation is treating information security risks in the order in which they are identified
* The organisation's risk assessment criteria have not been reviewed and approved by top management
* The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
According to ISO/IEC 27001:2022, clause 6.1.2, the organisation must establish and maintain an information security risk management process that is consistent with the organisation's context and aligned with its overall risk management approach1. This process must include the following steps:
* Establishing the risk assessment criteria, which must be approved by top management and reflect the organisation's risk appetite and objectives2
* Identifying the information security risks, which must consider the assets, threats, vulnerabilities, impacts, and likelihoods3
* Analysing the information security risks, which must determine the levels of risk and compare them with the risk criteria4
* Evaluating the information security risks, which must prioritise the risks and decide whether they need treatment or not5 Therefore, the audit findings B, E, and F indicate that the organisation is not following the required steps of the information security risk management process, and thus are nonconformities with the standard.
The other audit findings are not necessarily nonconformities, as they may be acceptable depending on the organisation's context and justification. For example:
* Audit finding A may be acceptable if the organisation has identified and treated the additional information security risks that are relevant to its scope and objectives, and has documented the rationale for doing so6
* Audit finding C may be acceptable if the organisation has assigned clear roles and responsibilities for the information security risk management process, and has ensured that the risk owners have the authority and competence to manage the risks7
* Audit finding D may be acceptable if the organisation has defined and communicated the meaning and implications of the emoji-based risk classification, and has ensured that it is consistent with the risk criteria and the risk treatment process8
* Audit finding G may be acceptable if the organisation has justified the use of discrete values for the probability of the information security risks, and has ensured that they are realistic and consistent with the risk criteria and the risk analysis method9
* Audit finding H may be acceptable if the organisation has established and maintained different systems for assessing operational and strategic information security risks, and has ensured that they are integrated and aligned with the overall risk management approach and the ISMS objectives10

NEW QUESTION # 131
What is the worst possible action that an employee may receive for sharing his or her password or access with others?

- A. The lowest rating on his or her performance assessment
- B. Termination
- C. Forced roll off from the project
- D. Three days suspension from work

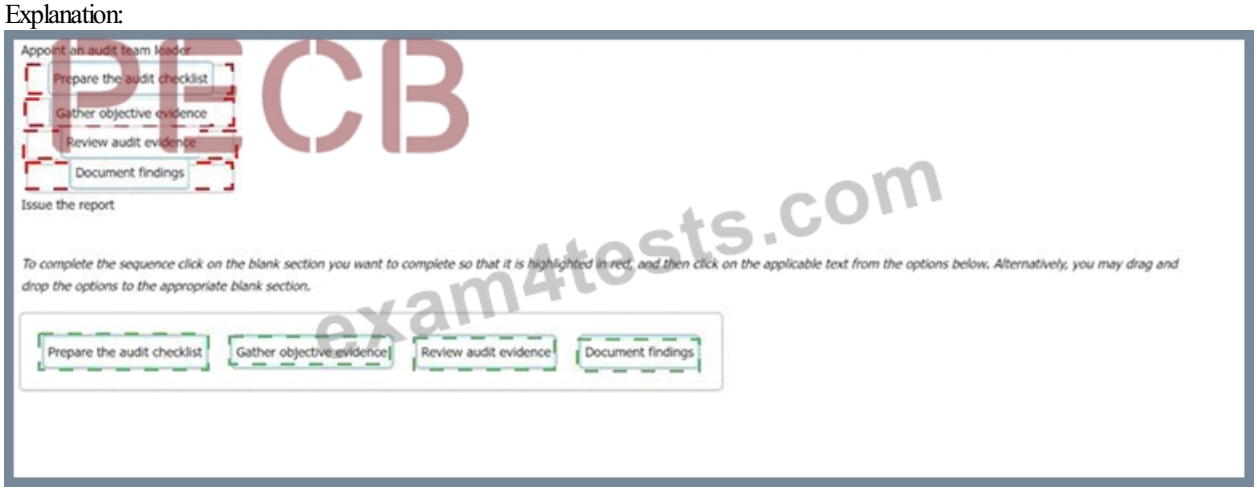
Answer: B

Explanation:
The worst possible action that an employee may receive for sharing his or her password or access with others is termination, because this is a serious breach of the organization's information security policy and access control policy. Sharing password or access with others may allow unauthorized users to access sensitive or confidential information, or to perform malicious or fraudulent activities on behalf of the employee. The employee should keep his or her password or access confidential and secure, and should not disclose it to anyone under any circumstances. Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], [ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements], Example of an information security policy, Example of an access control policy

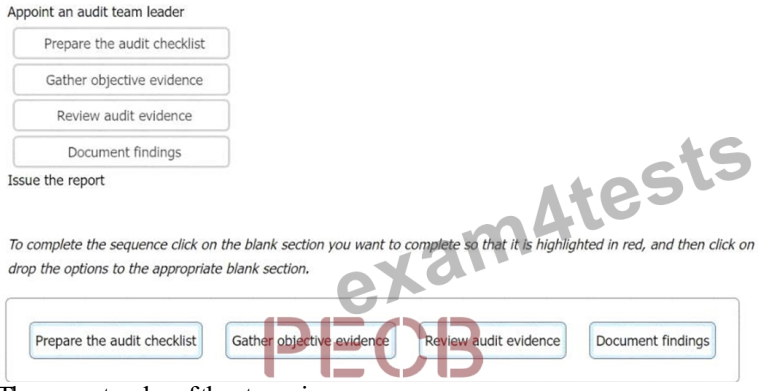
NEW QUESTION # 132
The following options are key actions involved in a first-party audit. Order the stages to show the sequence in which the actions should take place.

Answer:

Explanation:



Explanation



The correct order of the stages is:
Prepare the audit checklist
Gather objective evidence
Review audit evidence
Document findings
Audit preparation: This stage involves defining the audit objectives, scope, criteria, and plan. The auditor also prepares the audit checklist, which is a list of questions or topics that will be covered during the audit. The audit checklist helps the auditor to ensure that all relevant aspects of the ISMS are addressed and that the audit evidence is collected in a systematic and consistent manner12.
Audit execution: This stage involves conducting the audit activities, such as opening meeting, interviews, observations, document review, and closing meeting. The auditor gathers objective evidence, which is any information that supports the audit findings and conclusions. Objective evidence can be qualitative or quantitative, and can be obtained from various sources, such as records, statements, physical objects, or observations123.
Audit reporting: This stage involves reviewing the audit evidence, evaluating the audit findings, and documenting the audit results. The auditor reviews the audit evidence to determine whether it is sufficient, reliable, and relevant to support the audit findings. The auditor evaluates the audit findings to determine the degree of conformity or nonconformity of the ISMS with the audit criteria. The auditor documents the audit results in an audit report, which is a formal record of the audit process and outcomes. The audit report typically

includes the following elements123:
An introduction clarifying the scope, objectives, timing and extent of the work performed An executive summary indicating the key findings, a brief analysis and a conclusion The intended report recipients and, where appropriate, guidelines on classification and circulation Detailed findings and analysis Recommendations for improvement, where applicable A statement of conformity or nonconformity with the audit criteria Any limitations or exclusions of the audit scope or evidence Any deviations from the audit plan or procedures Any unresolved issues or disagreements between the auditor and the auditee A list of references, abbreviations, and definitions used in the report A list of appendices, such as audit plan, audit checklist, audit evidence, audit team members, etc.
Audit follow-up: This stage involves verifying the implementation and effectiveness of the corrective actions taken by the auditee to address the audit findings. The auditor monitors the progress and completion of the corrective actions, and evaluates their impact on the ISMS performance and conformity. The auditor may conduct a follow-up audit to verify the corrective actions on-site, or may rely on other methods, such as document review, remote interviews, or self-assessment by the auditee.
The auditor documents the follow-up results and updates the audit report accordingly123.
References:
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
ISO 19011:2018 - Guidelines for auditing management systems
The ISO 27001 audit process | ISMS.online

NEW QUESTION # 133
.....

It is known to us that the error correction is very important for these people who are preparing for the ISO-IEC-27001-Lead-Auditor exam in the review stage. It is very useful and helpful for a lot of people to learn from their mistakes, because many people will make mistakes in the same way, and it is very bad for these people to improve their accuracy. If you want to correct your mistakes when you are preparing for the ISO-IEC-27001-Lead-Auditor Exam, the study materials from our company will be the best choice for you.

Registration □ Search on ☀ www.troytecdumps.com □☀□ for 「 ISO-IEC-27001-Lead-Auditor 」 to obtain exam materials for free download □Guaranteed ISO-IEC-27001-Lead-Auditor Success

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, 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, study.stcs.edu.np, www.stes.tyc.edu.tw, learn.kausarwealth.com, pct.edu.pk, 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, Disposable vapes

BTW, DOWNLOAD part of Exam4Tests ISO-IEC-27001-Lead-Auditor dumps from Cloud Storage: https://drive.google.com/open?id=1bHs9qMOH9np1ZVu8kkRoIlzXh9C4pccy