PECB ISO-IEC-27001-Lead-Auditor Boot Camp - ISO-IEC-27001-Lead-Auditor Dumps Guide

BTW, DOWNLOAD part of ActualTestsIT ISO-IEC-27001-Lead-Auditor dumps from Cloud Storage: https://drive.google.com/open?id=1R-F7_fu8CpOTnaM8-EccxXcVRtq3W-i2

Wrong topic tend to be complex and no regularity, and the ISO-IEC-27001-Lead-Auditor torrent prep can help the users to form a good logical structure of the wrong question, this database to each user in the simulation in the practice of all kinds of wrong topic all induction and collation, and the ISO-IEC-27001-Lead-Auditor study question then to the next step in-depth analysis of the wrong topic, allowing users in which exist in the knowledge module, tell users of our ISO-IEC-27001-Lead-Auditor Exam Question how to make up for their own knowledge loophole, summarizes the method to deal with such questions for, to prevent such mistakes from happening again.

PECB ISO-IEC-27001-Lead-Auditor Certification is highly valued by organizations around the world. It is recognized as a standard of excellence in the field of information security management and is often a requirement for those seeking employment in this field. Individuals who hold this certification are considered experts in the field and are highly sought after by organizations looking to improve their information security management systems.

>> PECB ISO-IEC-27001-Lead-Auditor Boot Camp <<

Reliable ISO-IEC-27001-Lead-Auditor Boot Camp – 100% Latest PECB Certified ISO/IEC 27001 Lead Auditor exam Dumps Guide

With the development of artificial intelligence, we have encountered more challenges on development of the ISO-IEC-27001-Lead-Auditor exam materials. Only by improving our own soft power can we ensure we are not eliminated by the market. Select our ISO-IEC-27001-Lead-Auditor study questions to improve your work efficiency. As long as you study with our ISO-IEC-27001-Lead-Auditor training guide, then you will get the most related and specialized information on the subject to help you solve the questions on your daily work.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q228-Q233):

NEW QUESTION # 228
You are an experienced ISMS audit team leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-Do- Check-Act cycle in respect of the operation of the information security management system.
You do this by asking him to select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

Explanation:

Explanation:

* Review is the third stage of the Plan-Do-Check-Act (PDCA) cycle, which is a four-step model for implementing and improving an information security management system (ISMS) according to ISO /IEC 27001:202212. Review involves assessing and measuring the performance of the ISMS against the established policies, objectives, and criteria12.
* Assess is the verb that describes the action of reviewing the ISMS. Assess means to evaluate, analyze, or measure something in a systematic and objective manner3. Assessing the ISMS involves collecting and verifying audit evidence, identifying strengths and weaknesses, and determining the degree of conformity or nonconformity12.
* Regular is the adjective that describes the frequency or interval of reviewing the ISMS. Regular means occurring or done at fixed or uniform intervals4. Reviewing the ISMS at regular intervals means conducting internal audits and management reviews periodically, such as annually, quarterly, or monthly, depending on the needs and risks of the organization12.
* Suitability is one of the attributes that describes the quality or outcome of reviewing the ISMS. Suitability means being appropriate or fitting for a particular purpose, person, or situation5. Reviewing the ISMS for suitability means ensuring that it is aligned with the organization's strategic direction, business objectives, and information security requirements12.

References :=

* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* Assess | Definition of Assess by Merriam-Webster
* Regular | Definition of Regular by Merriam-Webster
* Suitability | Definition of Suitability by Merriam-Webster

NEW QUESTION # 229

You are performing an ISMS audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to verify the information security incident management process. The IT Security Manager presents the information security incident management procedure (Document reference ID:ISMS_L2_16, version 4).

You review the document and notice a statement "Any information security weakness, event, and incident should be reported to the Point of Contact (PoC) within 1 hour after identification". When interviewing staff, you found that there were differences in the understanding of the meaning of the phrase "weakness, event, and incident".

The IT Security Manager explained that an online "information security handling" training seminar was conducted 6 months ago. All the people interviewed participated in and passed the reporting exercise and course assessment.

You would like to investigate other areas further to collect more audit evidence. Select three options that would not be valid audit trails.

- A. Collect more evidence on how the organisation learns from information security incidents and makes improvements. (Relevant to control A.5.27)
- B. Collect more evidence on whether terms and definitions are contained in the information security policy. (Relevant to control 5.32) H: Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria. (Relevant to clause 8.13)

- C. Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
- D. Collect more evidence on how information security incidents are reported via appropriate channels (relevant to control A.6.8)
- E. Collect more evidence on how the organisation tests the business continuity plan. (Relevant to control A.5.30)
- F. Collect more evidence on how the organisation conducts information security incident training and evaluates its effectiveness. (Relevant to clause 7.2)
- G. Collect more evidence on how areas subject to information security incidents are quarantined to maintain information security during disruption (relevant to control A.5.29)

Answer: B,C

Explanation:
The three options that would not be valid audit trails are:
*Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
*Collect more evidence on whether terms and definitions are contained in the information security policy.
(Relevant to control 5.32)
*Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria.
(Relevant to clause 8.13) These options are not valid audit trails because they are not directly related to the information security incident management process, which is the focus of the audit. The audit trails should be relevant to the objectives, scope, and criteria of the audit, and should provide sufficient and reliable evidence to support the audit findings and conclusions1.
Option E is not valid because the PoC is not a part of the information security incident management process, but rather a role that is responsible for reporting and escalating information security incidents to the appropriate authorities2. The audit trail should focus on how the PoC performs this function, not how the organisation manages the PoC.
Option G is not valid because the terms and definitions are not a part of the information security incident management process, but rather a part of the information security policy, which is a high-level document that defines the organisation's information security objectives, principles, and responsibilities3. The audit trail should focus on how the information security policy is communicated, implemented, and reviewed, not whether it contains terms and definitions.
Option H is not valid because ISO 27035 is not a part of the information security incident management process, but rather a guidance document that provides best practices for managing information security incidents4. The audit trail should focus on how the organisation follows the requirements of ISO/IEC 27001:
2022 for information security incident management, not whether it uses ISO 27035 as an internal audit criteria.
The other options are valid audit trails because they are related to the information security incident management process, and they can provide useful evidence to evaluate the conformity and effectiveness of the process. For example:
*Option A is valid because it relates to control A.5.29, which requires the organisation to establish procedures to isolate and quarantine areas subject to information security incidents, in order to prevent further damage and preserve evidence5. The audit trail should collect evidence on how the organisation implements and tests these procedures, and how they ensure the continuity of information security during disruption.
*Option B is valid because it relates to control A.6.8, which requires the organisation to establish mechanisms for reporting information security events and weaknesses, and to ensure that they are communicated in a timely manner to the appropriate levels within the organisation6. The audit trail should collect evidence on how the organisation defines and uses these mechanisms, and how they monitor and review the reporting process.
*Option C is valid because it relates to clause 7.2, which requires the organisation to provide information security awareness, education, and training to all persons under its control, and to evaluate the effectiveness of these activities7. The audit trail should collect evidence on how the organisation identifies the information security training needs, how they deliver and record the training, and how they measure the learning outcomes and feedback.
*Option D is valid because it relates to control A.5.27, which requires the organisation to learn from information security incidents and to implement corrective actions to prevent recurrence or reduce impact8.
The audit trail should collect evidence on how the organisation analyses and documents the root causes and consequences of information security incidents, how they identify and implement corrective actions, and how they verify the effectiveness of these actions.
*Option F is valid because it relates to control A.5.30, which requires the organisation to establish and maintain a business continuity plan to ensure the availability of information and information processing facilities in the event of a severe information security incident9. The audit trail should collect evidence on how the organisation develops and updates the business continuity plan, how they test and review the plan, and how they communicate and train the relevant personnel on the plan.
References: 1: ISO 19011:2018, 6.2;
2: ISO/IEC 27001:2022, A.6.8.1;
3: ISO/IEC 27001:2022, 5.2;
4: ISO/IEC 27035:2016, Introduction;
5: ISO/IEC 27001:2022, A.5.29;

6: ISO/IEC 27001:2022, A.6.8;
7: ISO/IEC 27001:2022, 7.2;
8: ISO/IEC 27001:2022, A.5.27;
9: ISO/IEC 27001:2022, A.5.30;
10: ISO 19011:2018;
11: ISO/IEC 27001:2022;
12: ISO/IEC 27001:2022;
13: ISO/IEC 27035:2016;
14: ISO/IEC 27001:2022;
15: ISO/IEC 27001:2022;
16: ISO/IEC 27001:2022;
17: ISO/IEC 27001:2022;
18: ISO/IEC 27001:2022

NEW QUESTION # 230
Scenario 4: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs. Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology. equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit. Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence based approach, particularly in light of two information security incidents reported by Techvology in the past year The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards The auditors also verified whether Techvology complied with the contractual requirements established between the two entities This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to. Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
Based on the scenario above, answer the following question:
According to Scenario 4, what type of audit evidence did the auditors collect to determine the source of the information security incidents?

- A. Analytical and mathematical evidence
- B. Verbal and documentary evidence
- C. Confirmative and technical evidence

Answer: B

Explanation:
Comprehensive and Detailed In-Depth
A . Correct answer:
Auditors conducted interviews (verbal evidence) and analyzed incident resolution records, employee training logs, and governance policies (documentary evidence).
ISO 19011:2018 (Clause 6.4.7) states that audit evidence can be verbal, documented, observed, or analytical.
B . Incorrect:
Confirmative evidence involves third-party validation, which was not explicitly mentioned.
C . Incorrect:

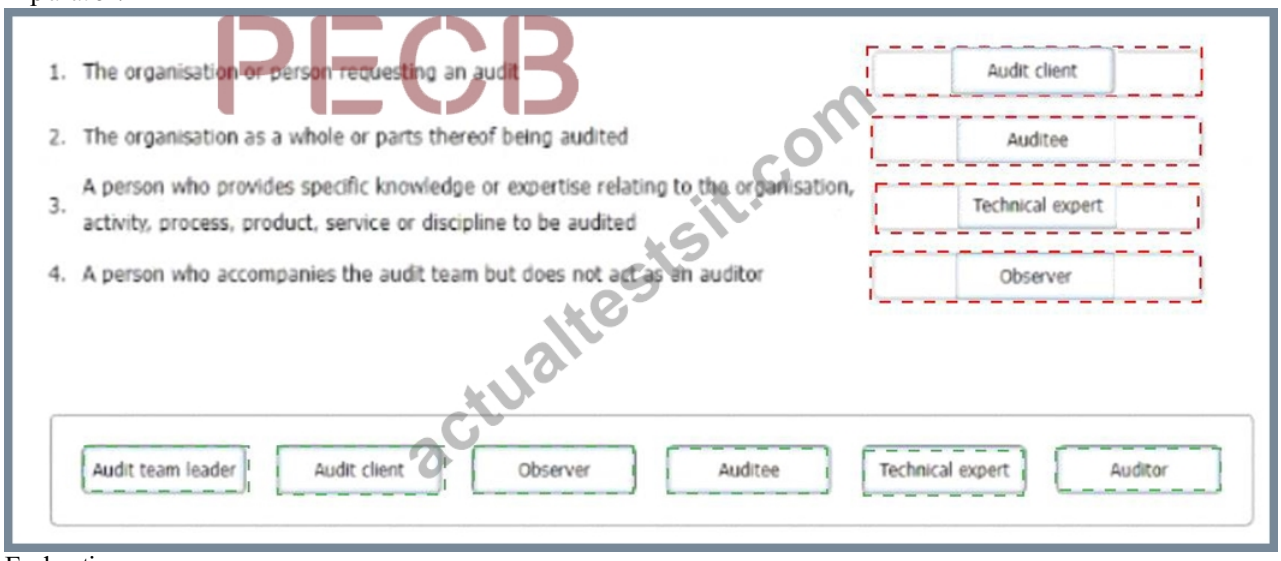
Mathematical analysis was not conducted in this audit.
Relevant Standard Reference:
ISO 19011:2018 Clause 6.4.7 (Audit Evidence Collection Methods)

NEW QUESTION # 231
Please match the roles to the following descriptions:

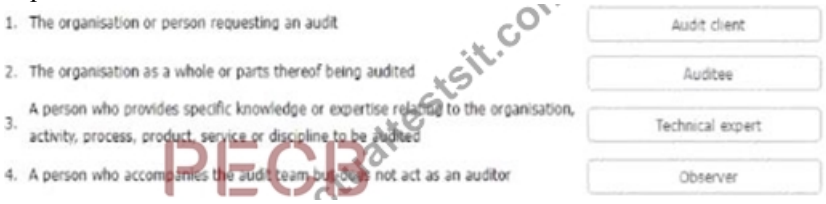
To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable test from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Answer:

Explanation:



Explanation



* The auditee is the organization or part of it that is subject to the audit. The auditee could be internal or external to the audit client . The auditee should cooperate with the audit team and provide them with access to relevant information, documents, records, personnel, and facilities .
* The audit client is the organization or person that requests an audit. The audit client could be internal or external to the auditee . The audit client should define the audit objectives, scope, criteria, and programme, and appoint the audit team leader .
* The technical expert is a person who provides specific knowledge or expertise relating to the organization, activity, process, product, service, or discipline to be audited. The technical expert could be internal or external to the audit team . The technical

expert should support the audit team in collecting and evaluating audit evidence, but should not act as an auditor .
* The observer is a person who accompanies the audit team but does not act as an auditor. The observer could be internal or external to the audit team . The observer should observe the audit activities without interfering or influencing them, unless agreed otherwise by the audit team leader and the auditee .
References :=
* [ISO 19011:2022 Guidelines for auditing management systems]
* [ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements]

NEW QUESTION # 232
You are an experienced ISMS audit team leader who is currently conducting a third party initial certification audit of a new client, using ISO/IEC 27001:2022 as your criteria.
It is the afternoon of the second day of a 2-day audit, and you are just about to start writing your audit report. So far no nonconformities have been identified and you and your team have been impressed with both the site and the organisation's ISMS. At this point, a member of your team approaches you and tells you that she has been unable to complete her assessment of leadership and commitment as she has spent too long reviewing the planning of changes.
Which one of the following actions will you take in response to this information?

- A. Suggest to the client that if they are prepared to upgrade your return flight to first class you will audit leadership and commitment in your own time tomorrow.
- B. Advise the auditee that the certification audit will need to be terminated and rescheduled.
- C. Contact the individual managing the audit programme and seek their permission to record a positive recommendation in the audit report.
- D. Contact your head office and await their further instructions of how to proceed.
- E. Advise the auditee and audit client that it is not possible to make a positive recommendation at this point.
- F. Given there have been no nonconformities identified and the overall impression of the organisation has been a good one, record a positive recommendation for certification in the audit report.
- G. Apologise to the client and tell them you will return at a later date to review leadership and commitment.

Answer: E

Explanation:
Review the audit plan and client availabilities to determine whether there is any opportunity for another member of your team to pick up this task before the closing meeting.
Explanation:
Leadership and commitment is a key requirement of ISO/IEC 27001:2022, as it establishes the top management's role and responsibility in establishing, implementing, maintaining, and continually improving the ISMS. Without assessing this aspect, the audit team cannot conclude that the ISMS is effective and conforms to the standard. Therefore, the audit team leader should advise the auditee and audit client that it is not possible to make a positive recommendation at this point, and explain the reason and the implications. The audit team leader should also consult with the certification body and the audit programme manager on the next steps, such as extending the audit duration, conducting a follow-up audit, or issuing a conditional certification, depending on the certification body's policy and the audit client's agreement. Reference: = ISO/IEC 27001:2022, clause 5, Leadership PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process PECB Candidate Handbook ISO 27001 Lead Auditor, page 22, Audit Report PECB Candidate Handbook ISO 27001 Lead Auditor, page 23, Audit Conclusion and Recommendation

NEW QUESTION # 233
.....

Auditor exam □ 《 www.dumpsmaterials.com 》 is best website to obtain ➡ ISO-IEC-27001-Lead-Auditor □□□ for free download □Latest ISO-IEC-27001-Lead-Auditor Exam Book

- ISO-IEC-27001-Lead-Auditor Boot Camp Will Be Your Powerful Weapon to Pass PECB Certified ISO/IEC 27001 Lead Auditor exam □ Search for 《 ISO-IEC-27001-Lead-Auditor 》 and download it for free immediately on ☀ www.pdfvce.com □☀□ □Printable ISO-IEC-27001-Lead-Auditor PDF
- Printable ISO-IEC-27001-Lead-Auditor PDF □ Latest ISO-IEC-27001-Lead-Auditor Exam Book □ ISO-IEC-27001-Lead-Auditor Exam Duration □ Search for 【 ISO-IEC-27001-Lead-Auditor 】 and download it for free immediately on " www.prepawayexam.com " □Frenquent ISO-IEC-27001-Lead-Auditor Update
- How Pdfvce will Help You in Passing the PECB ISO-IEC-27001-Lead-Auditor Certification Exam? □ Download ☀ ISO-IEC-27001-Lead-Auditor □☀□ for free by simply entering 【 www.pdfvce.com 】 website □Pass ISO-IEC-27001-Lead-Auditor Guarantee
- ISO-IEC-27001-Lead-Auditor Valid Test Forum □ Exam Dumps ISO-IEC-27001-Lead-Auditor Collection □ Valid ISO-IEC-27001-Lead-Auditor Exam Simulator □ Download □ ISO-IEC-27001-Lead-Auditor □ for free by simply searching on ➤ www.vce4dumps.com □ □Latest ISO-IEC-27001-Lead-Auditor Exam Book
- ISO-IEC-27001-Lead-Auditor Boot Camp Will Be Your Powerful Weapon to Pass PECB Certified ISO/IEC 27001 Lead Auditor exam □ The page for free download of ➽ ISO-IEC-27001-Lead-Auditor □ on （ www.pdfvce.com ） will open immediately □ISO-IEC-27001-Lead-Auditor Braindumps
- Prioritize Your Study Time ISO-IEC-27001-Lead-Auditor CONPLETE STUDY GUIDE □ Download ☀ ISO-IEC-27001-Lead-Auditor □☀□ for free by simply searching on [www.verifieddumps.com] □Exam Dumps ISO-IEC-27001-Lead-Auditor Collection
- Free PDF Quiz 2026 PECB ISO-IEC-27001-Lead-Auditor High Hit-Rate Boot Camp □ Download □ ISO-IEC-27001-Lead-Auditor □ for free by simply searching on { www.pdfvce.com } □ISO-IEC-27001-Lead-Auditor New Dumps Ebook
- Free PDF Quiz 2026 PECB ISO-IEC-27001-Lead-Auditor High Hit-Rate Boot Camp □ □ www.testkingpass.com □ is best website to obtain ➠ ISO-IEC-27001-Lead-Auditor □ for free download □Latest ISO-IEC-27001-Lead-Auditor Exam Labs
- Latest ISO-IEC-27001-Lead-Auditor Exam Book □ ISO-IEC-27001-Lead-Auditor Braindumps □ Latest ISO-IEC-27001-Lead-Auditor Exam Book □ Search on ⇛ www.pdfvce.com ⇚ for ☀ ISO-IEC-27001-Lead-Auditor □☀□ to obtain exam materials for free download □Exam Dumps ISO-IEC-27001-Lead-Auditor Collection
- Pass Guaranteed PECB - High Pass-Rate ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam Boot Camp □ Search for □ ISO-IEC-27001-Lead-Auditor □ and easily obtain a free download on ✔ www.vce4dumps.com □✔□ □ISO-IEC-27001-Lead-Auditor Valid Test Forum
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, estar.jp, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest ActualTestsIT ISO-IEC-27001-Lead-Auditor PDF Dumps and ISO-IEC-27001-Lead-Auditor Exam Engine Free Share: https://drive.google.com/open?id=1R-F7_fu8CpOTnaM8-EccxXcVRtq3W-i2