100% Pass PECB - Pass-Sure ISO-IEC-27001-Lead-Auditor - Examcollection PECB Certified ISO/IEC 27001 Lead Auditor exam Questions Answers

BTW, DOWNLOAD part of Test4Cram ISO-IEC-27001-Lead-Auditor dumps from Cloud Storage: https://drive.google.com/open?id=1sWeSxsoAYUDjX_za6522X83hfScBnq8r

When you know you will enjoy one year free update after purchase, you may consider how to get the latest PECB ISO-IEC-27001-Lead-Auditor exam torrent. Here, we will tell you, the Test4Cram system will send the update ISO-IEC-27001-Lead-Auditor exam dumps to you automatically. You can pay attention to your payment email. If you find there is update and do not find any update email, do not worry, you can check your spam. If there is still not, please contact us by email or online chat. Besides, if you have any questions about PECB ISO-IEC-27001-Lead-Auditor, please contact us at any time. Our 7/24 customer service will be always at your side and solve your problem at once.

PECB ISO-IEC-27001-Lead-Auditor Certification is highly respected in the information security industry and is recognized by organizations around the world. It demonstrates that the certified individual has the knowledge and skills to lead and manage an ISMS audit team and can ensure that an organization's information security management system is effective and compliant with the ISO/IEC 27001 standard. With this certification, professionals can enhance their career prospects and contribute to the success of their organization.

PECB Certified ISO/IEC 27001 Lead Auditor certification exam is designed for individuals who have a minimum of five years of professional experience in information security management, including two years of experience in auditing. PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam covers various topics such as the principles, concepts, and standards of information security management, the audit process, audit techniques, and reporting. It also requires candidates to demonstrate their ability to lead an audit team, plan and conduct an audit, and communicate effectively with stakeholders.

>> Examcollection ISO-IEC-27001-Lead-Auditor Questions Answers <<

ISO-IEC-27001-Lead-Auditor Reliable Dumps Questions | ISO-IEC-27001-Lead-Auditor Valid Exam Review

To fit in this amazing and highly accepted exam, you must prepare for it with high-rank practice materials like our ISO-IEC-27001-Lead-Auditor study materials. Our ISO-IEC-27001-Lead-Auditor exam questions are the Best choice in terms of time and money. If you are a beginner, start with the learning guide of ISO-IEC-27001-Lead-Auditor Practice Engine and our products will correct your learning problems with the help of the ISO-IEC-27001-Lead-Auditor training braindumps.

PECB ISO-IEC-27001-Lead-Auditor is a certification exam that validates the knowledge and skills of an individual in the field of information security management systems (ISMS). PECB, a leading certification body, offers ISO-IEC-27001-Lead-Auditor exam

to assess the competence of professionals who intend to become ISO/IEC 27001 Lead Auditors. ISO-IEC-27001-Lead-Auditor Exam evaluates the candidate's understanding of ISMS, risk management, auditing principles, and compliance with regulatory requirements.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q45-Q50):

NEW QUESTION # 45
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.
Your colleague seems unsure as to the difference between an information security event and an information security incident. You attempt to explain the difference by providing examples.
Which three of the following scenarios can be defined as information security incidents?

- A. The organisation's malware protection software prevents a virus
- B. A hard drive is used after its recommended replacement date
- C. An unhappy employee changes payroll records without permission
- D. The organisation receives a phishing email
- E. The organisation fails a third-party penetration test
- F. An employee fails to clear their desk at the end of their shift
- G. The organisation's marketing data is copied by hackers and sold to a competitor
- H. A contractor who has not been paid deletes top management ICT accounts

Answer: C,G,H

Explanation:
Explanation
According to ISO/IEC 27000:2018, which provides an overview and vocabulary of information security management systems, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant1. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security1. Therefore, based on this definition, three examples of information security incidents are:
* A contractor who has not been paid deletes top management ICT accounts: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of access, data, or functionality for the top management.
* An unhappy employee changes payroll records without permission: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in financial fraud, legal liability, or reputational damage for the organization.
* The organisation's marketing data is copied by hackers and sold to a competitor: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of confidentiality, competitive advantage, or customer trust for the organization.
The other options are not examples of information security incidents, but rather information security events that may or may not lead to incidents depending on their impact and severity. For example:
* The organisation's malware protection software prevents a virus: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, as it is prevented by the malware protection software.
* A hard drive is used after its recommended replacement date: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it fails or causes other problems.
* The organisation receives a phishing email: This is an example of an identified occurrence of a network state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it is opened or responded to by the recipient.
* An employee fails to clear their desk at the end of their shift: This is an example of an identified occurrence of a service state indicating a possible breach of information security policy or failure of
* safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the desk contains sensitive or confidential information that is accessed by unauthorized persons.
* The organisation fails a third-party penetration test: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the penetration test reveals serious vulnerabilities that are exploited by malicious actors.

References: ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary

NEW QUESTION # 46
Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.
Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments. Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.
During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC 27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.
Based on the scenario above, answer the following question:
What action should be taken regarding Techmanic's certification?

- A. Transfer the certification because they were not granted the extension certification
- B. Withdraw the certification because they failed to resolve nonconformities related to hosting services
- C. Suspend the certification because they used the certification out of its scope

Answer: C

Explanation:
Comprehensive and Detailed In-Depth
A . Correct answer:
Techmanic misrepresented its certification scope, which is a violation of ISO certification rules.
Suspension allows time for corrective action before withdrawal is considered.
B . Incorrect:
Certification withdrawal is only necessary if corrective actions fail after suspension.
C . Incorrect:
Transfer does not resolve misrepresentation issues.
Relevant Standard Reference:

NEW QUESTION # 47
Which two of the following are examples of audit methods that 'do not' involve human interaction?

- A. Performing a review of auditees procedures in preparation for an audit
- B. Observing work performed by remote surveillance
- C. Conducting an interview using a teleconferencing platform
- D. Reviewing the auditee's response to an audit finding
- E. Confirming the date and time of the audit
- F. Analysing data by remotely accessing the auditee's server

Answer: A,F

Explanation:
Audit methods are the techniques and procedures that auditors use to collect and evaluate audit evidence. Audit methods can be classified into two categories: those that involve human interaction and those that do not. Human interaction methods are those that require direct or indirect communication with the auditee or other relevant parties, such as interviews, questionnaires, surveys, observations, or walkthroughs. Non-human interaction methods are those that do not require any communication with the auditee or other parties, such as document reviews, data analysis, or remote surveillance.
Some examples of audit methods that do not involve human interaction are:
Performing a review of auditee's procedures in preparation for an audit: This method involves examining the auditee's documented information, such as policies, processes, records, or reports, to verify their adequacy and effectiveness in meeting the audit criteri a. The auditor does not need to interact with the auditee or anyone else to perform this method.
Analysing data by remotely accessing the auditee's server: This method involves accessing and processing the auditee's data, such as performance indicators, logs, metrics, or statistics, to verify their accuracy and reliability in meeting the audit criteria. The auditor does not need to interact with the auditee or anyone else to perform this method.
Reference:
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 6.2.2]

NEW QUESTION # 48
Integrity of data means

- A. Data should be viewable at all times
- B. Accuracy and completeness of the data
- C. Data should be accessed by only the right people

Answer: B

Explanation:
Integrity of data means accuracy and completeness of the data. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Data should be viewable at all times is not related to integrity, but to availability. Data should be accessed by only the right people is not related to integrity, but to confidentiality. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4.

NEW QUESTION # 49
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) and explains that the process is based on ISO/IEC 27035-1:2016.
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 "weakness, event, and incident".
The IT Security Manager explained that an online "information security handling" training seminar was conducted 6 months ago. All of the interviewed persons participated in and passed the reporting exercise and course assessment.
You are preparing the audit findings. Select two options that are correct.

- A. There is a nonconformity (NC). The terminology of the the incident management reporting process is unclear as evidenced by staff misunderstanding of the meaning of "weakness, event and incident". This is not conforming with clause 9.1 and control A.5.24.
- B. There is no nonconformance. The information security handling training has been effective. This conforms with clause 7.2 and control A.6.3.
- C. There is an opportunity for improvement (OFI). The information security weaknesses, events, and incidents are reported. This is relevant to clause 9.1 and control A.5.24.
- D. There is no nonconformance. The information security weaknesses, events, and incidents are reported. This conforms with clause 9.1 and control A.5.24.
- E. There is a nonconformity (NC). The information security incident training has failed. This is not conforming with clause 7.2 and control A.6.3.
- F. There is an opportunity for improvement (OFI). The information security incident training effectiveness can be improved. This is relevant to clause 7.2 and control A.6.3.

Answer: A,F

Explanation:
According to ISO/IEC 27001:2022 clause 7.2, the organization must ensure that the persons doing work under its control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. The organization must also provide information security awareness education and training to its personnel and relevant interested parties. According to control A.6.3, the organization must ensure that all employees and contractors are made aware of the information security incident management procedures and their expected roles and responsibilities. Therefore, an opportunity for improvement (OFI) can be identified if the information security incident training effectiveness can be improved, as evidenced by the differences in the understanding of the meaning of "weakness, event, and incident" among the staff.
According to ISO/IEC 27001:2022 clause 9.1, the organization must monitor, measure, analyze and evaluate the information security performance and the effectiveness of the ISMS. The organization must also retain appropriate documented information as evidence of the monitoring and measurement results. According to control A.5.24, the organization must establish and maintain an information security incident management process that includes the following activities:
* reporting information security events and weaknesses;
* assessing and deciding on information security events;
* responding to information security incidents;
* learning from information security incidents;
* collecting evidence and disclosing information.
Therefore, a nonconformity (NC) can be identified if the terminology of the incident management reporting process is unclear, as evidenced by the staff misunderstanding of the meaning of "weakness, event, and incident". This could lead to inconsistent or inaccurate reporting, assessment, response, learning, and disclosure of information security incidents, which could affect the information security performance and the effectiveness of the ISMS.
Reference:
* ISO/IEC 27001:2022, clauses 7.2, 9.1, and Annex A controls A.5.24 and A.6.3
* [PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 15-16, 18-19, 22-23
* ISO/IEC 27035-1:2016, clauses 4, 5, 6, 7, and 8
* ISO 27001 - Annex A.16: Information Security Incident Management
* ISO 27001:2022 Annex A Control 5.24 - What's New?

NEW QUESTION # 50
.....

download for free □ISO-IEC-27001-Lead-Auditor Valid Test Testking

- PDF ISO-IEC-27001-Lead-Auditor Download □ ISO-IEC-27001-Lead-Auditor Exam Guide □ High ISO-IEC-27001-Lead-Auditor Passing Score □ Simply search for ➤ ISO-IEC-27001-Lead-Auditor □ for free download on ☀ www.vceengine.com □☀□ □ISO-IEC-27001-Lead-Auditor Test Simulator Fee
- ISO-IEC-27001-Lead-Auditor exam dumps, PECB ISO-IEC-27001-Lead-Auditor test cost □ Immediately open ➤ www.pdfvce.com □ and search for ➤ ISO-IEC-27001-Lead-Auditor □ to obtain a free download □ISO-IEC-27001-Lead-Auditor Valid Braindumps Files
- Customizable PECB ISO-IEC-27001-Lead-Auditor Practice Exam Software □ Search on ▷ www.dumpsmaterials.com ◁ for ➽ ISO-IEC-27001-Lead-Auditor □ to obtain exam materials for free download □Reliable ISO-IEC-27001-Lead-Auditor Braindumps Free
- app.parler.com, www.pshunv.com, 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, ncon.edu.sa, myportal.utt.edu.tt, fitrialbaasitu.com, 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, Disposable vapes

What's more, part of that Test4Cram ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1sWeSxsoAYUDjX_za6522X83hfScBnq8r