Mock ISO-IEC-27001-Lead-Auditor Exams - ISO-IEC-27001-Lead-Auditor PDF

P.S. Free 2025 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by ExamDumpsVCE: https://drive.google.com/open?id=1RagR8E2D6TUHhM7m9DwbrCV4oWAEsMrK

Only 20-30 hours on our ISO-IEC-27001-Lead-Auditor learning guide are needed for the client to prepare for the test and it saves our client's time and energy. Most people may wish to use the shortest time to prepare for the ISO-IEC-27001-Lead-Auditor test and then pass the test with our ISO-IEC-27001-Lead-Auditor Study Materials successfully because they have to spend their most time and energy on their jobs, learning, family lives and other important things. And our ISO-IEC-27001-Lead-Auditor exam braindumps won't let you down!

PECB ISO-IEC-27001-Lead-Auditor Certification is recognized worldwide and is highly valued by employers. It is a testament to the candidate's knowledge and expertise in the field of information security management and auditing. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is also an excellent way to advance one's career and increase earning potential. Individuals who have earned the certification can work in various roles, including as an auditor, consultant, or manager in the field of information security.

>> Mock ISO-IEC-27001-Lead-Auditor Exams <<

PECB ISO-IEC-27001-Lead-Auditor Practice Test - Quick Tips To Pass (2025)

The learning material is open in three excellent formats, PDF, a desktop practice test, and a web-based practice test. PECB ISO-

IEC-27001-Lead-Auditor Dumps is organized by experts while saving the furthest down-the-line plan to them for the PECB ISO-IEC-27001-Lead-Auditor Exam. The sans bug plans have been given to you all to drift through the PECB ISO-IEC-27001-Lead-Auditor certification exam.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q78-Q83):

NEW QUESTION # 78
Information or data that are classified as _____ do not require labeling.

- A. Internal
- B. Confidential
- C. Public
- D. Highly Confidential

Answer: C

Explanation:
Information or data that are classified as public do not require labeling. Public information or data are those that are intended for general disclosure and have no impact on the organization's operations or reputation if disclosed. Labeling is a method of implementing classification, which is a process of structuring information according to its sensitivity and value for the organization. Labeling helps to identify the level of protection and handling required for each type of information. Information or data that are classified as internal, confidential, or highly confidential require labeling, as they contain information that is not suitable for public disclosure and may cause harm or loss to the organization if disclosed. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 37. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 14.

NEW QUESTION # 79
Scenario 4: SendPay is a financial company that provides its services through a network of agents and financial institutions. One of their main services is transferring money worldwide. SendPay, as a new company, seeks to offer top quality services to its clients. Since the company offers international transactions, it requires from their clients to provide personal information, such as their identity, the reason for the transactions, and other details that might be needed to complete the transaction. Therefore, SendPay has implemented security measures to protect their clients' information, including detecting, investigating, and responding to any information security threats that may emerge. Their commitment to offering secure services was also reflected during the ISMS implementation where the company invested a lot of time and resources.
Last year, SendPay unveiled their digital platform that allows money transactions through electronic devices, such as smartphones or laptops, without requiring an additional fee. Through this platform, SendPay's clients can send and receive money from anywhere and at any time. The digital platform helped SendPay to simplify the company's operations and further expand its business. At the time, SendPay was outsourcing its software operations, hence the project was completed by the software development team of the outsourced company. The same team was also responsible for maintaining the technology infrastructure of SendPay.
Recently, the company applied for ISO/IEC 27001 certification after having an ISMS in place for almost a year. They contracted a certification body that fit their criteri a. Soon after, the certification body appointed a team of four auditors to audit SendPay's ISMS. During the audit, among others, the following situations were observed:
1. The outsourced software company had terminated the contract with SendPay without prior notice. As a result, SendPay was unable to immediately bring the services back in-house and its operations were disrupted for five days. The auditors requested from SendPay's representatives to provide evidence that they have a plan to follow in cases of contract terminations. The representatives did not provide any documentary evidence but during an interview, they told the auditors that the top management of SendPay had identified two other software development companies that could provide services immediately if similar situations happen again.
2. There was no evidence available regarding the monitoring of the activities that were outsourced to the software development company. Once again, the representatives of SendPay told the auditors that they regularly communicate with the software development company and that they are appropriately informed for any possible change that might occur.
3. There was no nonconformity found during the firewall testing. The auditors tested the firewall configuration in order to determine the level of security provided by these services. They used a packet analyzer to test the firewall policies which enabled them to check the packets sent or received in real-time.
Based on this scenario, answer the following question:
Why could SendPay not restore their services back in-house after the contract termination? Refer to scenario 4.

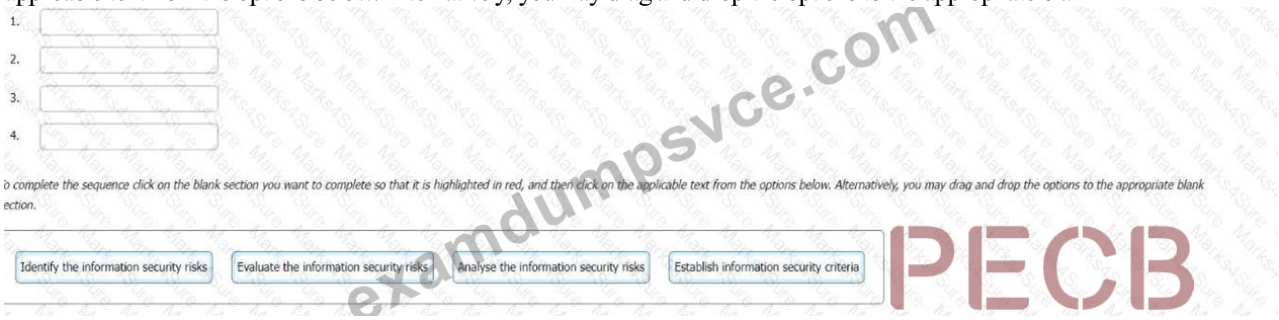
- A. Because the outsourced software company terminated the contract with SendPay without prior notice
- B. Because SendPay did not monitor the technology infrastructure of the outsourced software operations

- C. Because SendPay lacked a comprehensive business continuity plan with potential impact of contract terminations

Answer: C

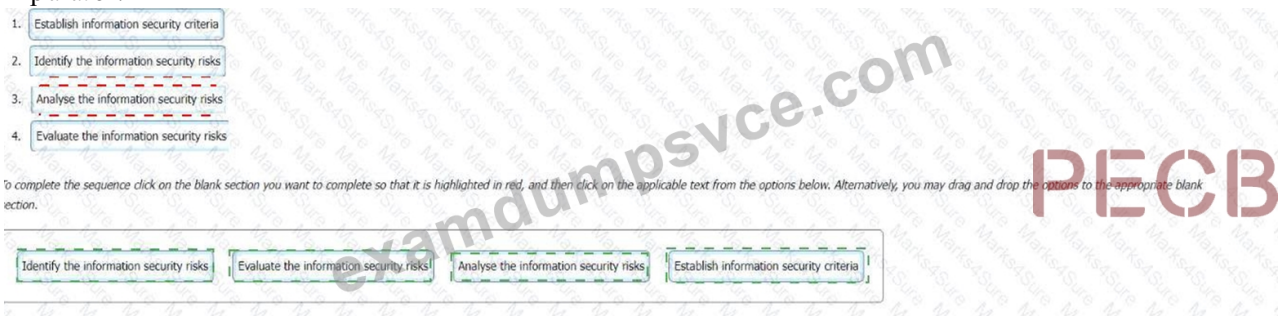
Explanation:
SendPay's inability to restore their services immediately after the contract termination indicates a lack of a comprehensive business continuity plan that addresses the potential impacts of such terminations. This oversight can result in significant operational disruptions, as observed.

NEW QUESTION # 80
Select the correct sequence for the information security risk assessment process in an ISMS.
To complete the sequence 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 options to the appropriate blank



Answer:

Explanation:



Explanation:

According to ISO 27001:2022, the standard for information security management systems (ISMS), the correct sequence for the information security risk assessment process is as follows:
* Establish information security criteria
* Identify the information security risks
* Analyse the information security risks
* Evaluate the information security risks
The first step is to establish the information security criteria, which include the risk assessment methodology, the risk acceptance criteria, and the risk evaluation criteria. These criteria define how the organization will perform the risk assessment, what level of risk is acceptable, and how the risks will be compared and prioritized.
The second step is to identify the information security risks, which involve identifying the assets, threats, vulnerabilities, and existing controls that are relevant to the ISMS. The organization should also identify the potential consequences and likelihood of each risk scenario.
The third step is to analyse the information security risks, which involve estimating the level of risk for each risk scenario based on the criteria established in the first step. The organization should also consider the sources of uncertainty and the confidence level of the risk estimation.
The fourth step is to evaluate the information security risks, which involve comparing the estimated risk levels with the risk

acceptance criteria and determining whether the risks are acceptable or need treatment.
The organization should also prioritize the risks based on the risk evaluation criteria and the objectives of the ISMS.
References: ISO 27001:2022 Clause 6.1.2 Information security risk assessment, ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide - Advisera, ISO 27001 Risk Assessment: 7 Step Guide - IT Governance UK Blog

NEW QUESTION # 81
Which two of the following phrases would apply to "audit objectives"?

- A. Revising management policy
- B. Auditor competence
- C. Audit duration
- D. Checking legal compliance
- E. Identifying opportunities for improvement, if required
- F. Determining conformity

Answer: E,F

Explanation:
Explanation
The audit objectives are the purpose and scope of an audit, as defined by the audit client and the auditor. According to the ISO/IEC 27001 standard, the audit objectives for an ISMS audit may include determining the extent of conformity of the ISMS with the audit criteria, evaluating the ability of the ISMS to ensure the organization meets its information security objectives, and identifying potential areas for improvement of the ISMS12. References: = 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, page 192: ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 4.2.1.

NEW QUESTION # 82
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 has been undertaken effectively
- B. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
- C. Verification should focus on whether any action undertaken taken has been undertaken efficiently
- D. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
- E. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
- F. Verification should focus on whether any action undertaken is complete

Answer: A,F

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 # 83
.....

Considering that our customers are from different countries, there is a time difference between us, but we still provide the most thoughtful online after-sale service twenty four hours a day, seven days a week, so just feel free to contact with us through email anywhere at any time. Our commitment of helping you to Pass ISO-IEC-27001-Lead-Auditor Exam will never change. Considerate 24/7 service shows our attitudes, we always consider our candidates' benefits and we guarantee that our ISO-IEC-27001-Lead-Auditor test questions are the most excellent path for you to pass the exam.

search for ➤ ISO-IEC-27001-Lead-Auditor □ to download exam materials for free □Test ISO-IEC-27001-Lead-Auditor Collection

- PECB Mock ISO-IEC-27001-Lead-Auditor Exams: PECB Certified ISO/IEC 27001 Lead Auditor exam - www.prep4pass.com Ensures you a Easy Studying Experience □ Search for □ ISO-IEC-27001-Lead-Auditor □ and download exam materials for free through 「 www.prep4pass.com 」 □ISO-IEC-27001-Lead-Auditor Test Lab Questions
- 泰納克.官網.com, lms.arohispace9.com, www.stes.tyc.edu.tw, rhinotech.cc:88, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, joshwhi204.thenerdsblog.com, daotao.wisebusiness.edu.vn, 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, huntertraders.com, Disposable vapes

BONUS!!! Download part of ExamDumpsVCE ISO-IEC-27001-Lead-Auditor dumps for free: https://drive.google.com/open?id=1RagR8E2D6TUHhM7m9DwbrCV4oWAEsMrK