Valid ISO-IEC-27001-Lead-Auditor Premium VCE Braindumps Materials - DumpsTests
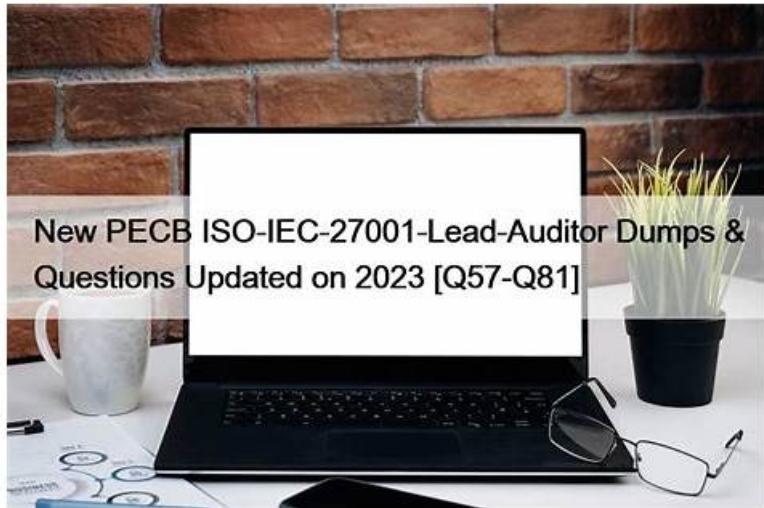
A considerable amount of effort goes into our products. So in most cases our ISO-IEC-27001-Lead-Auditor study materials are truly your best friend. On one hand, our ISO-IEC-27001-Lead-Auditor study materials are the combination of the latest knowledge and the newest technology, which could constantly inspire your interest of study. On the other hand, our ISO-IEC-27001-Lead-Auditor Study Materials can predicate the exam correctly. Therefore you can handle the questions in the real exam like a cork. Through highly effective learning method and easily understanding explanation, you will pass the ISO-IEC-27001-Lead-Auditor exam with no difficulty.

To be eligible for the PECB ISO-IEC-27001-Lead-Auditor Exam, candidates must have a minimum of five years of professional experience, with at least two years of experience in information security management. They must also have completed a PECB-certified ISO/IEC 27001 Foundation training course or have equivalent knowledge. ISO-IEC-27001-Lead-Auditor exam consists of two parts: a written exam and a practical exam. The written exam is four hours long and consists of 150 multiple-choice questions. The practical exam is two hours long and requires candidates to demonstrate their auditing skills in a simulated audit scenario. Upon successful completion of both exams, candidates will be awarded the PECB Certified ISO/IEC 27001 Lead Auditor certification.

>> ISO-IEC-27001-Lead-Auditor Certification Dumps <<

100% Pass 2026 High Pass-Rate PECB ISO-IEC-27001-Lead-Auditor: PECB Certified ISO/IEC 27001 Lead Auditor exam Certification Dumps

The learning material is available in three different easy-to-use formats. The first one is a ISO-IEC-27001-Lead-Auditor PDF dumps form and it is a printable and portable form. Users can save the notes by taking out prints of PECB ISO-IEC-27001-Lead-Auditor PDF questions or can access them via their smartphones, tablets, and laptops. The PECB ISO-IEC-27001-Lead-Auditor Pdf Dumps form can be used anywhere anytime and is essential for students who like to learn from their smart devices.

PECB ISO-IEC-27001-Lead-Auditor (PECB Certified ISO/IEC 27001 Lead Auditor) Exam is designed to evaluate the knowledge and skills of individuals who wish to become certified lead auditors in the field of information security management. ISO-IEC-27001-Lead-Auditor Exam is based on the ISO/IEC 27001 standard, which is internationally recognized as the leading framework for information security management systems (ISMS).

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q225-Q230):

NEW QUESTION # 225
You are performing an ISMS audit at a European-based residential nursing home called ABC that provides healthcare services. The

next step in your audit plan is to verify the effectiveness of the continual improvement process.

During the audit, you learned most of the residents' family members (90%) receive WeCare medical devices promotion advertisements through email and SMS once a week via ABC's healthcare mobile app. All of them do not agree on the use of the collected personal data for marketing or any other purposes than nursing and medical care on the signed service agreement with ABC. They have very strong reason to believe that ABC is leaking residents' and family members' personal information to a non-relevant third party and they have filed complaints.

The Service Manager says that, after investigation, all these complaints have been treated as nonconformities.

The corrective actions have been planned and implemented according to the nonconformity and corrective management procedure (Document reference ID: ISMS_L2_10.1, version 1).

You write a nonconformity which you will follow up on later. Select the words that best complete the sentence:

☐

Answer:

Explanation:

☐

Explanation:

One possible way to complete the sentence is:

"When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue." According to ISO/IEC 27001:2022, clause 10.1, the organization shall continually improve the suitability, adequacy, and effectiveness of the ISMS by evaluating the performance and the effectiveness of the ISMS, ensuring that the policy and objectives are aligned with the strategic direction of the organization, and taking actions to achieve the intended outcomes of the ISMS. One of the ways to achieve continual improvement is to identify and correct nonconformities and take actions to eliminate their causes and prevent their recurrence.

Therefore, when reviewing the effectiveness of the corrective actions, an auditor should look for evidence that the organization has analyzed the root cause of the nonconformity, implemented appropriate changes to the ISMS, and verified that the changes have resulted in the desired improvement and prevented the recurrence of the issue. References: =
* ISO/IEC 27001:2022, clause 10.1, Nonconformity and corrective action
* ISO/IEC 27001:2022, clause 10.2, Continual improvement
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION # 226

Select the words that best complete the sentence:

"The purpose of maintaining regulatory compliance in a management system is to 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:

☐

According to ISO 27001:2013, clause 5.2, the top management of an organization must establish, implement and maintain an information security policy that is appropriate to the purpose of the organization and provides a framework for setting information security objectives. The information security policy must also include a commitment to comply with the applicable legal, regulatory and contractual requirements, as well as any other requirements that the organization subscribes to. Therefore, maintaining regulatory compliance is part of fulfilling the management system policy and ensuring its effectiveness and suitability. References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 5.2
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* ISO 27001 Policy: How to write it according to ISO 27001

NEW QUESTION # 227

You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.

The next step in your audit plan is to verify the information security on ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organization outsourced the mobile app development to a professional software development company with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified. The IT Manager presented the software security management procedure and summarised the process as follows:

The mobile app development shall adopt "security-by-design" and "security-by-default" principles, as a minimum. The following security functions for personal data protection shall be available:

Access control.

Personal data encryption, i.e., Advanced Encryption Standard (AES) algorithm, key lengths: 256 bits; and Personal data pseudonymization.

Vulnerability checked and no security backdoor

You sample the latest Mobile App Test report - details as follows:

You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymization tests failed. Also, whether the Service Manager is authorized to approve the test.

The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymization functions failed is that these functions heavily slowed down the system and service performance. An extra

150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.

You sample one of the medical staff's mobile and found that ABC's healthcare mobile app, version

1.01 is installed. You found that version 1.01 has no test record.

The IT Manager explains that because of frequent ransomware attacks, the outsourced mobile app development company gave a free minor update on the tested software, performed an emergency release of the updated software, and gave a verbal guarantee that there will be no impact on any security functions. Based on his 20 years of information security experience, there is no need to re- test.

You are preparing the audit findings Select two options that are correct.

- A. There is a nonconformity (NC). The IT. Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
- B. There is NO nonconformity (NC). The IT Manager demonstrates good leadership. (Relevant to clause 5.1, control 5.4)
- C. There is an opportunity for improvement (OI). The organisation selects an external service provider based on the extent of free services it will provide. (Relevant to clause 8.1, control A.5.21)
- D. There is a nonconformity (NC). The organisation does not control planned changes and review the consequences of unintended changes. (Relevant to clause 8.1)
- E. There is NO nonconformity (NC). The IT Manager demonstrates he is fully competent. (Relevant to clause 7.2)
- F. There is an opportunity for improvement (OI). The IT Manager should make the decision to continue the service based on appropriate testing. (Relevant to clause 8.1, control A.8.30)

Answer: A,D

Explanation:

According to ISO/IEC 27001, organizations must control planned changes and review the consequences of unintended changes in order to ensure continued alignment with information security requirements. In this scenario, the organization failed to perform appropriate testing after an emergency update to the mobile app, which constitutes a nonconformity with clause 8.1 of the standard.

Reference:

- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor

ISO/IEC 27001 requires that organizations adhere to their established procedures for software security management. The IT Manager's approval of the app despite failed security tests and lack of proper documentation for the new version indicates noncompliance with the procedure, thus reflecting a nonconformity.

Reference:

- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor

NEW QUESTION # 228

During a third-party certification audit, you are presented with a list of issues by an auditee. Which four of the following constitute 'internal' issues in the context of a management system to ISO 27001:2022?

- A. A reduction in grants as a result of a change in government policy
- B. A rise in interest rates in response to high inflation
- C. Inability to source raw materials due to government sanctions
- D. Increased absenteeism as a result of poor management
- E. Poor morale as a result of staff holidays being reduced
- F. Higher labour costs as a result of an aging population
- G. Poor levels of staff competence as a result of cuts in training expenditure

- H. A fall in productivity linked to outdated production equipment

Answer: D,E,G,H

Explanation:

According to ISO 27001:2022 clause 4.1, the organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system (ISMS)12 External issues are factors outside the organisation that it cannot control, but can influence or adapt to. They include political, economic, social, technological, legal, and environmental factors that may affect the organisation's information security objectives, risks, and opportunities12 Internal issues are factors within the organisation that it can control or change. They include the organisation's structure, culture, values, policies, objectives, strategies, capabilities, resources, processes, activities, relationships, and performance that may affect the organisation's information security management system12 Therefore, the following issues are considered 'internal' in the context of a management system to ISO
27001:2022:

Poor levels of staff competence as a result of cuts in training expenditure: This is an internal issue because it relates to the organisation's capability, resource, and process of developing and maintaining the competence of its personnel involved in the ISMS. The organisation can control or change its training expenditure and its impact on staff competence12 Poor morale as a result of staff holidays being reduced: This is an internal issue because it relates to the organisation's culture, value, and relationship with its employees. The organisation can control or change its staff holiday policy and its impact on staff morale12 Increased absenteeism as a result of poor management: This is an internal issue because it relates to the organisation's performance, structure, and accountability of its management. The organisation can control or change its management practices and its impact on staff absenteeism12 A fall in productivity linked to outdated production equipment: This is an internal issue because it relates to the organisation's capability, resource, and process of ensuring the availability and suitability of its production equipment. The organisation can control or change its equipment maintenance and upgrade and its impact on productivity12 The following issues are considered 'external' in the context of a management system to ISO 27001:2022:

Higher labour costs as a result of an aging population: This is an external issue because it relates to the social and demographic factor that affects the availability and cost of labour in the market. The organisation cannot control or change the aging population, but can influence or adapt to its impact on labour costs12 A rise in interest rates in response to high inflation: This is an external issue because it relates to the economic and monetary factor that affects the cost and availability of capital in the market. The organisation cannot control or change the interest rates or inflation, but can influence or adapt to its impact on capital costs12 A reduction in grants as a result of a change in government policy: This is an external issue because it relates to the political and legal factor that affects the availability and conditions of public funding for the organisation. The organisation cannot control or change the government policy, but can influence or adapt to its impact on grants12 Inability to source raw materials due to government sanctions: This is an external issue because it relates to the political and legal factor that affects the availability and cost of raw materials in the market. The organisation cannot control or change the government sanctions, but can influence or adapt to its impact on raw materials12 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 # 229

You are performing an ISMS audit at a residential nursing home (ABC) that provides healthcare services. The next step in your audit plan is to verify the information security of ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organization outsourced the mobile app development to a professional software development company with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO
22301) and
ISMS (ISO/IEC 27001) certified.
The IT Manager presented the software security management procedure and summarised the process as following:
The mobile app development shall adopt "security-by-design" and "security-by-default" principles, as a minimum.
The following security functions for personal data protection shall be available:
Access control.
Personal data encryption, i.e., Advanced Encryption Standard (AES) algorithm, key lengths: 256 bits; and Personal data pseudonymization.
Vulnerability checked and no security backdoor
You sample the latest Mobile App Test report, details as follows:

The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymisation functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You are preparing the audit findings. Select the correct option.

- A. There is a nonconformity (NC). The organisation and developer perform security tests that fail.
  (Relevant to clause 8.1, control A.8.29)
- B. There is NO nonconformity (NC). The Service Manager makes a good decision to continue the service.
  (Relevant to clause 8.1, control A.8.30)
- C. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure.
  (Relevant to clause 8.1, control A.8.30)
- D. There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.
  (Relevant to clause 8.1, control A.8.29)

Answer: C

NEW QUESTION # 230
......