

Valid ISO-IEC-27001-Lead-Implementer Premium VCE Braindumps Materials - Itexamguide



DOWNLOAD the newest Itexamguide ISO-IEC-27001-Lead-Implementer PDF dumps from Cloud Storage for free:
https://drive.google.com/open?id=1nGVfHIPaAEDj6KzJ4Zbfl2_NufFsShkt

This society is ever – changing and the test content will change with the change of society. You don't have to worry that our ISO-IEC-27001-Lead-Implementer study materials will be out of date. In order to keep up with the change direction of the exam, our question bank has been constantly updated. We have dedicated IT staff that checks for updates every day and sends them to you automatically once they occur. The update for our ISO-IEC-27001-Lead-Implementer Study Materials will be free for one year and half price concession will be offered one year later.

Achieving the PECB ISO-IEC-27001-Lead-Implementer Certification demonstrates a candidate's ability to implement and manage a robust ISMS that meets the requirements of the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification can enhance a candidate's career prospects and credibility in the field of information security and can also benefit organizations by ensuring that their information assets are well-protected.

>> **Training ISO-IEC-27001-Lead-Implementer Kit** <<

Vce PECB ISO-IEC-27001-Lead-Implementer Format | Latest Study ISO-IEC-27001-Lead-Implementer Questions

The certificate is of significance in our daily life. At present we will provide all candidates who want to pass the ISO-IEC-27001-Lead-Implementer exam with three different versions for your choice. Any of the three versions can work in an offline state, and the version makes it possible that the websites is available offline. If you use the quiz prep, you can use our latest ISO-IEC-27001-

Lead-Implementer Exam Torrent in anywhere and anytime. How can you have the chance to enjoy the study in an offline state? You just need to download the version that can work in an offline state, and the first time you need to use the version of our ISO-IEC-27001-Lead-Implementer quiz torrent online.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q108-Q113):

NEW QUESTION # 108

Which approach should organizations use to implement an ISMS based on ISO/IEC 27001?

- A. An approach that is suitable for organization's scope
- B. Only the approach provided by the standard
- C. Any approach that enables the ISMS implementation within the 12month period

Answer: A

Explanation:

ISO/IEC 27001:2022 does not prescribe a specific approach for implementing an ISMS, but rather provides a set of requirements and guidelines that can be adapted to the organization's context, scope, and objectives. Therefore, organizations can use any approach that is suitable for their scope, as long as it meets the requirements of the standard and enables the achievement of the intended outcomes of the ISMS. The approach should also consider the needs and expectations of the interested parties, the risks and opportunities related to information security, and the legal and regulatory obligations of the organization.

NEW QUESTION # 109

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

- A. Personal data protection legislation
- B. ISO/IEC 27002:2005
- C. Intellectual Property Rights
- D. ISO/IEC 27001:2005

Answer: A

NEW QUESTION # 110

Question:

An organization has compared its actual performance against predetermined performance targets. What is the primary purpose of this action?

- A. To eliminate the need for manual tracking and reporting
- B. To assess whether the organization's security objectives are being met
- C. To verify that all security incidents are resolved

Answer: B

Explanation:

ISO/IEC 27001:2022 Clause 9.1 -Monitoring, measurement, analysis, and evaluation:

"The organization shall evaluate the performance and effectiveness of the information security management system. The evaluation shall include... comparison against performance indicators and security objectives." The purpose is to ensure that security objectives (Clause 6.2) are being met. Measuring performance allows organizations to determine whether controls and processes are effective and aligned with strategic goals.

Option A is too narrow, and Option C is incorrect because manual tracking may still be required in some cases.

NEW QUESTION # 111

FinanceX, a well-known financial institution, uses an online banking platform that enables clients to easily and securely access their bank accounts. To log in, clients are required to enter the one-time authorization code sent to their smartphone. What can be concluded from this scenario?

- A. FinanceX has implemented an integrity control that avoids the involuntary corruption of data
- B. FinanceX has incorrectly implemented a security control that could become a vulnerability
- C. FinanceX has implemented a security control that ensures the confidentiality of information

Answer: C

Explanation:

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. A security control is a measure that is put in place to protect the confidentiality, integrity, and availability of information assets. In this scenario, FinanceX has implemented a security control that ensures the confidentiality of information by requiring clients to enter a one-time authorization code sent to their smartphone when they log in to their online banking platform. This control prevents unauthorized access to the clients' bank accounts and protects their sensitive information from being disclosed to third parties. The one-time authorization code is a form of two-factor authentication, which is a security technique that requires two pieces of evidence to verify the identity of a user. In this case, the two factors are something the user knows (their username and password) and something the user has (their smartphone). Two-factor authentication is a recommended security control for online banking platforms, as it provides a higher level of security than single-factor authentication, which relies only on one piece of evidence, such as a password.

NEW QUESTION # 112

Scenario 7: InfoSec is a multinational corporation headquartered in Boston, MA, which provides professional electronics, gaming, and entertainment services. After facing numerous information security incidents, InfoSec has decided to establish teams and implement measures to prevent potential incidents in the future. Emma, Bob, and Anna were hired as the new members of InfoSec's information security team, which consists of a security architecture team, an incident response team (IRT) and a forensics team. Emma's job is to create information security plans, policies, protocols, and training to prepare InfoSec to respond to incidents effectively. Emma and Bob would be full-time employees of InfoSec, whereas Anna was contracted as an external consultant. Bob, a network expert, will deploy a screened subnet network architecture. This architecture will isolate the demilitarized zone (DMZ) to which hosted public services are attached and InfoSec's publicly accessible resources from their private network. Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company's network. Bob is also responsible for ensuring that a thorough evaluation of the nature of an unexpected event is conducted, including the details on how the event happened and what or whom it might affect.

Anna will create records of the data, reviews, analysis, and reports in order to keep evidence for the purpose of disciplinary and legal action, and use them to prevent future incidents. To do the work accordingly, she should be aware of the company's information security incident management policy beforehand. Among others, this policy specifies the type of records to be created, the place where they should be kept, and the format and content that specific record types should have.

Why did InfoSec establish an IRT? Refer to scenario 7.

- A. To assess, respond to, and learn from information security incidents
- B. To comply with the ISO/IEC 27001 requirements related to incident management
- C. To collect, preserve, and analyze the information security incidents

Answer: A

Explanation:

Based on his tasks, Bob is part of the incident response team (IRT) of InfoSec. According to the ISO/IEC 27001:2022 standard, an IRT is a group of individuals who are responsible for responding to information security incidents in a timely and effective manner. The IRT should have the authority, skills, and resources to perform the following activities:

- * Identify and analyze information security incidents and their impact
 - * Contain, eradicate, and recover from information security incidents
 - * Communicate with relevant stakeholders and authorities
 - * Document and report on information security incidents and their outcomes
 - * Review and improve the information security incident management process and controls
- Bob's job is to deploy a network architecture that can prevent potential attackers from accessing InfoSec's private network, and to conduct a thorough evaluation of the nature and impact of any unexpected events that might occur. These tasks are aligned with the objectives and responsibilities of an IRT, as defined by the ISO/IEC 27001:2022 standard.

NEW QUESTION # 113

.....

