

New ISO-IEC-27001-Lead-Implementer Exam Labs | ISO-IEC-27001-Lead-Implementer Reliable Dumps Ebook



BTW, DOWNLOAD part of BraindumpsPass ISO-IEC-27001-Lead-Implementer dumps from Cloud Storage:
<https://drive.google.com/open?id=1fuLTb-oedAv6DZn0Soe11v1BxkxFXGGN>

Your life will take place great changes after obtaining the ISO-IEC-27001-Lead-Implementer certificate. Many companies like to employ versatile and comprehensive talents. What you have learnt on our ISO-IEC-27001-Lead-Implementer preparation prep will meet their requirements. So you will finally stand out from a group of candidates and get the desirable job. At the same time, what you have learned from our ISO-IEC-27001-Lead-Implementer Exam Questions are the latest information in the field, so that you can obtain more skills to enhance your capacity.

Passing the PECB ISO-IEC-27001-Lead-Implementer Certification Exam demonstrates that the candidate has the necessary expertise and competencies to implement an effective and efficient ISMS based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification is recognized globally and is highly valued by employers, as it validates the candidate's ability to protect an organization's sensitive information and ensure its compliance with regulatory requirements.

>> New ISO-IEC-27001-Lead-Implementer Exam Labs <<

ISO-IEC-27001-Lead-Implementer Reliable Dumps Ebook | Examcollection ISO-IEC-27001-Lead-Implementer Dumps Torrent

Our ISO-IEC-27001-Lead-Implementer learning materials are carefully compiled by industry experts based on the examination questions and industry trends in the past few years. The knowledge points are comprehensive and focused. You don't have to worry about our learning from ISO-IEC-27001-Lead-Implementer exam question. We assure you that our ISO-IEC-27001-Lead-Implementer learning materials are easy to understand and use the fewest questions to convey the most important information. As long as you follow the steps of our ISO-IEC-27001-Lead-Implementer quiz torrent, your mastery of knowledge will be very comprehensive and you will be very familiar with the knowledge points. This will help you pass the exam more smoothly. The ISO-IEC-27001-Lead-Implementer learning materials are of high quality, mainly reflected in the adoption rate. As for our ISO-IEC-27001-Lead-Implementer Exam Question, we guaranteed a higher passing rate than that of other agency. More importantly, we will

promptly update our ISO-IEC-27001-Lead-Implementer quiz torrent based on the progress of the letter and send it to you. 99% of people who use our ISO-IEC-27001-Lead-Implementer quiz torrent has passed the exam and successfully obtained their certificates, which undoubtedly show that the passing rate of our ISO-IEC-27001-Lead-Implementer exam question is 99%. So our product is a good choice for you. Choose our ISO-IEC-27001-Lead-Implementer learning materials, you will gain a lot and lay a solid foundation for success.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q175-Q180):

NEW QUESTION # 175

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration testing and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties. In addition, the top management of Operaze decided to include most of the company's departments within the ISMS scope. The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties. In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled. However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company. Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company. Based on scenario 5, in which category of the interested parties does the HR manager of Operaze belong?

- A. Both A and B
- B. Positively influenced interested parties, because the ISMS will increase the effectiveness and efficiency of the HR Department
- C. Negatively influenced interested parties, because the HR Department will deal with more documentation

Answer: C

Explanation:

According to ISO/IEC 27001, interested parties are those who can affect, be affected by, or perceive themselves to be affected by the organization's information security activities, products, or services. Interested parties can be classified into four categories based on their influence and interest in the ISMS:

Positively influenced interested parties: those who benefit from the ISMS and support its implementation and operation

Negatively influenced interested parties: those who are adversely affected by the ISMS and oppose its implementation and operation

High-interest interested parties: those who have a strong interest in the ISMS and its outcomes, regardless of their influence

Low-interest interested parties: those who have a weak interest in the ISMS and its outcomes, regardless of their influence

In scenario 5, the HR manager of Operaze belongs to the category of negatively influenced interested parties, because he/she perceives that the ISMS will create more paperwork and documentation for the HR Department, and therefore opposes its implementation and operation. The HR manager does not benefit from the ISMS and does not support its objectives and requirements.

Reference:

ISO/IEC 27001:2013, clause 4.2: Understanding the needs and expectations of interested parties ISO/IEC 27001:2013, Annex

A.18.1.4: Assessment of and decision on information security events ISO/IEC 27001 Lead Implementer Course, Module 2:

Introduction to Information Security Management System (ISMS) concepts as required by ISO/IEC 27001 ISO/IEC 27001 Lead

Implementer Course, Module 4: Planning the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module

6: Implementing the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 7: Performance

evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course,

Module 8: Continual improvement of the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 9:

Preparing for the ISMS certification audit

NEW QUESTION # 176

Scenario 10: ProEBank

ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leverages the city's advanced technological and financial ecosystem. To enhance its security posture, ProEBank has implemented an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.

To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them. Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.

During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential conflict of interest with one of the auditors, who had previously worked for ProEBank's main competitor in the banking industry. To ensure the integrity of the audit process, ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team. After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.

Three weeks later, the team conducted an on-site visit to the auditee's location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001, was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit, the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected. The audit team leader then issued a recommendation for certification.

After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body. To prepare for their ISO/IEC 27001 certification audit, ProEBank trained employees, prepared documentation, and identified key personnel to support the audit. However, they did not conduct a self-assessment before the audit.

Did ProEBank follow all of the best practices while preparing for the certification audit?

- A. No - the company should not have informed its employees regarding the upcoming audit
- B. Yes - the company followed all of the best practices in preparation for the certification audit
- C. No - the company should have also conducted a self-assessment to prepare for the audit

Answer: C

NEW QUESTION # 177

Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB, a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately, Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.

To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Based on scenario 3, which information security control of Annex A of ISO/IEC 27001 did Socket Inc.

implement by establishing a new system to maintain, collect, and analyze information related to information security threats?

- A. Annex A 5.5 Contact with authorities
- B. Annex A 5.7 Threat Intelligence
- C. Annex A 5.13 Labeling of information

Answer: B

Explanation:

Annex A 5.7 Threat Intelligence is a new control in ISO 27001:2022 that aims to provide the organisation with relevant information

regarding the threats and vulnerabilities of its information systems and the potential impacts of information security incidents. By establishing a new system to maintain, collect, and analyze information related to information security threats, Socket Inc. implemented this control and improved its ability to prevent, detect, and respond to information security incidents.

References:

* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A 5.7 Threat Intelligence

* ISO/IEC 27002:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection controls, Clause 5.7 Threat Intelligence

* PECB ISO/IEC 27001:2022 Lead Implementer Course, Module 6: Implementation of Information Security Controls Based on ISO/IEC 27002:2022, Slide 18: A.5.7 Threat Intelligence

NEW QUESTION # 178

What is the main purpose of Annex A 7.1 Physical security perimeters of ISO/IEC 27001?

- A. To prevent unauthorized physical access, damage, and interference to the organization's information and other associated assets
- B. To maintain the confidentiality of information that is accessible by personnel or external parties
- C. To ensure access to information and other associated assets is defined and authorized

Answer: A

Explanation:

Explanation

Annex A 7.1 of ISO/IEC 27001 : 2022 is a control that requires an organization to define and implement security perimeters and use them to protect areas that contain information and other associated assets.

Information and information security assets can include data, infrastructure, software, hardware, and personnel. The main purpose of this control is to prevent unauthorized physical access, damage, and interference to these assets, which could compromise the confidentiality, integrity, and availability of the information. Physical security perimeters can include fences, walls, gates, locks, alarms, cameras, and other barriers or devices that restrict or monitor access to the facility or area. The organization should also consider the environmental and fire protection of the assets, as well as the disposal of any waste or media that could contain sensitive information.

References:

ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Section 5.3.1.7, page 101 ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 17 ISO/IEC 27002 : 2022, Control 7.1 - Physical Security Perimeters 123

NEW QUESTION # 179

What is the best description of a risk analysis?

- A. A risk analysis calculates the exact financial consequences of damages.
- B. A risk analysis is a method of mapping risks without looking at company processes.
- C. A risk analysis helps to estimate the risks and develop the appropriate security measures.

Answer: C

NEW QUESTION # 180

.....

When we get into the job, our ISO-IEC-27001-Lead-Implementer training materials may bring you a bright career prospect. Companies need employees who can create more value for the company, but your ability to work directly proves your value. Our ISO-IEC-27001-Lead-Implementer certification guide can help you improve your ability to work in the shortest amount of time, for more promotion opportunities and space for development. Believe it or not that up to you, our ISO-IEC-27001-Lead-Implementer Training Materials are powerful and useful, it can solve all your stress and difficulties in reviewing the ISO-IEC-27001-Lead-Implementer exams.

ISO-IEC-27001-Lead-Implementer Reliable Dumps Ebook: <https://www.braindumps.com/PECB/ISO-IEC-27001-Lead-Implementer-practice-exam-dumps.html>

- Updated PECB ISO-IEC-27001-Lead-Implementer Exam Questions for ISO-IEC-27001-Lead-Implementer Exam

