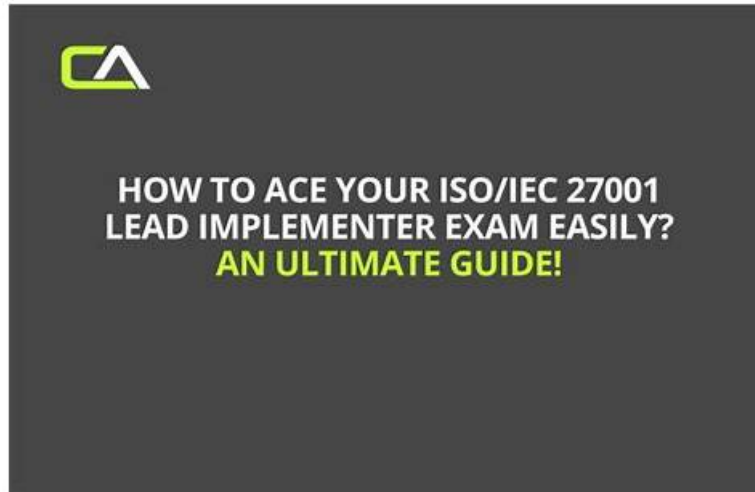


Valid ISO-IEC-27001-Lead-Implementer Exam Bootcamp & Official ISO-IEC-27001-Lead-Implementer Practice Test



BONUS!!! Download part of itPass4sure ISO-IEC-27001-Lead-Implementer dumps for free: <https://drive.google.com/open?id=133xEXT-TwinIo2BkDoByqgvag2XJEL7>

No matter in the day or on the night, you can consult us the relevant information about our ISO-IEC-27001-Lead-Implementer preparation exam through the way of chatting online or sending emails. I'm sure our 24-hour online service will not disappoint you as we offer our service 24/7 on our ISO-IEC-27001-Lead-Implementer Study Materials. And we will give you the most considerate suggestions on our ISO-IEC-27001-Lead-Implementer learning guide with all our sincere and warm heart.

PECB ISO-IEC-27001-Lead-Implementer certification exam is designed for individuals who aspire to become certified in implementing an information security management system (ISMS) based on the ISO/IEC 27001 standard. ISO-IEC-27001-Lead-Implementer exam is offered by the Professional Evaluation and Certification Board (PECB), a leading provider of professional certifications in various fields.

PECB Certified ISO/IEC 27001 Lead Implementer exam is a four-hour exam that consists of multiple-choice questions. ISO-IEC-27001-Lead-Implementer exam covers various topics related to the implementation and management of an ISMS, including the ISO/IEC 27001 standard, risk assessment, risk treatment, performance evaluation, and improvement of an ISMS. ISO-IEC-27001-Lead-Implementer exam is designed to evaluate the candidate's knowledge, skills, and understanding of the ISMS implementation process and their ability to manage an ISMS in an organization. Successful completion of the exam and the certification process demonstrates the candidate's proficiency in implementing and managing an ISMS based on the ISO/IEC 27001 standard.

PECB ISO-IEC-27001-Lead-Implementer Certification Exam is a globally recognized certification that validates the expertise of individuals in implementing and managing an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification exam focuses on the necessary skills and knowledge to effectively plan, implement, manage, and maintain an ISMS in any organization. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification exam is designed to provide professionals with a comprehensive understanding of the principles, methodologies, and techniques for implementing and managing an ISMS in accordance with the ISO/IEC 27001 standard.

>> Valid ISO-IEC-27001-Lead-Implementer Exam Bootcamp <<

Official ISO-IEC-27001-Lead-Implementer Practice Test & Braindumps ISO-IEC-27001-Lead-Implementer Torrent

It would be really helpful to purchase PECB Certified ISO/IEC 27001 Lead Implementer Exam exam dumps right away. If you buy this PECB Certification Exams product right now, we'll provide you with up to 1 year of free updates for ISO-IEC-27001-Lead-

Implementer authentic questions. You can prepare using these no-cost updates in accordance with the most recent test content changes provided by the ISO-IEC-27001-Lead-Implementer Exam Dumps. The ISO-IEC-27001-Lead-Implementer actual questions we sell also come with a free demo.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q133-Q138):

NEW QUESTION # 133

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.

What is the next step that Operaze's ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.

- A. Obtain top management's approval for the information security policy
- B. Communicate the information security policy to all employees
- C. Implement the information security policy

Answer: A

Explanation:

According to ISO/IEC 27001 : 2022 Lead Implementer, the information security policy is a high-level document that defines the organization's objectives, principles, and commitments regarding information security. The policy should be aligned with the organization's strategic direction and context, and should provide a framework for setting information security objectives and establishing the ISMS. The policy should also be approved by top management, who are ultimately responsible for the ISMS and its performance.

Therefore, after drafting the information security policy, the next step that Operaze's ISMS implementation team should take is to obtain top management's approval for the policy. This will ensure that the policy is consistent with the organization's vision and values, and that it has the necessary support and resources for its implementation and maintenance.

NEW QUESTION # 134

According to ISO/IEC 27000, which of the following best describes the possible scope of a management system?

- A. It should cover the entire organization without exceptions
- B. It is limited to IT infrastructure and cannot include non-technical departments
- C. It can vary to include the entire organization or specific sections, depending on the needs

Answer: C

NEW QUESTION # 135

Company X restricted the access of the internal auditor of some of its documentation taking into account its confidentiality. Is this acceptable?

- A. No. restricting the internal auditor's access to offices and documentation can negatively affect the internal audit process
- B. Yes. confidential information should not be increased by internal auditors
- C. Yes. it is up to the company to determine what an internal auditor can access

Answer: A

NEW QUESTION # 136

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation.

SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Is Alex suitable for the position of internal auditor within the company?

- A. Yes, Alex's recent experience in the day-to-day operations of the Compliance Department would benefit the internal auditor role
- B. No, the internal audit can be conducted only by individuals who have not had operational roles
- C. No, Alex should wait for a reasonable period of time to pass before transitioning to the internal auditor position

Answer: B

NEW QUESTION # 137

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. Based on scenario 7, what should Anna be aware of when gathering data?

Answer: A

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, Disposable vapes

2025 Latest itPass4sure ISO-IEC-27001-Lead-Implementer PDF Dumps and ISO-IEC-27001-Lead-Implementer Exam Engine
Free Share: <https://drive.google.com/open?id=133xEXT-TwinIo2BkDoByqgvvag2XJEL7>