Free PDF Quiz PECB - ISO-IEC-27001-Lead-Implementer–High-quality Trustworthy Source

P.S. Free & New ISO-IEC-27001-Lead-Implementer dumps are available on Google Drive shared by PassCollection: https://drive.google.com/open?id=1qIkbWwjNwLxdHNw7kFIJ6QBGRD8E8zaG

A lot of our candidates used up all examination time and leave a lot of unanswered questions of the ISO-IEC-27001-Lead-Implementer exam questions. It is a bad habit. In your real exam, you must answer all questions in limited time. So you need our timer to help you on ISO-IEC-27001-Lead-Implementer Practice Guide. Our timer is placed on the upper right of the page. The countdown time will run until it is time to submit your exercises of the ISO-IEC-27001-Lead-Implementer study materials. Also, it will remind you when the time is soon running out.

To prepare for the PECB ISO-IEC-27001-Lead-Implementer certification exam, candidates can attend training courses offered by PECB or other authorized training providers. They can also study the ISO/IEC 27001 standard and related materials, such as the ISO/IEC 27002 standard, and practice implementing and managing an ISMS in a real-world setting. By passing the exam and obtaining the PECB Certified ISO/IEC 27001 Lead Implementer certification, professionals can demonstrate their expertise and commitment to information security management.

PECB ISO-IEC-27001-Lead-Implementer Certification Exam is an essential certification for professionals who wish to specialize in information security management and implement an ISMS based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification demonstrates the candidate's knowledge, skills, and expertise in implementing an effective and efficient ISMS, which is crucial in today's digital age.

>> Trustworthy ISO-IEC-27001-Lead-Implementer Source <<

ISO-IEC-27001-Lead-Implementer Certification Dumps - ISO-IEC-27001-Lead-Implementer Exam Objectives Pdf

We know that it is hard to stay and study for the PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer) exam dumps in one place for a long time. Therefore, you have the option to use PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer) PDF questions anywhere and anytime. PassCollection PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer) dumps are designed according to

the PECB ISO-IEC-27001-Lead-Implementer Certification Exam standard and have hundreds of questions similar to the actual PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer) exam. PassCollection PECB Certified ISO/IEC 27001 Lead Implementer Exam (ISO-IEC-27001-Lead-Implementer) web-based practice exam software also works without installation.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q190-Q195):

NEW QUESTION # 190
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decidedto implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.
One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues What is the difference between training and awareness? Refer to scenario 6.

- A. Training helps acquire certain skills, whereas awareness develops certain habits and behaviors.
- B. Training helps transfer a message with the intent of informing, whereas awareness helps change the behavior toward the message
- C. Training helps acquire a skill, whereas awareness helps apply it in practice

Answer: A

Explanation:
According to ISO/IEC 27001, training and awareness are two different but complementary activities that aim to enhance the information security competence and performance of the organization's personnel. Training is the process of providing instruction and guidance to help individuals acquire certain skills, knowledge, or abilities related to information security. Awareness is the process of raising the level of consciousness and understanding of the importance and benefits of information security, and developing certain habits and behaviors that support the information security objectives and requirements.
In scenario 6, Colin is holding a training and awareness session for the personnel of Skyver, which means he is combining both activities to achieve a more effective and comprehensive information security education. The training part of the session covers topics such as Skyver's information security policies and procedures, and techniques for mitigating phishing and malware. The awareness part of the session covers topics such as Skyver's information security approaches and challenges, and the benefits of information security for the organization and its customers. The purpose of the session is to help the personnel acquire the necessary skills to perform their information security roles and responsibilities, and to develop the appropriate habits and behaviors to protect the information assets of the organization.
References:
* ISO/IEC 27001:2013, clause 7.2.2: Information security awareness, education and training
* 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
* ISO 27001 Security Awareness Training and Compliance - InfosecTrain1
* ISO/IEC 27001 compliance and cybersecurity awareness training2
* ISO 27001 Free Training | Online Course | British Assessment Bureau

NEW QUESTION # 191
Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.

Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity,the audit findings, and recommendations.
Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management
How does SunDee's negligence affect the ISMS certificate? Refer to scenario 8.

- A. SunDee might not be able to renew the ISMS certificate, because it has not conducted management reviews at planned intervals
- B. SunDee might not be able to renew the ISMS certificate, because the internal audit lasted longer than planned
- C. SunDee will renew the ISMS certificate, because it has conducted an Internal audit to evaluate the ISMS effectiveness

Answer: A

Explanation:
According to ISO/IEC 27001:2013, clause 9.3, the top management of an organization must review the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review must consider the status of actions from previous management reviews, changes in external and internal issues, the performance and effectiveness of the ISMS, feedback from interested parties, results of risk assessment and treatment, and opportunities for continual improvement. The management review must also result in decisions and actions related to the ISMS policy and objectives, resources, risks and opportunities, and improvement. The management review is a critical process that demonstrates the commitment and involvement of the top management in the ISMS and its alignment with the strategic direction of the organization. The management review also provides input for the internal audit and the certification audit.
SunDee has neglected to conduct management reviews regularly, which means that it has not fulfilled the requirement of clause 9.3. This is a major nonconformity that could jeopardize the renewal of the ISMS certificate. The certification body will verify whether SunDee has conducted management reviews and whether they have been effective and documented. If SunDee cannot provide evidence of management reviews, it will have to take corrective actions and undergo a follow-up audit before the certificate can be renewed. Alternatively, the certification body may decide to suspend or withdraw the certificate if SunDee fails to address the nonconformity within a specified time frame.
References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 9.3
* PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001
* PECB, ISO/IEC 27001 Lead Implementer Exam Preparation Guide, Section 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001

NEW QUESTION # 192
Which statement is an example of risk retention?

- A. An organization has implemented a data loss protection software
- B. An organization terminates work in the construction site during a severe storm
- C. An organization has decided to release the software even though some minor bugs have not been fixed yet

Answer: C

Explanation:
Explanation
According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, either because the bugs are not critical or because the cost of fixing them would outweigh the benefits.
References:
ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process
3, ISO 27001: Top risk treatment options and controls explained

NEW QUESTION # 193
Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.
Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:
A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department The approved action plan was implemented and all actions described in the plan were documented.
Based on scenario 9. did the ISMS project manager complete the corrective action process appropriately?

- A. No, the corrective action process should also include the review of the implementation of the selected actions
- B. Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions
- C. No, the corrective action did not address the root cause of the nonconformity

Answer: A

Explanation:
According to ISO/IEC 27001:2022, the corrective action process consists of the following steps12:
* Reacting to the nonconformity and, as applicable, taking action to control and correct it and deal with the consequences
* Evaluating the need for action to eliminate the root cause(s) of the nonconformity, in order that it does not recur or occur elsewhere
* Implementing the action needed
* Reviewing the effectiveness of the corrective action taken
* Making changes to the information security management system, if necessary In scenario 9, the ISMS project manager did not complete the last step of reviewing the effectiveness of the corrective action taken. This step is important to verify that the corrective action has achieved the intended results and that no adverse effects have been introduced. The review can be done by using various methods, such as audits, tests, inspections, or performance indicators3. Therefore, the ISMS project manager did not complete the corrective action process appropriately.

NEW QUESTION # 194
Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed.
Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc.
implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations.
Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.
Socket Inc. safeguarded its information processing facilities against power failures and other disruptions.
Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc.
used data masking based on the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.
The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.
Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.
Based on the scenario above, answer the following question:
Based on scenario 3, did Socket Inc. adhere to the requirements of ISO/IEC 27001 regarding ISMS documented information?

- A. Yes, there is no mandatory requirement on how to document processes or security controls in the standard
- B. Yes, the standard requires that all security controls be included in a single document
- C. No, Socket Inc. consolidated all controls of a group into a single document while the standard requires the controls to be documented in four groups

Answer: A

NEW QUESTION # 195
.....

If you intend to take the PECB ISO-IEC-27001-Lead-Implementer exam to open doors to high-paying jobs, you need an authentic PECB ISO-IEC-27001-Lead-Implementer practice exam material to get a passing score on the first attempt. Many people do not find a platform that is credible to purchase updated PECB ISO-IEC-27001-Lead-Implementer prep material. This leads to a waste of time and money, and ultimately failure in the ISO-IEC-27001-Lead-Implementer exam.