First-hand PECB Pdf ISO-IEC-27001-Lead-Implementer Pass Leader - ISO-IEC-27001-Lead-Implementer Vce PECB Certified ISO/IEC 27001 Lead Implementer Exam Torrent

P.S. Free 2026 PECB ISO-IEC-27001-Lead-Implementer dumps are available on Google Drive shared by PrepAwayPDF: https://drive.google.com/open?id=1t1Dyas5thiutoNd843-AACDEdVh4iA05

You plan to place an order for our PECB ISO-IEC-27001-Lead-Implementer test questions answers; you should have a credit card. Mostly we just support credit card. If you just have debit card, you should apply a credit card or you can ask other friend to help you pay for ISO-IEC-27001-Lead-Implementer test questions answers. Normally we suggest candidates to pay by PayPal, here it is no need for you to have a PayPal account. When you click PayPal it will transfer to credit card payment. If you choose SWREG payment for ISO-IEC-27001-Lead-Implementer Test Questions Answers, it will have extra tax for some countries.

PECB ISO-IEC-27001-Lead-Implementer exam is a certification program offered by the Professional Evaluation and Certification Board (PECB) that focuses on the implementation of information security management systems (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification is designed for individuals who are responsible for implementing and maintaining information security management systems within an organization. ISO-IEC-27001-Lead-Implementer Exam Tests the candidate's knowledge and expertise in implementing and managing an ISMS, risk assessment, and compliance with legal and regulatory requirements. The PECB ISO-IEC-27001-Lead-Implementer certification is a globally recognized credential that demonstrates the candidate's proficiency in implementing and managing an ISMS in accordance with the ISO/IEC 27001 standard.

>> Pdf ISO-IEC-27001-Lead-Implementer Pass Leader <<

Vce PECB ISO-IEC-27001-Lead-Implementer Torrent, Latest ISO-IEC-27001-Lead-Implementer Test Prep

Many exam candidates feel hampered by the shortage of effective ISO-IEC-27001-Lead-Implementer practice materials, and the thick books and similar materials causing burden for you. Serving as indispensable choices on your way of achieving success

especially during this exam, more than 98 percent of candidates pass the exam with our ISO-IEC-27001-Lead-Implementer practice materials and all of former candidates made measurable advance and improvement. All ISO-IEC-27001-Lead-Implementer practice materials fall within the scope of this exam for your information. The content is written promptly and helpfully because we hired the most processional experts in this area to compile the PECB Certified ISO/IEC 27001 Lead Implementer Exam practice materials.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q130-Q135):

NEW QUESTION # 130
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.
Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
Based on scenario 2, which information security principle is the IT team aiming to ensure by establishing a user authentication process that requires user identification and password when accessing sensitive information?

- A. Confidentiality
- B. Integrity
- C. Availability

Answer: A

Explanation:
Explanation
Confidentiality is one of the three information security principles, along with integrity and availability, that form the CIA triad. Confidentiality means protecting information from unauthorized access or disclosure, and ensuring that only those who are authorized to view or use it can do so. Confidentiality is essential for preserving the privacy and trust of the information owners, such as customers, employees, or business partners.
The IT team of Beauty is aiming to ensure confidentiality by establishing a user authentication process that requires user identification and password when accessing sensitive information. User authentication is a security control that verifies the identity and credentials of the users who attempt to access a system or network, and grants or denies them access based on their authorization level. User authentication helps to prevent unauthorized users, such as hackers, competitors, or malicious insiders, from accessing confidential information that they are not supposed to see or use. User authentication also helps to create an audit trail that records who accessed what information and when, which can be useful for accountability and compliance purposes.
References:
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls What is Information Security | Policy, Principles & Threats | Imperva1 What is information security? Definition, principles, and jobs2 What is Information Security? Principles, Types - KnowledgeHut3

NEW QUESTION # 131
NeuroTrustMed is a leading medical technology company based in Seoul, South Korea. The company specializes in developing AI-assisted neuroimaging solutions used in early diagnosis and treatment planning for neurological disorders. As a data-intensive company handling sensitive patient health records and medical research data, NeuroTrustMed places a strong emphasis on

cybersecurity and regulatory compliance. The company has maintained an ISO/IEC 27001-certified ISMS for the past three years. It continuously reviews and improves its ISMS to address emerging threats, support innovation in medical diagnostics, and maintain stakeholder trust. As part of its commitment to continual improvement, NeuroTrustMed actively tracks potential nonconformities, performs root-cause analyses, implements corrective and preventive actions, and ensures all changes are documented and aligned with the company's strategic objectives. When a new data protection regulation came into effect affecting cross-regional data handling, the information security team conducted a gap assessment between current policies and the new regulation. Then, it updated relevant documentation and processes to meet compliance. Following these revisions, NeuroTrustMed updated the ISMS documentation and added a new entry in the improvement register. The register, maintained in the form of a structured spreadsheet, included a unique change number, a description of the update, and a high-priority classification due to legal compliance, the dates of initiation and completion, and the sign-off by the information security manager. Around the same period, during a scheduled management review, the information security team also identified a pattern of onboarding errors. While these had not resulted in any data breaches, they posed a risk of unauthorized access. In response, the onboarding procedure was revised and an automated verification step was added to ensure accuracy before access is granted. To understand the underlying cause, the team collected data on the provisioning process. They analyzed process logs, interviewed onboarding staff, and traced access errors back to a misconfigured step in the HR-to-IT handover workflow. The team validated this finding through test cases before implementing any changes. Once confirmed, the information security team documented the nonconformity in the ISMS log. The documentation included a description of the issue, impacted systems, affected users, and a brief risk assessment of potential consequences related to access management. Based on the scenario above, answer the following question.
According to scenario 9. did NeuroTrustMed document the change in accordance with continual improvement practices?

- A. Yes, the change was documented in a structured spreadsheet with appropriate metadata and formal approval.
- B. No, changes should only be recorded if they result from nonconformities.
- C. No, the register should have been implemented in the form of a database rather than a spreadsheet.

Answer: A

Explanation:
NeuroTrustMed documented the ISMS change in full accordance with continual improvement practices, making Option C the correct answer.
ISO/IEC 27001:2022 Clause 10.1 - Continual improvement and Clause 10.2 - Nonconformity and corrective action require organizations to:
* Record changes,
* Track actions taken,
* Retain documented information as evidence.
The scenario states that NeuroTrustMed maintained an improvement register containing:
* A unique change number,
* Description of the update,
* Priority classification,
* Initiation and completion dates,
* Formal sign-off by the information security manager.
This fully satisfies Clause 7.5 - Documented information and demonstrates controlled, auditable improvement.
* Option A is incorrect because ISO/IEC 27001 does not mandate a database over a spreadsheet.
* Option B is incorrect because improvements may result from regulatory changes, risks, or opportunities-not only nonconformities.

NEW QUESTION # 132
The identified owner of an asset is always an individual

- A. True
- B. False

Answer: B

NEW QUESTION # 133
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.
Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only

authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out- of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
According to scenario 2. Beauty has reviewed all user access rights. What type of control is this?

- A. Corrective and managerial
- B. Legal and technical
- C. Detective and administrative

Answer: C

Explanation:
* Preventive controls: These are controls that aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Examples of preventive controls are encryption, firewalls, locks, policies, etc.
* Detective controls: These are controls that aim to detect or discover the occurrence of a security incident or its symptoms. Examples of detective controls are logs, alarms, audits, etc.
* Corrective controls: These are controls that aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact. Examples of corrective controls are backups, recovery plans, incident response teams, etc.
* Administrative controls: These are controls that involve the management and governance of information security, such as policies, procedures, roles, responsibilities, awareness, training, etc.
* Technical controls: These are controls that involve the use of technology or software to implement information security, such as encryption, firewalls, anti-malware, authentication, etc.
* Physical controls: These are controls that involve the protection of physical assets or locations from unauthorized access, damage, or theft, such as locks, fences, cameras, guards, etc.
* Legal controls: These are controls that involve the compliance with laws, regulations, contracts, or agreements related to information security, such as privacy laws, data protection laws, confidentiality agreements, etc.
In scenario 2, the action of Beauty reviewing all user access rights is best described as a "Preventive and Administrative" control.
* Preventive Control: The review of user access rights is a preventive measure. It is designed to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to specific files. By controlling access rights, the organization aims to prevent potential security breaches and protect sensitive data.
* Administrative Control: This action also falls under administrative controls, sometimes referred to as managerial controls. These controls involve policies, procedures, and practices related to the management of the organization and its employees. In this case, the review of access rights is a part of the company's administrative procedures to manage the security of information systems.

NEW QUESTION # 134
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j