

2026 PECB Realistic Hot ISO-IEC-27001-Lead-Implementer Questions Free PDF Quiz

NEW QUESTION # 40

What do employees need to know to report a security incident?

- A. Who is responsible for the incident and whether it was intentional.
- B. The measures that should have been taken to prevent the incident in the first place.
- C. Whether the incident has occurred before and what was the resulting damage.
- D. How to report an incident and to whom.

Answer: D

NEW QUESTION # 41

You are the owner of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks. What is this risk strategy called?

- A. Risk passing
- B. Risk avoiding
- C. Risk bearing
- D. Risk neutral

Answer: D

NEW QUESTION # 42

Companies use 27002 for compliance for which of the following reasons:

- A. A structured program that helps with security and compliance
- B. Compliance with ISO 27002 is sufficient to comply with all regulations
- C. Explicit requirements for all regulations

Answer: A

NEW QUESTION # 43

Susan sends an email to Paul. Who determines the meaning and the value of information in this email?

- A. Paul and Susan, the sender and the recipient of the information.
- B. Susan, the sender of the information.
- C. Paul, the recipient of the information.

Answer: C

NEW QUESTION # 44

A PECB ISO-IEC-27001-Lead-Implementer PECB Certified ISO/IEC 27001 Lead Implementer exam practice questions is a helpful, proven strategy to crack the PECB ISO-IEC-27001-Lead-Implementer

Lead IPass PECB ISO-IEC-27001-Lead-Implementer PDF Dumps Format

P.S. Free & New ISO-IEC-27001-Lead-Implementer dumps are available on Google Drive shared by PracticeMaterial: https://drive.google.com/open?id=16h3pZUcPgM4_g-LBV9A7vn_phNwepNz4

In spite of the high-quality of our ISO-IEC-27001-Lead-Implementer study braindumps, our after-sales service can be the most attractive project in our ISO-IEC-27001-Lead-Implementer guide questions. We have free online service which means that if you have any trouble using our ISO-IEC-27001-Lead-Implementer learning materials or operate different versions on the platform mistakenly, we can provide help for you remotely in the shortest time. And we know more on the ISO-IEC-27001-Lead-Implementer Exam Dumps, so we can give better suggestions according to your situlation.

PECB ISO-IEC-27001-Lead-Implementer Certification Exam is a highly recognized and sought-after certification for professionals in the IT and information security industry. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification is designed to provide the necessary knowledge and skills required to plan, implement, and maintain an information security management system (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification exam is conducted by PECB, a leading provider of training, examination, and certification services in the field of information security.

The ISO/IEC 27001 standard is a globally recognized standard for information security management. It provides a framework for organizations to manage and protect their sensitive information and assets from various threats, such as cyber-attacks, data breaches, and other security incidents. The ISO/IEC 27001 standard specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS.

ISO-IEC-27001-Lead-Implementer Authorized Certification & ISO-IEC-27001-Lead-Implementer Training Courses

We are living in a good society; everything is changing so fast with the development of technology. So an ambitious person must be able to realize his dreams if he is willing to make efforts. Winners always know the harder they work the luckier they are. If you purchase our study materials to prepare the ISO-IEC-27001-Lead-Implementer exam, your passing rate will be much higher than others. Also, the operation of our study material is smooth and flexible and the system is stable and powerful. You can install the ISO-IEC-27001-Lead-Implementer Exam Guide on your computers, mobile phone and other electronic devices. There are no restrictions to the number equipment you install. In short, it depends on your own choice. We sincerely hope that you can enjoy the good service of our products.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q218-Q223):

NEW QUESTION # 218

Del&Co has decided to improve their staff-related controls to prevent incidents. Which of the following is NOT a preventive control related to the Del&Co's staff?

- A. Video cameras
- B. Control of physical access to the equipment
- C. Authentication and authorization

Answer: A

Explanation:

According to ISO/IEC 27001:2022, Annex A.7, the objective of human resource security is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, and to reduce the risk of human error, theft, fraud, or misuse of facilities. The standard specifies eight controls in this domain, which are:

A).7.1 Prior to employment: This control covers the screening, terms and conditions, and roles and responsibilities of employees and contractors before they are hired.

A).7.2 During employment: This control covers the awareness, education, and training, disciplinary process, and management responsibilities of employees and contractors during their employment.

A).7.3 Termination and change of employment: This control covers the return of assets, removal of access rights, and exit interviews of employees and contractors when they leave or change their roles.

The other controls in Annex A are related to other aspects of information security, such as organizational, physical, and technological controls. For example:

A).9.2 User access management: This control covers the authentication and authorization of users to access information systems and services, based on their roles and responsibilities.

A).11.1 Secure areas: This control covers the control of physical access to the equipment and information assets, such as locks, alarms, guards, etc.

A).13.2 Information transfer: This control covers the protection of information during its transfer, such as encryption, digital signatures, secure protocols, etc.

Therefore, video cameras are not a preventive control related to the staff, but rather a physical control related to the equipment and assets. Video cameras can be used to monitor and record the activities of the staff, but they cannot prevent them from causing incidents. They can only help to detect and investigate incidents after they occur.

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Annex A; PECB ISO/IEC 27001 Lead Implementer Course, Module 8: Implementation of Information Security Controls.

NEW QUESTION # 219

Org Y, a well-known bank, 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. Org Y has implemented an integrity control that avoids the involuntary corruption of data
- B. Org Y has incorrectly implemented a security control that could become a vulnerability

- C. Org Y has implemented a security control that ensures the confidentiality of information

Answer: C

NEW QUESTION # 220

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives. Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action.

Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in.

Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

What type of controls did Beauty implement to ensure the safety of products and unique formulas stored in the warehouse?

- A. Administrative
- B. Technical
- C. Legal

Answer: B

NEW QUESTION # 221

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [

BTW, DOWNLOAD part of PracticeMaterial ISO-IEC-27001-Lead-Implementer dumps from Cloud Storage:

https://drive.google.com/open?id=16h3pZUcPgM4_g-LBV9A7vn_phNwepNz4