

# ISO-IEC-27001-Lead-Implementer Books PDF - ISO-IEC-27001-Lead-Implementer Valid Exam Practice



PECB ISO-IEC-27001-Lead-Implementer exam include many steps where a customer can ask any assistance from the team, Most of the PECB ISO-IEC-27001-Lead-Implementer test students work hard to get the credibility and integrity among their fellows and boss, But if they use our ISO-IEC-27001-Lead-Implementer test prep, they won't need so much time to prepare the exam and master exam content in a short time, We never concoct any praise but show our capacity by the efficiency and profession of our ISO-IEC-27001-Lead-Implementer practice materials.

Helen Bradley tells you all you need to know about filters, including <https://www.dumpsfree.com/ISO-IEC-27001-Lead-Implementer-valid-exam.html> how to apply multiple filters at once, how to find hidden options, and how to change the colors that a filter applies to your images.

## Download ISO-IEC-27001-Lead-Implementer Exam Dumps

A deep comparison involves comparing data members for each object. The next few sections discuss how these costs are used, The service of ISO-IEC-27001-Lead-Implementer test guide is very prominent.

Levels of Management, PECB ISO-IEC-27001-Lead-Implementer exam include many steps where a customer can ask any assistance from the team, Most of the PECB ISO-IEC-27001-Lead-Implementer test students work hard to get the credibility and integrity among their fellows and boss.

But if they use our ISO-IEC-27001-Lead-Implementer test prep, they won't need so much time to prepare the exam and master exam content in a short time, We never concoct any praise but show

Exam ISO-IEC-27001-Lead-Implementer Question Test Certification ISO-IEC-27001-Lead-Implementer Cost & Vce ISO-IEC-27001-Lead-Implementer Test Simulator

BTW, DOWNLOAD part of PrepAwayPDF ISO-IEC-27001-Lead-Implementer dumps from Cloud Storage:  
[https://drive.google.com/open?id=1pgOo1NnfB7qAeSenex0j\\_CuBCvXQLJuK](https://drive.google.com/open?id=1pgOo1NnfB7qAeSenex0j_CuBCvXQLJuK)

We know the certificate of ISO-IEC-27001-Lead-Implementer exam guide is useful and your prospective employer wants to see that you can do the job with strong prove, so our ISO-IEC-27001-Lead-Implementer study materials could be your opportunity. Our ISO-IEC-27001-Lead-Implementer practice dumps are sensational from the time they are published for the importance of ISO-IEC-27001-Lead-Implementer Exam as well as the efficiency of our ISO-IEC-27001-Lead-Implementer training engine. And we can help you get success and satisfy your eager for the certificate.

## The best resource for getting prepared for the PECB ISO IEC 27001 Lead Implementer Exam:

All the resources mentioned above are important for the PECB ISO IEC 27001 Lead Implementer certification exam. However, a great resource is practice exams of the PrepAwayPDF software will direct you throughout your preparation process. You will get to know about your weak points and areas of the ISO IEC 27001 Lead Implementer Certification Exam. **ISO IEC 27001 Lead Implementer exam dumps** will help you to understand the concepts better and get prepared yourself effectively for the exam. It is also advisable to refer to study guides for the PECB ISO IEC 27001 Lead Implementer examination. You can avail the offer of a free trial of the training simulator, you can do this analysis in a day. If you have purchased the premium account, you can do learning in-depth.

PECB ISO-IEC-27001-Lead-Implementer Certification Exam is intended for professionals who are responsible for managing and implementing an ISMS in an organization. This includes IT professionals, security managers, risk management professionals, and other individuals who are involved in the implementation and management of an ISMS. ISO-IEC-27001-Lead-Implementer exam is also suitable for individuals who are seeking to enhance their knowledge and understanding of the ISO/IEC 27001 standard.

>> ISO-IEC-27001-Lead-Implementer Books PDF <<

## ISO-IEC-27001-Lead-Implementer Valid Exam Practice & Latest ISO-IEC-27001-Lead-Implementer Study Notes

PrepAwayPDF's products can not only help you successfully pass PECB certification ISO-IEC-27001-Lead-Implementer Exams, but also provide you a year of free online update service, which will deliver the latest product to customers at the first time to let them have a full preparation for the exam. If you fail the exam, we will give you a full refund.

**Hit the link below, to get more info about the exam:**

Details about the ISO IEC 27001 Lead Implementer Certification Exam

## PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q131-Q136):

### NEW QUESTION # 131

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 decided to 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. Based on scenario 6, when should Colin deliver the next training and awareness session?

- A. After he determines the employees' availability and motivation
- **B. After he conducts a competence needs analysis and records the competence related issues**
- C. After he ensures that the group of employees targeted have satisfied the organization's needs

**Answer: B**

Explanation:

According to ISO/IEC 27001:2022, clause 7.2.3, the organization shall conduct a competence needs analysis to determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization shall also evaluate the effectiveness of the actions taken to acquire the necessary competence and retain appropriate documented information as evidence of competence.

Therefore, Colin should deliver the next training and awareness session after he conducts a competence needs analysis and records the competence related issues, such as the level of understanding, the gaps in knowledge, and the feedback from the participants. ISO/IEC 27001:2022, clause 7.2.3; PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 8.

### NEW QUESTION # 132

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?

- A. The type of data that helps prevent future occurrences of information security incidents
- B. The use of the buffer zone that blocks potential attacks coming from malicious websites where data can be collected
- **C. The collection and preservation of records**

**Answer: C**

Explanation:

According to the ISO/IEC 27001 : 2022 standard, information security incident management is the process of ensuring a consistent and effective approach to the management of information security incidents, events and weaknesses. One of the objectives of this process is to collect and preserve evidence that can be used for disciplinary and legal action, as well as for learning and improvement. Therefore, Anna should be aware of the collection and preservation of records when gathering data for the forensics team. She should follow the information security incident management policy of InfoSec, which specifies the type, format, content and location of the records to be created and maintained. She should also ensure that the records are protected from unauthorized access, modification, deletion or disclosure, and that they are retained for an appropriate period of time.

ISO/IEC 27001 : 2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Clause 16.1.7, Collection of evidence ISO/IEC 27001 : 2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Annex A.16.1.7, Collection of evidence ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Chapter 9, Information security incident management

### NEW QUESTION # 133

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, what would help Socket Inc. address similar information security incidents in the future?

- A. Using the access control system to ensure that only authorized personnel is granted access
- B. Using the MongoDB database with the default settings
- **C. Using cryptographic keys to protect the database from unauthorized access**

**Answer: C**

### NEW QUESTION # 134

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed for threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings, Texas H&H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Which situation described in scenario 7 Indicates that Texas H&H Inc. implemented a detective control?

- A. Texas H&H Inc. integrated the incident management policy in Its information security policy
- **B. Texas H&H Inc. hired an expert to conduct a forensic analysis**
- C. Texas H&H Inc. tested its system for malicious activity and checked cloud based email settings

**Answer: B**

#### NEW QUESTION # 135

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.

Based on scenario 2, what type of controls did Beauty use during incident investigation?

- A. Corrective controls
- **B. Detective controls**
- C. Preventive controls

**Answer: B**

#### NEW QUESTION # 136

.....

**ISO-IEC-27001-Lead-Implementer Valid Exam Practice:** <https://www.prepawaypdf.com/PECB/ISO-IEC-27001-Lead-Implementer-practice-exam-dumps.html>

- Valid ISO-IEC-27001-Lead-Implementer Cram Materials ☐ ISO-IEC-27001-Lead-Implementer Accurate Answers ☐ ISO-IEC-27001-Lead-Implementer Vce Test Simulator ☐ Search for ➡ ISO-IEC-27001-Lead-Implementer ☐ and download it for free immediately on ➡ [www.prepawayete.com](http://www.prepawayete.com) ☐ ☐ ISO-IEC-27001-Lead-Implementer Valid Test Sims
- Pass Guaranteed Quiz 2026 ISO-IEC-27001-Lead-Implementer - PECB Certified ISO/IEC 27001 Lead Implementer Exam Books PDF ☐ Go to website ▶ [www.pdfvce.com](http://www.pdfvce.com) ◀ open and search for [ ISO-IEC-27001-Lead-Implementer ] to

