# Premium ISO-IEC-27001-Lead-Implementer Files | Latest ISO-IEC-27001-Lead-Implementer Study Materials


What's more, part of that ValidDumps ISO-IEC-27001-Lead-Implementer dumps now are free: https://drive.google.com/open?id=1JUFPJvG8AQMeUQWCZB_p-pkBZqMQCZQA

ISO-IEC-27001-Lead-Implementer preparation materials will be the good helper for your qualification certification. We are concentrating on providing high-quality authorized ISO-IEC-27001-Lead-Implementer study guide all over the world so that you can clear exam one time. ISO-IEC-27001-Lead-Implementer reliable exam bootcamp materials contain three formats: PDF version, Soft test engine and APP test engine so that our products are enough to satisfy different candidates' habits and cover nearly full questions & answers of the real ISO-IEC-27001-Lead-Implementer test.

The ISO/IEC 27001 standard is a globally recognized framework for information security management. It provides a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. The Lead Implementer certification exam focuses on the practical implementation of the standard, providing professionals with the knowledge and skills needed to implement and manage an ISMS in accordance with ISO/IEC 27001.

**>> Premium ISO-IEC-27001-Lead-Implementer Files <<**

## Pass Guaranteed PECB - ISO-IEC-27001-Lead-Implementer - High-quality Premium PECB Certified ISO/IEC 27001 Lead Implementer Exam Files

Due to the shortage of useful practice materials or being scanty for them, many candidates may choose the bad quality exam materials, but more and more candidates can choose our ISO-IEC-27001-Lead-Implementer study materials. Actually, some practice materials are shooting the breeze about their effectiveness, but our ISO-IEC-27001-Lead-Implementer training quiz are real high quality practice materials with passing rate up to 98 to 100 percent. And you will be amazed to find that our ISO-IEC-27001-Lead-Implementer exam questions are exactly the same ones in the real exam.

The ISO/IEC 27001 standard provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system. The standard covers a wide range of topics, including risk assessment,

security controls, and information security policies. The PECB ISO-IEC-27001-Lead-Implementer Exam covers all of these topics and more, ensuring that certified professionals have a comprehensive understanding of the standard and how to apply it in their organizations.

## PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q241-Q246):

**NEW QUESTION # 241**
In the context ofcontact with special interest groups, any information-sharing agreements should identify requirements for the protection of _____ information.

- A. Authentic
- B. Authorization
- C. Confidential
- D. Availability

**Answer: C**

**NEW QUESTION # 242**
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. which information security control of Annex A of ISO/IEC 27001 did Socket Inc. implement by establishing a new system to maintain, collect, and analyze information related to information security threats?

- A. Annex A 5 7 Threat Intelligence
- B. Annex A 5.13 Labeling of information
- C. Annex A 5.5 Contact with authorities

**Answer: A**

Explanation:
Annex A 5.7 Threat Intelligence is a new control in ISO 27001:2022 that aims to provide the organisation with relevant information regarding the threats and vulnerabilities of its information systems and the potential impacts of information security incidents. By establishing a new system to maintain, collect, and analyze information related to information security threats, Socket Inc. implemented this control and improved its ability to prevent, detect, and respond to information security incidents.
Reference:
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A 5.7 Threat Intelligence ISO/IEC 27002:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection controls, Clause 5.7 Threat Intelligence PECB ISO/IEC 27001:2022 Lead Implementer Course, Module 6: Implementation of Information Security Controls Based on ISO/IEC 27002:2022, Slide 18: A.5.7 Threat Intelligence

**NEW QUESTION # 243**
Upon the risk assessment outcomes. Socket Inc. decided to:
* Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

* Require the change of passwords at least once every 60 days
* Keep backup copies of files on IT-provided network drives
* Assign users to a separate network when they have access to cloud storage files storing customers' personal data.
What is the most important asset to Socket Inc. associated with the use of cloud storage? Refer to scenario 5.

- A. Employees with access to cloud storage files
- B. IT provided network drives
- C. Customers' personal data

**Answer: C**

**NEW QUESTION # 244**
Scenario 7: CyTekShield
CyTekShield based in Dublin. Ireland, is a cybersecurity consulting provider specializing in digital risk management and enterprise security solutions. After facing multiple security incidents. CyberTekShield formed expanded its information security team by bringing in Sadie and Niamh as part of the team. This team is structured into three key divisions: incident response, security architecture and forensics Sadie will separate the demilitarized zone from CyTekShield's private network and publicly accessible resources, as part of implementing a screened subnet network architecture. In addition, Sadie will carry out comprehensive evaluations of any unexpected incidents, analyzing their causes and assessing their potential impact. She also developed security strategies and policies. Whereas Niamh. a specialized expert in forensic investigations, will be responsible for creating records of different data for evidence purposes To do this effectively, she first reviewed the company's information security incident management policy, which outlines the types of records to be created, their storage location, and the required format and content for specific record types.
To support the process of handling of evidence related to information security events. CyTekShield has established internal procedures. These procedures ensure that evidence is properly identified, collected, and preserved within the company CyTekShield's procedures specify how to handle records in various storage mediums, ensuring that all evidence is safeguarded in its original state, whether the devices are powered on or off.
As part of CyTekShield's initiative to strengthen information security measures, Niamh will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments Upon completion of the risk assessment process, Niamh is responsible to develop and implement a plan for treating information security risks and document the risk treatment results.
Furthermore, while implementing the communication plan for information security, the CyTekShield's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.
Has CyTekShield appropriately addressed the handling of evidence related to information security events?

- A. Yes - it has appropriately addressed the handling of evidence
- B. No - as it does not include proper training for staff involved in evidence handling
- C. No - because the process of evidence acquisition was not fully detailed

**Answer: A**

**NEW QUESTION # 245**
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