2022 Updated PECB ISO-IEC-27001-Lead-Implementer Certification Study Guide Pass ISO-IEC-27001-Lead-Implementer Fast [Q24-Q46

2022 Updated PECB ISO-IEC-27001-Lead-Implementer Certification Study Guide Pass ISO-IEC-27001-Lead-Implementer Fast ISO-IEC-27001-Lead-Implementer Dumps PDF 2022 Program Your Preparation EXAM SUCCESS

PECB ISO-IEC-27001-Lead-Implementer Exam Syllabus Topics:

TopicDetailsTopic 1- Support an organization in operating, maintaining, and continually improving an ISMS based on ISO- IEC 27001- Implementing an ISMS based on ISO- IEC 27001Topic 2- Prepare an organization to undergo a third-party certification audit- Fundamental principles and concepts of an information security management system (ISMS)Topic 3- Initiate and plan the implementation of an ISMS based on ISO- IEC 27001- Planning an ISMS implementation based on ISO - IEC 27001Topic 4- Interpret the ISO- IEC 27001 requirements for an ISMS from the perspective of an implementer- Information security management system (ISMS)

Topics covered by the PECB ISO IEC 27001 Lead Implementer Certification Exam: **ISO IEC 27001 Lead Implementer exam dumps** cover the following topics of the ISO IEC 27001 Lead Implementer Certification Exam:

- Monitoring and measurement of an ISMS based on ISO/IEC 27001: 20%- Planning an ISMS implementation based on ISO/IEC 27001: 10%- Continual improvement of an ISMS based on ISO/IEC 27001: 10% **QUESTION 24**

What sort of security does a Public Key Infrastructure (PKI) offer?

* It provides digital certificates that can be used to digitally signdocuments. Such signatures irrefutably determine from whom a

document was sent.
* Having a PKI shows customers that a web-based business is secure.
* By providing agreements, procedures and an organization structure, a PKI defines which person or which system belongs to which specific public key.
* A PKI ensures that backups of company data are made on a regular basis.

QUESTION 25

The company Midwest Insurance has taken many measures to protect its information. It uses an Information Security Management System, the input and output of data in applications is validated, confidential documents are sent in encrypted form and staff use tokens to access information systems. Which of these is not a technical measure?
* Information Security Management System
* The use of tokens to gain access to information systems
* Validation of input and output data in applications
* Encryption ofinformation

QUESTION 26

You apply for a position in another company and get the job. Along with your contract, you are asked to sign a code of conduct. What is a code of conduct?
* A code ofconduct specifies how employees are expected to conduct themselves and is the same for all companies.
* A code of conduct is a standard part of a labor contract.
* A code of conduct differs from company to company and specifies, among other things, the rules of behavior with regard to the usage of information systems.

QUESTION 27

Which of the following measures is a correctivemeasure?
* Incorporating an Intrusion Detection System (IDS) in the design of a computer center
* Installing a virus scanner in an information system
* Making a backup of the data that has been created or altered that day
* Restoring a backup of the correct database after a corrupt copy of the database was written over the original

QUESTION 28

Responsibilities for information security in projects should be defined and allocated to:
* the project manager
* specified roles defined in the used project management method of the organization
* the InfoSec officer
* the owner of the involved asset

QUESTION 29

You have juststarted working at a large organization. You have been asked to sign a code of conduct as well as a contract. What does the organization wish to achieve with this?
* A code of conduct helps to prevent the misuse of IT facilities.
* A code of conduct is alegal obligation that organizations have to meet.
* A code of conduct prevents a virus outbreak.
* A code of conduct gives staff guidance on how to report suspected misuses of IT facilities.

QUESTION 30

A company moves into a new building. A few weeks after the move, a visitor appears unannounced in the office of the director. An investigation shows that visitors passes grant the same access as the passes of the company’s staff. Which kind of security measure could have prevented this?
* physical security measure
* An organizational security measure
* A technical security measure

QUESTION 31

What is an example of a good physical security measure?
* All employees and visitors carry an access pass.
* Printers that are defective or have been replacedare immediately removed and given away as garbage for recycling.
* Maintenance staff can be given quick and unimpeded access to the server area in the event of disaster.

QUESTION 32

What do employees need to know to report a security incident?
* How to report an incident and to whom.
* Whether the incident has occurred before and what was the resulting damage.
* The measures that should have been taken to prevent the incident in the first place.
* Who is responsible for the incident and whether it was intentional.

QUESTION 33

We can acquire and supply information in various ways. The value of the information depends on whether it is reliable. What are the reliability aspects of information?
* Availability, Information Value and Confidentiality
* Availability, Integrity and Confidentiality
* Availability, Integrity and Completeness
* Timeliness, Accuracy and Completeness

QUESTION 34

Susan sends an email to Paul. Who determines the meaning and the value of information in this email?
* Paul, therecipient of the information.
* Paul and Susan, the sender and the recipient of the information.
* Susan, the sender of the information.

QUESTION 35

One of the ways Internet of Things (IoT) devices can communicate with each other (or ‘the outside world’) is using a so-called short-range radio protocol. Which kind of short-range radio protocol makes it possible to use your phone as a credit card?
* Near Field Communication (NFC)
* Bluetooth
* Radio Frequency Identification (RFID)
* The 4G protocol

QUESTION 36

Physical labels and _____ are two common forms of labeling which are mentioned in ISO 27002.
* metadata
* teradata
* bridge

QUESTION 37

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?
* Risk bearing
* Risk avoiding
* Risk neutral
* Risk passing

QUESTION 38

Logging in to a computer system is an access-granting process consisting of three steps: identification, authentication and authorization. What occurs during the first step of this process: identification?
* Thefirst step consists of checking if the user is using the correct certificate.
* The first step consists of checking if the user appears on the list of authorized users.
* The first step consists of comparing the password with the registered password.
* The first step consists of granting access to the information to which the user is authorized.

QUESTION 39

What should be used to protect data on removable media ifdata confidentiality or integrity are important considerations?
* backup on another removable medium
* cryptographic techniques
* a password
* logging

QUESTION 40

What are the data protection principles set out in the GDPR?
* Purpose limitation, proportionality, availability, data minimisation
* Purpose limitation, proportionality, data minimisation, transparency
* Target group, proportionality, transparency, data minimisation
* Purpose limitation, pudicity, transparency, data minimisation

QUESTION 41

Which of the following measures is a preventive measure?
* Installing a logging system that enables changes in a system to be recognized
* Shutting down all internet traffic after a hacker has gained access to thecompany systems
* Putting sensitive information in a safe
* Classifying a risk as acceptable because the cost of addressing the threat is higher than the value of the information at risk

QUESTION 42

What is an example of a security incident?
* The lighting in the department no longer works.
* A member of staff loses a laptop.
* You cannot set the correct fonts in your word processing software.
* A file is saved under an incorrect name.

QUESTION 43

A non-human threat for computer systems is a flood. In which situation is a flood always a relevant threat?
* If the riskanalysis has not been carried out.
* When computer systems are kept in a cellar below ground level.
* When the computer systems are not insured.
* When the organization is located near a river.

Who can take the PECB ISO IEC 27001 Lead Implementer Certification Exam?

The targeted audience for this certification are individuals who plan and implement information security management systems and who lead and manage the implementation team. Moreover, ISO/IEC 27001 is one of the most used standards in information security, so people in the security field are the main target audience for this certification. **ISO IEC 27001 Lead Implementer exam dumps** recommend that individuals having designations like CISSP, CISM, CISSP, CISM, ISO/IEC 27001 Lead Implementer, or CISA with any level of experience can also apply.

Get Perfect Results with Premium ISO-IEC-27001-Lead-Implementer Dumps Updated 50 Questions:
https://www.examcollectionpass.com/PECB/ISO-IEC-27001-Lead-Implementer-practice-exam-dumps.html]