[2025 New ISO-IEC-27001-Lead-Implementer exam Free Sample Questions to Practice [Q62-Q79

[2025 New ISO-IEC-27001-Lead-Implementer exam Free Sample Questions to Practice Cover Real ISO-IEC-27001-Lead-Implementer Exam Questions Make Sure You 100% Pass

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

TopicDetailsTopic 1- Implementation of an ISMS based on ISO- IEC 27001: The topic focuses on establishing policies, procedures, and controls, managing resources. The sections also delves into conducting training programs for staff awareness, and ensuring proper documentation to meet compliance requirements.Topic 2- Planning of an ISMS implementation based on ISO- IEC 27001: It involves conducting a gap analysis, setting ISMS objectives, identifying risks and opportunities, and developing a Statement of Applicability (SoA) to guide implementation efforts effectively.Topic 3- Fundamental principles and concepts of an information security management system: This topic covers information security basics, emphasizing confidentiality, integrity, and availability (CIA), along with the importance of risk management in establishing a robust Information Security Management System (ISMS).

NO.62 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&#8217;s information security team, which consists of a security architecture team, an incident response team (IRT) and a forensics team Emma&#8217;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 (OMZ) to which hosted public services are attached and InfoSec&#8217;s publicly accessible resources from their private network Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company&#8217;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&#8217;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 this scenario, answer the following question:

Based on his tasks, which team is Bob part of?
* Forensics team
* Security architecture team
* Incident response team

NO.63 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 decidedto implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company&#8217;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&#8217;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&#8217;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 What is the difference between training and awareness? Refer to scenario 6.
* Training helps acquire certain skills, whereas awareness develops certain habits and behaviors.
* Training helps acquire a skill, whereas awareness helps apply it in practice
* Training helps transfer a message with the intent of informing, whereas awareness helps change the behavior toward the message
According to ISO/IEC 27001, training and awareness are two different but complementary activities that aim to enhance the information security competence and performance of the organization&#8217;s personnel. Training is the process of providing instruction and guidance to help individuals acquire certain skills, knowledge, or abilities related to information security. Awareness is the process of raising the level of consciousness and understanding of the importance and benefits of information security, and developing certain habits and behaviors that support the information security objectives and requirements.

In scenario 6, Colin is holding a training and awareness session for the personnel of Skyver, which means he is combining both activities to achieve a more effective and comprehensive information security education. The training part of the session covers topics such as Skyver&#8217;s information security policies and procedures, and techniques for mitigating phishing and malware. The awareness part of the session covers topics such as Skyver&#8217;s information security approaches and challenges, and the benefits of information security for the organization and its customers. The purpose of the session is to help the personnel acquire the necessary skills to perform their information security roles and responsibilities, and to develop the appropriate habits and behaviors to protect the information assets of the organization.

References:

* ISO/IEC 27001:2013, clause 7.2.2: Information security awareness, education and training

* ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001

* ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001

* ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC 27001

* ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit

* ISO 27001 Security Awareness Training and Compliance &#8211; InfosecTrain1

* ISO/IEC 27001 compliance and cybersecurity awareness training2

* ISO 27001 Free Training | Online Course | British Assessment Bureau

NO.64 Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization&#8217;s premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization&#8217;s topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Based on scenario 3, did Socket Inc. comply with ISO/IEC 27001 organizational controls regarding its operating procedures?
* Yes, it did comply with ISO/IEC 27001 requirements
* No, operating procedures for information processing facilities should have been specifically provided to personnel who require them
* No, operating procedures for information processing facilities should have been exclusively available to the Information Technology Department or a similar unit within the company

NO.65 What action should UX Software take to mitigate residual risks? Refer to scenario 4.
* UX Software should immediately implement new controls to treat all residual risks
* UX Software should evaluate, calculate, and document the value of risk reduction following risk treatment
* UX Software should accept the residual risks only above the acceptance level

NO.66 An organization that has an ISMS in place conducts management reviews at planned intervals, but does not retain documented information on the results. Is this in accordance with the requirements of ISO/IEC 27001?
* Yes. ISO/IEC 27001 does not require organizations to document the results of management reviews
* No, ISO/IEC 27001 requires organizations to document the results of management reviews
* Yes. ISO/IEC 27001 requires organizations to document the results of management reviews only if they are conducted ad hoc

NO.67 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&#8217; data and medical history, and communicate with all the

[involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic&#8217;s patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients&#8217; privacy.

In scenario 1, HealthGenic experienced a number of service interruptions due to the loss of functionality of the software. Which principle of information security has been affected in this case?
* Availability
* Confidentiality
* Integrity
Explanation

Availability of information is the property of being accessible and usable upon demand by an authorized entity. In other words, availability ensures that the information and the systems that support it are always ready for use when needed. In the scenario, the availability of information was affected when HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software.

This means that the software was not able to handle the demand and provide the required functionality to the users. Therefore, the correct answer is A.

References: ISO/IEC 27001:2013, Information technology &#8211; Security techniques &#8211; Information security management systems &#8211; Requirements, clause 3.13.

NO.68 Based on scenario 4, what type of assets were identified during risk assessment?
* Supporting assets
* Primary assets
* Business assets

NO.69 Based on scenario 2. which principle of information security was NOT compromised by the attack?
* Confidentiality
* integrity
* Availability

NO.70 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?
* Annex A 5.5 Contact with authorities
* Annex A 5 7 Threat Intelligence
* Annex A 5.13 Labeling of information

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 &#8211; Security techniques &#8211; Information security management systems

&#8211; Requirements, Annex A 5.7 Threat Intelligence ISO/IEC 27002:2022 Information technology &#8211; Security techniques &#8211; 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

NO.71 Why should the security testing processes be defined and implemented in the development life cycle?
* To protect the production environment and data from compromise by development and test activities
* To validate if information security requirements are met when applications are deployed to the production environment
* To Identify organizational assets and define appropriate protection responsibilities

NO.72 Which security controls must be implemented to comply with ISO/IEC 27001?
* Those designed by the organization only
* Those included in the risk treatment plan
* Those listed in Annex A of ISO/IEC 27001, without any exception

NO.73 Kyte. a company that has an online shopping website, has added a Q&A section to its website; however, its Customer Service Department almost never provides answers to users&#8217; questions. Which principle of an effective communication strategy has Kyte not followed?
* Clarity
* Appropriateness
* Responsiveness
Explanation

A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, such as the internet. A DMZ is designed to provide a layer of protection for the internal network by limiting the exposure of publicly accessible resources and services to potential attackers. A DMZ is an example of a preventive control, which is a type of security control that aims to prevent or deter cyberattacks from occurring in the first place. Preventive controls reduce the likelihood of a successful attack by implementing safeguards and countermeasures that make it more difficult or costly for an attacker to exploit vulnerabilities or bypass security mechanisms. Other examples of preventive controls include encryption, authentication, access control, firewalls, antivirus software, and security awareness training. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 83)
References:

PECB ISO/IEC 27001 Lead Implementer Course Manual, page 83

PECB ISO/IEC 27001 Lead Implementer Info Kit, page 7

NO.74 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&#8217; information.

Beauty&#8217;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&#8217; 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 the scenario above, answer the following question:

After investigating the incident. Beauty decided to install a new anti-malware software. What type of security control has been implemented in this case?
* Preventive
* Detective
* Corrective
Explanation

A corrective security control is a type of control that is implemented to restore the normal operations of a system or network after a security incident or breach has occurred. Corrective controls aim to mitigate the impact of the incident, prevent further damage, and restore the confidentiality, integrity, and availability of the information and assets affected by the incident. Examples of corrective controls include backup and recovery, disaster recovery plans, incident response teams, and anti-malware software.

In this case, Beauty decided to install a new anti-malware software after investigating the incident that exposed customers&#8217; information due to the out-of-date anti-malware software. The new anti-malware software is a corrective control because it is intended to remove the malicious code that compromised the system and prevent similar incidents from happening again. The new anti-malware software also helps to restore the trust and confidence of the customers and the reputation of the company.

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 &#8211; Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Security Controls? | IBM3 What Are Security Controls? &#8211; F54

NO.75 An organization has decided to conduct information security awareness and training sessions on a monthly basis for all employees. Only 45% of employees who attended these sessions were able to pass the exam.

What does the percentage represent?
* Measurement objective
* Attribute
* Performance indicator
According to the ISO/IEC 27001:2022 standard, a performance indicator is &#8220;a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization&#8221; (section 3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.

References:

* ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection &#8211; Information security management systems &#8211; Requirements1

* ISO/IEC 27001 Lead Implementer Info Kit

* Key performance indicators for an ISO 27001 ISMS2

NO.76 An organization has decided to conduct information security awareness and training sessions on a monthly basis for all employees. Only 45% of employees who attended these sessions were able to pass the exam.

What does the percentage represent?
* Measurement objective
* Attribute
* Performance indicator
Explanation

According to the ISO/IEC 27001:2022 standard, a performance indicator is &#8220;a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization&#8221; (section 3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.

References:

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection &#8211; Information security management systems &#8211; Requirements1 ISO/IEC 27001 Lead Implementer Info Kit Key performance indicators for an ISO 27001 ISMS2

NO.77 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

NO.78 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&#8217; data and medical history, and communicate with all the

[involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic&#8217;s patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients&#8217; privacy.

Which situation described in scenario 1 represents a threat to HealthGenic?
* HealthGenic did not train its personnel to use the software
* The software company modified information related to HealthGenic&#8217;s patients
* HealthGenic used a web-based medical software for storing patients&#8217; confidential information
According to ISO/IEC 27001:2022, a threat is any incident that could negatively affect the confidentiality, integrity or availability of an asset1. In this scenario, the asset is the information related to HealthGenic&#8217;s patients, which is stored and processed by the web-based medical software. The software company&#8217;s modification of some files that comprised sensitive information related to HealthGenic&#8217;s patients is an incident that could negatively affect the confidentiality and integrity of the asset, as it resulted in incomplete and incorrect medical reports and invaded the patients&#8217; privacy. Therefore, this situation represents a threat to HealthGenic.

References:

* ISO/IEC 27001:2022 &#8211; Information security, cybersecurity and privacy protection &#8211; Information security management systems &#8211; Requirements

* ISO 27001 Key Terms &#8211; PJR

NO.79 Peter works at the company Midwest Insurance. His manager, Linda, asks him to send the terms and conditions for a life insurance policy to Rachel, a client. Who determines the value of the information in the insurance terms and conditions document?
* The recipient, Rachel
* The person who drafted the insurance terms and conditions
* The manager, Linda
* The sender, Peter

PECB ISO-IEC-27001-Lead-Implementer exam is designed to test the knowledge and skills of individuals in the implementation of an ISMS based on the ISO/IEC 27001 standard. ISO-IEC-27001-Lead-Implementer exam covers various topics such as the planning, implementation, monitoring, and review of an ISMS. It also covers the risk management process, security controls, and the legal and regulatory requirements that organizations need to comply with.

Real ISO-IEC-27001-Lead-Implementer Quesions Pass Certification Exams Easily:
https://www.dumpsmaterials.com/ISO-IEC-27001-Lead-Implementer-real-torrent.html]