Vendor:PECB

Exam Code:LEAD-IMPLEMENTER

Exam Name:PECB Certified ISO/IEC 27001 Lead Implementer

Version: Demo

QUESTION 1

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 (OMZ) 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. InfoSec contracted Anna as an external consultant. Based on her tasks, is this action compliant with ISO/IEC 27001?

A. No, the skills of incident response or forensic analysis shall be developed internally

B. Yes, forensic investigation may be conducted internally or by using external consultants

C. Yes, organizations must use external consultants for forensic investigation, as required by the standard

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 8.2.3, the organization shall establish and maintain an incident response process that includes the following activities:

a) planning and preparing for incident response, including defining roles and responsibilities, establishing communication channels, and providing training and awareness;

b) detecting and reporting information security events and weaknesses; c) assessing and deciding on information security incidents; d) responding to information security incidents according to predefined procedures;

e) learning from information security incidents, including identifying root causes, taking corrective actions, and improving the incident response process; f) collecting evidence, where applicable.

The standard does not specify whether the incident response process should be performed internally or externally, as long as the organization ensures that the process is effective and meets the information security objectives. Therefore, the

organization may decide to use external consultants for forensic investigation, as long as they comply with the organization\\'s policies and procedures, and protect the confidentiality, integrity, and availability of the information involved.

References: ISO/IEC 27001:2022, clause 8.2.3; PECB ISO/IEC 27001 Lead Implementer Study Guide, section 8.2.3.

QUESTION 2

\\'The ISMS covers all departments within Company XYZ that have access to customers\\' data. The purpose of the ISMS is to ensure the confidentiality, integrity, and availability of customers\\' data, and ensure compliance with the applicable regulatory requirements regarding information security." What does this statement ^"describe?

A. The information systems boundary of the ISMS scope

B. The organizational boundaries of the ISMS scope

C. The physical boundary of the ISMS scope

Correct Answer: B

Explanation: The statement describes the organizational boundaries of the ISMS scope, which define which parts of the organization are included or excluded from the ISMS. The organizational boundaries can be based on criteria such as departments, functions, processes, activities, or locations. In this case, the statement specifies that the ISMS covers all departments within Company XYZ that have access to customers\\' data, and excludes the ones that do not. The statement also explains the purpose of the ISMS, which is to ensure the confidentiality, integrity, and availability of customers\\' data, and ensure compliance with the applicable regulatory requirements regarding information security. The statement does not describe the information systems boundary of the ISMS scope, which defines which information systems are included or excluded from the ISMS. The information systems boundary can be based on criteria such as hardware, software, networks, databases, or applications. The statement does not mention any specific information systems that are covered by the ISMS. The statement also does not describe the physical boundary of the ISMS scope, which defines which physical locations are included or excluded from the ISMS. The physical boundary can be based on criteria such as buildings, rooms, cabinets, or devices. The statement does not mention any specific physical locations that are covered by the ISMS. References: ISO/IEC 27001:2013, clause 4.3: Determining the scope of the information security management system ISO/IEC 27001 Lead Implementer Course, Module 4: Planning the ISMS based on ISO/IEC 27001 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/IEC 27001 scope statement | How to set the scope of your ISMS - Advisera1 How to Write an ISO 27001 Scope Statement (+3 Examples) - Compleye2 How To Use an Information Flow Map to Determine Scope of Your ISMS3 ISMS SCOPE DOCUMENT - Resolver4 Define the Scope and Objectives - ISMS Info5

QUESTION 3

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. Lisa found some of the issues being discussed in the training and awareness session too

technical, thus not fully understanding the session. What does this indicate?

A. Lisa did not take actions to acquire the necessary competence

B. The effectiveness of the training and awareness session was not evaluated

C. Skyver did not determine differing team needs in accordance to the activities they perform and the intended results

Correct Answer: C

Explanation: According to the ISO/IEC 27001:2022 Lead Implementer Training Course Guide1, one of the requirements of ISO/IEC 27001 is to ensure that all persons doing work under the organization\\'s control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. To achieve this, the organization should determine the necessary competence of persons doing work under its control that affects its information security performance, provide training or take other actions to acquire the necessary competence, evaluate the effectiveness of the actions taken, and retain appropriate documented information as evidence of competence. The organization should also determine differing team needs in accordance to the activities they perform and the intended results, and provide appropriate training and awareness programs to meet those needs. Therefore, the scenario indicates that Skyver did not determine differing team needs in accordance to the activities they perform and the intended results, since Lisa, who works in the HR Department, found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. This implies that the session was not tailored to the specific needs and roles of the HR personnel, and that the information security expert did not consider the level of technical knowledge and skills required for them to perform their work effectively and securely. References: ISO/IEC 27001:2022 Lead Implementer Training Course Guide1 ISO/IEC 27001:2022 Lead Implementer Info Kit2

QUESTION 4

Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management [^system implementation, TradeB\\'s top management contracted two experts to direct and manage the ISMS implementation project. First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity

Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted

Based on scenario 4, the fact that TradeB defined the level of risk based on three nonnumerical categories indicates that;

A. The level of risk will be evaluated against qualitative criteria

B. The level of risk will be defined using a formula

C. The level of risk will be evaluated using quantitative analysis

Correct Answer: A

Explanation: Qualitative risk assessment is a method of evaluating risks based on nonnumerical categories, such as low, medium, and high. It is often used when there is not enough data or resources to perform a quantitative risk assessment, which involves numerical values and calculations. Qualitative risk assessment relies on the subjective judgment and experience of the risk assessors, and it can be influenced by various factors, such as the context, the stakeholders, and the criteria. According to ISO/IEC 27001:2022, Annex A, control A.8.2.1 states: "The organization shall define and apply an information security risk assessment process that: ... d) identifies the risk owners; e) analyses the risks: i) assesses the consequences that would result if the risks identified were to materialize; ii) assesses the realistic likelihood of the occurrence of the risks; f) identifies and evaluates options for the treatment of risks; g) determines the levels of residual risk and whether these are acceptable; and h) identifies the risk owners for the residual risks." Therefore, TradeB\\'s decision to define the level of risk based on three nonnumerical categories indicates that they used a qualitative risk assessment process. References: ISO/IEC 27001:2022, Annex A, control A.8.2.1 PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slides 12-13

QUESTION 5

An organization has adopted a new authentication method to ensure secure access to sensitive areas and facilities of the company. It requires every employee to use a two-factor authentication (password and QR code). This control has been documented, standardized, and communicated to all employees, however its use has been "left to individual initiative, and it is likely that failures can be detected. Which level of maturity does this control refer to?

A. Optimized

B. Defined

C. Quantitatively managed

Correct Answer: B

Explanation: According to the ISO/IEC 27001:2022 Lead Implementer objectives and content, the maturity levels of information security controls are based on the ISO/IEC 15504 standard, which defines five levels of process capability:

incomplete, performed, managed, established, and optimized1. Each level has a set of attributes that describe the characteristics of the process at that level. The level of defined corresponds to the attribute of process performance, which

means that the process achieves its expected outcomes2. In this case, the control of two-factor authentication has been documented, standardized, and communicated, which implies that it has a clear purpose and expected outcomes.

However, the control is not consistently implemented, monitored, or measured, which means that it does not meet the attributes of the higher levels of managed, established, or optimized. Therefore, the control is at the level of defined, which

is the second level of maturity.

References:

1: ISO/IEC 27001:2022 Lead Implementer Course Brochure, page 5

2: ISO/IEC 27001:2022 Lead Implementer Course Presentation, slide 25

QUESTION 6

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\\' information. Beauty\\'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\\' 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?

A. Preventive

B. Detective

C. Corrective

Correct Answer: C

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\\' information due to the out-of-date anti-malware software. The new antimalware 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 - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Security Controls? | IBM3 What Are Security Controls? - F54

QUESTION 7

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 (OMZ) 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.

Why did InfoSec establish an IRT? Refer to scenario 7.

A. To comply with the ISO/IEC 27001 requirements related to incident management

B. To collect, preserve, and analyze the information security incidents

C. To assess, respond to, and learn from information security incidents

Correct Answer: C

Explanation: Based on his tasks, Bob is part of the incident response team (IRT) of InfoSec. According to the ISO/IEC 27001:2022 standard, an IRT is a group of individuals who are responsible for responding to information security incidents in a timely and effective manner. The IRT should have the authority, skills, and resources to perform the following activities: Identify and analyze information security incidents and their impact Contain, eradicate, and recover from information security incidents Communicate with relevant stakeholders and authorities Document and report on information security incidents and their outcomes Review and improve the information security incident management process and controls Bob\\'s job is to deploy a network architecture that can prevent potential attackers from accessing InfoSec\\'s private network, and to conduct a thorough evaluation of the nature and impact of any unexpected events that might occur. These tasks are aligned with the objectives and responsibilities of an IRT, as defined by the ISO/IEC 27001:2022 standard. References: ISO/IEC 27001:2022, Information technology -- Security techniques -- Information security management systems -- Requirements, Clause 10.2, Information security incident management ISO/IEC 27035-1:2023, Information technology -- Information security incident management -- Part 1: Principles of incident management ISO/IEC 27035-2:2023, Information technology -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response PECB, ISO/IEC 27001 Lead Implementer Course, Module 10, Information security incident management

---

QUESTION 8

The IT Department of a financial institution decided to implement preventive controls to avoid potential security breaches. Therefore, they separated the development, testing, and operating equipment, secured their offices, and used cryptographic keys. However, they are seeking further measures to enhance their security and minimize the risk of security breaches. Which of the following controls would help the IT Department achieve this objective?

A. Alarms to detect risks related to heat, smoke, fire, or water

B. Change all passwords of all systems

C. An access control software to restrict access to sensitive files

Correct Answer: C

Explanation: An access control software is a type of preventive control that is designed to limit the access to sensitive files and information based on the user\\'s identity, role, or authorization level. An access control software helps to protect the confidentiality, integrity, and availability of the information by preventing unauthorized users from viewing, modifying, or deleting it. An access control software also helps to create an audit trail that records who accessed what information and when, which can be useful for accountability and compliance purposes. The IT Department of a financial institution decided to implement preventive controls to avoid potential security breaches. Therefore, they separated the development, testing, and operating equipment, secured their offices, and used cryptographic keys. However, they are seeking further measures to enhance their security and minimize the risk of security breaches. An access control software would help the IT Department achieve this objective by adding another layer of protection to their sensitive files and information, and ensuring that only authorized personnel can access them. 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 - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Information Security Controls? - SecurityScorecard4 What Are the Types of Information Security Controls? - RiskOptics2 Integrity is the property of safeguarding the accuracy and completeness of information and processing methods. A breach of integrity occurs when information is modified or destroyed in an unauthorized or unintended manner. In this case, Diana accidently modified the order details of a customer without their permission, which resulted in the customer receiving an incorrect product. This means that the information about the customer\\'s order was not accurate or complete, and therefore, the integrity principle was breached. Availability and confidentiality are two other information security principles, but they were not violated in this case. Availability is the property of being accessible and usable upon demand by an authorized entity, and confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. References: ISO/IEC 27001:2022 Lead Implementer Course Content, Module 5: Introduction to Information Security Controls based on ISO/IEC 27001:20221; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 3.7: Integrity2

QUESTION 9

An employee of the organization accidentally deleted customers\\' data stored in the database. What is the impact of this action?

A. Information is not accessible when required

B. Information is modified in transit

C. Information is not available to only authorized users

Correct Answer: A

Explanation: According to ISO/IEC 27001:2022, availability is one of the three principles of information security, along with confidentiality and integrity1. Availability means that information is accessible and usable by authorized persons

whenever it is needed2. If an employee of the organization accidentally deleted customers\\' data stored in the database, this would affect the availability of the information, as it would not be accessible when required by the authorized persons,

such as the customers themselves, the organization\\'s staff, or other stakeholders. This could result in loss of trust, reputation, or business opportunities for the organization, as well as dissatisfaction or inconvenience for the customers.

References:

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements What is ISO 27001? A detailed and straightforward guide - Advisera

---

QUESTION 10

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^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company\\'s top management, was a potential conflict of interest. The request was not accepted by the certification body

NetworkFuse should_____to ensure that employees are prepared for the audit. Refer to scenario 10.

A. Conduct practice interviews

B. Observe the technologies used

C. Select a certification body that provides combined audits

Correct Answer: A

Explanation: One of the ways to prepare employees for an ISO/IEC 27001 audit is to conduct practice interviews with them. This can help them to familiarize themselves with the audit process, the types of questions they might be asked, and the evidence they need to provide to demonstrate compliance with the standard. Practice interviews can also help employees to identify any gaps or weaknesses in their knowledge or performance, and to address them before the actual audit. Practice interviews can be conducted by internal auditors, managers, or consultants, and should cover the relevant scope, objectives, and criteria of the audit. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113) References: PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113 PECB ISO/IEC 27001 Lead Implementer Info Kit, page 10 5 Step Plan: How to Prepare for an ISO 27001 Certification Audit

---

QUESTION 11

Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management [^system implementation, TradeB\\'s top management contracted two experts to direct and manage the ISMS implementation project.

First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity

Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted

What should TradeB do in order to deal with residual risks? Refer to scenario 4.

A. TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment

B. TradeB should immediately implement new controls to treat all residual risks

C. TradeB should accept the residual risks only above the acceptance level

Correct Answer: A

Explanation: According to ISO/IEC 27001 : 2022 Lead Implementer, residual risk is the risk remaining after risk treatment. Residual risk should be compared with the acceptable level of risk, which is the level of risk that the organization is willing to tolerate. If the residual risk is below the acceptable level of risk, then the risk can be accepted. If the residual risk is above the acceptable level of risk, then additional risk treatment options should be considered. Therefore, TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment, which is the difference between the initial risk and the residual risk. This will help TradeB to determine whether the risk treatment was effective and whether the residual risk is acceptable or not. References: ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process

---

QUESTION 12

An organization uses Platform as a Services (PaaS) to host its cloud-based services As such, the cloud provider manages most off the services to the organization. However, the organization still manages_____

A. Operating system and visualization

B. Servers and storage

C. Application and data

Correct Answer: C