LEAD-IMPLEMENTER$^{Q\&As}$

PECB Certified ISO/IEC 27001 Lead Implementer

Pass PECB LEAD-IMPLEMENTER Exam with 100% Guarantee

Following Questions and Answers are all new published by PECB Official Exam Center

QUESTION 1

An organization wants to enable the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. Which control should it implement7

A. Use of privileged utility programs

B. Clock synchronization

C. Installation of software on operational systems

Correct Answer: B

Explanation: Clock synchronization is the control that enables the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. According to ISO/IEC 27001:2022, Annex A, control A.8.23.1 states: "The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source." This ensures that the timestamps of the events and data are consistent and accurate across different systems and sources, which facilitates the identification of causal relationships, patterns, trends, and anomalies. Clock synchronization also helps to establish the sequence of events and the responsibility of the parties involved in an incident. References: ISO/IEC 27001:2022, Annex A, control A.8.23.1 PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 21

QUESTION 2

Diana works as a customer service representative for a large e-commerce company. One day, she accidently modified the order details of a customer without their permission Due to this error, the customer received an incorrect product. Which information security principle was breached in this case7

A. Availability

B. Confidentiality

C. Integrity

Correct Answer: C

Explanation: According to ISO/IEC 27001:2022, information security controls are measures that are implemented to protect the confidentiality, integrity, and availability of information assets1. Controls can be preventive, detective, or corrective, depending on their purpose and nature2. Preventive controls aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Detective controls aim to detect or discover the occurrence of a security incident or its symptoms. Corrective controls aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact2. In this scenario, Socket Inc. implemented several security controls to prevent information security incidents from recurring, such as: Segregation of networks: This is a preventive and technical control that involves separating different parts of a network into smaller segments, using devices such as routers, firewalls, or VPNs, to limit the access and communication between them3. This can enhance the security and performance of the network, as well as reduce the administrative efforts and costs3. Privileged access rights: This is a preventive and administrative control that involves granting access to information assets or systems only to authorized personnel who have a legitimate need to access them, based on their roles and responsibilities4. This can reduce the risk of unauthorized access, misuse, or modification of information assets or systems4. Cryptographic controls: This is a preventive and technical control that involves the use of cryptography, which is the science of protecting information by transforming it into an unreadable format, to protect the confidentiality, integrity, and authenticity of information assets or systems. This can prevent unauthorized access, modification, or disclosure of information assets or systems. Information security threat management: This is a preventive and administrative control that involves the identification, analysis, and response to information security threats, which are any incidents that could negatively affect the confidentiality, integrity, or availability of information assets or systems. This can help the organization to anticipate, prevent, or mitigate the impact of information security threats. Information security integration into project management: This is a preventive and administrative control that involves the incorporation of information security requirements and controls into the planning, execution, and closure of projects, which are temporary endeavors undertaken to create a unique product, service, or result. This can ensure that information security risks and opportunities are identified and addressed throughout the project life cycle. However, information backup is not a preventive control, but a corrective control. Information backup is a corrective and technical control that involves the creation and maintenance of copies of information assets or systems, using dedicated software and utilities, to ensure that they can be recovered in case of data loss, corruption, accidental deletion, or cyber incidents. This can help the organization to restore the normal state of information assets or systems after a security incident or mitigate its impact. Therefore, information backup does not prevent information security incidents from recurring, but rather helps the organization to recover from them.

QUESTION 3

Kyte. a company that has an online shopping website, has added a QandA section to its website; however, its Customer Service Department almost never provides answers to users\\' questions. Which principle of an effective communication strategy has Kyte not followed?

A. Clarity

B. Appropriateness

C. Responsiveness

Correct Answer: B

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

QUESTION 4

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 ensures that the group of employees targeted have satisfied the organization\\'s needs

B. After he conducts a competence needs analysis and records the competence related issues

C. After he determines the employees\\' availability and motivation

Correct 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. References: ISO/IEC 27001:2022, clause 7.2.3; PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 8.

QUESTION 5

Which of the following is NOT part of the steps required by ISO/IEC 27001 that an organization must take when a nonconformity is detected?

A. React to the nonconformity, take action to control and correct it. and deal with its consequences

B. Evaluate the need for action to eliminate the causes of the nonconformity so that it does not recur or occur elsewhere

C. Communicate the details of the nonconformity to every employee of the organization and suspend the employee that caused the nonconformity

Correct Answer: C

Explanation: According to the ISO/IEC 27001 : 2022 Lead Implementer course, the steps required by ISO/IEC 27001 that an organization must take when a nonconformity is detected are as follows1: React to the nonconformity, take action to control and correct it, and deal with its consequences Evaluate the need for action to eliminate the causes of the nonconformity so that it does not recur or occur elsewhere Implement any action needed Review the effectiveness of the corrective action Make changes to the information security management system (ISMS) if necessary Therefore, communicating the details of the nonconformity to every employee of the organization and suspending the employee that caused the nonconformity is not part of the steps required by ISO/IEC 27001. This option is not only unnecessary, but also potentially harmful, as it could violate the principles of confidentiality, integrity, and availability of information, as well as the human rights and dignity of the employee involved2. Instead, the organization should follow the established procedures for reporting, recording, and analyzing nonconformities, and ensure that the corrective actions are appropriate, proportional, and fair3. References: 1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10:

Nonconformity and Corrective Action, slide 9 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10: Nonconformity and Corrective Action, slide 10 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10: Nonconformity and Corrective Action, slide