LEAD-IMPLEMENTER Q&As

PECB Certified ISO/IEC 27001 Lead Implementer

Pass PECB LEAD-IMPLEMENTER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/lead-implementer.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which tool is used to identify, analyze, and manage interested parties?

A. The probability/impact matrix

B. The power/interest matrix

C. The likelihood/severity matrix

Correct Answer: B

Explanation: The power/interest matrix is a tool that can be used to identify, analyze, and manage interested parties according to ISO/IEC 27001:2022. The power/interest matrix is a two-dimensional diagram that plots the level of power and interest of each interested party in relation to the organization\\'s information security objectives. The power/interest matrix can help the organization to prioritize the interested parties, understand their expectations and needs, and develop appropriate communication and engagement strategies. The power/interest matrix can also help the organization to identify potential risks and opportunities related to the interested parties. References: ISO/IEC 27001:2022, clause 4.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 12.

QUESTION 2

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.

Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001\\' Refer to scenario 3.

A. No, the control should be implemented only for defining rules for cryptographic key management

B. Yes, the control for the effective use of the cryptography can include cryptographic key management

C. No, because the standard provides a separate control for cryptographic key management

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, Annex A.8.24, the control for the effective use of cryptography is intended to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This control can include cryptographic key management, which is the process of generating, distributing, storing, using, and destroying cryptographic keys in a secure manner. Cryptographic key management is essential for ensuring the security and functionality of cryptographic solutions, such as encryption, digital signatures, or authentication. The standard provides the following guidance for implementing this control: A policy on the use of cryptographic controls should be developed and implemented. The policy should define the circumstances and conditions in which the different types of cryptographic controls should be used, based on the information classification scheme, the relevant agreements, legislation, and regulations, and the assessed risks. The policy should also define the standards and techniques to be used for each type of cryptographic control, such as the algorithms, key lengths, key formats, and key lifecycles. The policy should be reviewed and updated regularly to reflect the changes in the technology, the business environment, and the legal requirements. The cryptographic keys should be managed through their whole lifecycle, from generation to destruction, in a secure and controlled manner, following the principles of need-to-know and segregation of duties. The cryptographic keys should be protected from unauthorized access, disclosure, modification, loss, or theft, using appropriate physical and logical security measures, such as encryption, access control, backup, and audit. The cryptographic keys should be changed or replaced periodically, or when there is a suspicion of compromise, following a defined process that ensures the continuity of the cryptographic services and the availability of the information. The cryptographic keys should be securely destroyed when they are no longer required, or when they reach their end of life, using methods that prevent their recovery or reconstruction. 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 Understanding Cryptographic Controls in Information Security5

QUESTION 3

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\\' 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\\'s patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients\\' 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?

A. Availability

B. Confidentiality

C. Integrity

Correct Answer: A

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 -- Security techniques -- Information security management systems -Requirements, clause 3.13.

QUESTION 4

What risk treatment option has Company A implemented if it has required from its employees the change of email passwords at least once every 60 days?

A. Risk modification

B. Risk avoidance

C. Risk retention

Correct Answer: A

Explanation: Risk modification is one of the four risk treatment options defined by ISO/IEC 27001, which involves applying controls to reduce the likelihood and/or impact of the risk. By requiring its employees to change their email passwords at least once every 60 days, Company A has implemented a risk modification option to reduce the risk of unauthorized access to its email accounts. Changing passwords frequently can make it harder for attackers to guess or crack the passwords, and can limit the damage if a password is compromised. The other three risk treatment options are: Risk avoidance: This option involves eliminating the risk source or discontinuing the activity that causes the risk. For example, Company A could avoid the risk of email compromise by not using email at all, but this would also mean losing the benefits of email communication. Risk retention: This option involves accepting the risk and its consequences, either because the risk is too low to justify any treatment, or because the cost of treatment is too high compared to the potential loss. For example, Company A could retain the risk of email compromise by not implementing any security measures, but this would expose the company to potential breaches and reputational damage. Risk transfer: This option involves sharing or transferring the risk to a third party, such as an insurer, a supplier, or a partner. For example, Company A could transfer the risk of email compromise by outsourcing its email service to a cloud provider, who would be responsible for the security and availability of the email accounts. References: ISO/IEC 27001:2013, clause 6.1.3: Information security risk treatment 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 27001 Risk Assessment and Risk Treatment: The Complete Guide - Advisera1 Infosec Risk Treatment for ISO 27001 Requirement 8.3 - ISMS.online2 ISO 27001 Clause 6.1.3 Information security risk treatment3 ISO 27001 Risk Treatment Plan - Scrut Automation4

QUESTION 5

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 scenario 2, Beauty should have implemented (1)_____ to detect (2)_____.

A. (1) An access control software, (2) patches

B. (1) Network intrusions, (2) technical vulnerabilities

C. (1) An intrusion detection system, (2) intrusions on networks

Correct Answer: C

Explanation: An intrusion detection system (IDS) is a device or software application that monitors network activities, looking for malicious behaviors or policy violations, and reports their findings to a management station. An IDS can help an

organization to detect intrusions on networks, which are unauthorized attempts to access, manipulate, or harm network resources or data. In the scenario, Beauty should have implemented an IDS to detect intrusions on networks, such as the

one that exposed customers\\' information due to the out-of-date anti-malware software. An IDS could have alerted the IT team about the suspicious network activity and helped them to respond faster and more effectively.

Therefore, the correct answer is C.

References: ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements, clause 3.14; ISO/IEC 27039:2015, Information technology -- Security techniques -- Selection,

deployment and operations of intrusion detection and prevention systems (IDPS), clause 4.1.