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

PECB Certified ISO/IEC 27001 Lead Implementer

Pass PECB LEAD-IMPLEMENTER Exam with 100% Guarantee

QUESTION 1

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company\\'s departments within the ISMS scope. The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze\\'s top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze\\'s top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.

Based on the scenario above, answer the following question:

What led Operaze to implement the ISMS?

A. Identification of vulnerabilities

B. Identification of threats

C. Identification of assets

Correct Answer: A

Explanation: According to the scenario, Operaze conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration testing and code review, the company identified some issues in its ICT systems, such as improper user permissions, misconfigured security settings, and insecure network configurations. These issues are examples of vulnerabilities, which are weaknesses or gaps in the protection of an asset that can be exploited by a threat. Therefore, the identification of vulnerabilities led Operaze to implement the ISMS. References: ISO/IEC 27001:2022 Lead Implementer Training Course Guide1 ISO/IEC 27001:2022 Lead Implementer Info Kit2

QUESTION 2

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly

Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company\\'s stock.

Tessa was SunDee\\'s internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee\\'s negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management

Based on the scenario above, answer the following question:

What caused SunDee\\'s workforce disruption?

A. The negligence of performance evaluation and monitoring and measurement procedures

B. The inconsistency of reports written by different employees

C. The voluminous written reports

Correct Answer: A

Explanation: According to ISO/IEC 27001:2013, clause 9.1, an organization must monitor, measure, analyze and evaluate its information security performance and effectiveness. This includes determining what needs to be monitored and measured, the methods for doing so, when and by whom the monitoring and measurement shall be performed, when the results shall be analyzed and evaluated, and who shall be responsible for ensuring that the actions arising from the analysis and evaluation are taken 1. SunDee failed to comply with this requirement and did not monitor or measure the performance and effectiveness of its ISMS for the past two years. As a result, the company did not have any objective evidence or indicators to demonstrate the achievement of its information security objectives, the effectiveness of its controls, the satisfaction of its interested parties, or the identification and treatment of its risks. This also meant that the company did not conduct regular management reviews of its ISMS, as required by clause 9.3, which would provide an opportunity for the top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS, and to decide on any changes or improvements needed 1. Just before the recertification audit, the company decided to conduct an internal audit, as required by clause 9.2, which is a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled 1. However, the company did not have a well-defined audit program, scope, criteria, or methodology, and relied on the written reports of its staff for the past two years. This caused a disruption in the workforce, as most of the staff had to compile their reports for their departments, leaving the Production Department with less than the optimum workforce, which decreased the company\\'s stock. Moreover, the internal audit process was very inconsistent, as the reports were written by different employees with different styles, formats, and levels of detail. The internal audit process also lacked any qualitative measures, such as performance indicators, metrics, or benchmarks, to evaluate the performance and effectiveness of the ISMS. Therefore, the cause of SunDee\\'s workforce disruption was the negligence of performance evaluation and monitoring and measurement procedures, which led to a lack of objective evidence, a poorly planned and executed internal audit, and a decrease in the company\\'s productivity and stock value.

QUESTION 3

Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.

Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:

A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department

The approved action plan was implemented and all actions described in the plan were documented.

Based on scenario 9. is the action plan for the identified nonconformities sufficient to eliminate the detected nonconformities?

A. Yes, because a separate action plan has been created for the identified nonconformity

B. No, because the action plan does not include a timeframe for implementation

C. No, because the action plan does not address the root cause of the identified nonconformity

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 10.1, an action plan for nonconformities and corrective actions should include the following elements1: What needs to be done Who is responsible for doing it When it will be completed How the effectiveness of the actions will be evaluated How the results of the actions will be documented In scenario 9, the action plan only describes what needs to be done and who is responsible for doing it, but it does not specify when it will be completed, how the effectiveness of the actions will be evaluated, and how the results of the actions will be documented. Therefore, the action plan is not sufficient to eliminate the detected nonconformities. References:

1: ISO/IEC 27001:2022, Information technology -- Security techniques -- Information security management systems -- Requirements, clause 10.1, Nonconformity and corrective action.

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. 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 5

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 6

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 7

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly

Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company\\'s stock.

Tessa was SunDee\\'s internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee\\'s negligence of

ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management

According to scenario 8, Tessa created a plan for ISMS monitoring and measurement and presented it to the top management Is this acceptable?

A. No, Tessa should only communicate the issues found to the top management

B. Yes, Tessa can advise the top management on improving the company\\'s functions

C. No, Tessa must implement all the improvements needed for issues found during the audit

Correct Answer: B

Explanation: According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the roles and responsibilities of an internal auditor is to provide recommendations for improvement based on the audit findings1. Therefore, Tessa can create a plan for ISMS monitoring and measurement and present it to the top management as a way of advising them on how to improve the company\\'s functions. However, Tessa is not responsible for implementing the improvements or communicating the issues found to the top management. Those tasks belong to the process owners and the management representative, respectively2. References: 1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 14 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide

QUESTION 8

Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.

Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:

A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department

The approved action plan was implemented and all actions described in the plan were documented.

Based on scenario 9, OpenTech has taken all the actions needed, except____________.

A. Corrective actions

B. Preventive actions

C. Permanent corrections

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 10.1, corrective actions are actions taken to eliminate the root causes of nonconformities and prevent their recurrence, while preventive actions are actions taken to eliminate the root causes of potential nonconformities and prevent their occurrence. In scenario 9, OpenTech has taken corrective actions to address the nonconformity related to the monitoring procedures, but not preventive actions to avoid similar nonconformities in the future. For example, OpenTech could have taken preventive actions such as conducting regular reviews of the access control policy, providing training and awareness to the staff on the policy, or implementing automated controls to prevent user ID reuse. References: ISO/IEC 27001:2022, Information technology -- Security techniques -- Information security management systems -- Requirements, clause 10.1 PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Performance evaluation, improvement and certification audit of an ISMS, slide 8.3.1.1

QUESTION 9

An organization has justified the exclusion of control 5.18 Access rights of ISO/IEC 27001 in the Statement of Applicability (SoA) as follows: "An access control reader is already installed at the main entrance of the building." Which statement is correct\\'

A. The justification for the exclusion of a control is not required to be included in the SoA

B. The justification is not acceptable, because it does not reflect the purpose of control 5.18

C. The justification is not acceptable because it does not indicate that it has been selected based on the risk assessment results

Correct Answer: B

Explanation: According to ISO/IEC 27001:2022, clause 6.1.3, the Statement of Applicability (SoA) is a document that identifies the controls that are applicable to the organization\\'s ISMS and explains why they are selected or not. The SoA is based on the results of the risk assessment and risk treatment, which are the previous steps in the risk management process. Therefore, the justification for the exclusion of a control should be based on the risk assessment results and the risk treatment plan, and should reflect the purpose and objective of the control. Control 5.18 of ISO/IEC 27001:2022 is about access rights to information and other associated assets, which should be provisioned, reviewed, modified and removed in accordance with the organization\\'s topic-specific policy on and rules for access control. The purpose of this control is to prevent unauthorized access to, modification of, and destruction of information assets. Therefore, the justification for the exclusion of this control should explain why the organization does not need to implement this control to protect its information assets from unauthorized access. The justification given by the organization in the question is not acceptable, because it does not reflect the purpose of control 5.18. An access control reader at the main entrance of the building is a physical security measure, which is related to control 5.15 of ISO/IEC 27001:2022, not control 5.18. Control 5.18 is about logical access rights to information systems and services, which are not addressed by the access control reader. Therefore, the organization should either provide a valid justification for the exclusion of control 5.18, or include it in the SoA and implement it according to the risk assessment and risk treatment results. References: ISO/IEC 27001:2022, clause 6.1.3, control 5.18; PECB ISO/IEC 27001 Lead Implementer Course, Module 5, slide 18, Module 6, slide 10.

QUESTION 10

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 11

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 12

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?

A. Annex A 5.5 Contact with authorities

B. Annex A 5 7 Threat Intelligence

C. Annex A 5.13 Labeling of information

Correct Answer: B

Explanation: 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. References: ISO/IEC 27001:2022 Information technology -- Security techniques -- Information security management systems -- Requirements, Annex A 5.7 Threat Intelligence ISO/IEC 27002:2022 Information technology -- Security techniques -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

QUESTION 13

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 14

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.

Based on scenario 1. what is a potential impact of the loss of integrity of information in HealthGenic?

A. Disruption of operations and performance degradation

B. Incomplete and incorrect medical reports

C. Service interruptions and complicated user interface

Correct Answer: B

Explanation: The loss of integrity of information in HealthGenic means that the information was modified or corrupted in an unauthorized or improper way, resulting in inaccurate, incomplete, or unreliable data. This can have a serious impact on the quality and safety of the medical services provided by HealthGenic, as well as the trust and satisfaction of the patients and their families. In particular, incomplete and incorrect medical reports can lead to:

Misdiagnosis or delayed diagnosis of the patients\\' conditions, which can affect their treatment and recovery.

Prescription of wrong or inappropriate medications or dosages, which can cause adverse effects or interactions.

Violation of the patients\\' privacy and confidentiality, which can expose them to identity theft, fraud, or discrimination.

Legal liability and reputational damage for HealthGenic, which can result in lawsuits, fines, or loss of customers.

Therefore, it is essential for HealthGenic to ensure the integrity of its information by implementing appropriate security controls and measures, such as encryption, authentication, backup, audit, and incident response.

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

QUESTION 15

A small organization that is implementing an ISMS based on ISO/lEC 27001 has decided to outsource the internal audit function to a third party. Is this acceptable?

A. Yes, outsourcing the internal audit function to a third party is often a better option for small organizations to demonstrate independence and impartiality

B. No, the organizations cannot outsource the internal audit function to a third party because during internal audit, the organization audits its own system

C. No, the outsourcing of the internal audit function may compromise the independence and impartiality of the internal audit team

Correct Answer: A

Explanation: According to the ISO/IEC 27001:2022 standard, an internal audit is an audit conducted by the organization itself to evaluate the conformity and effectiveness of its information security management system (ISMS). The standard

requires that the internal audit should be performed by auditors who are objective and impartial, meaning that they should not have any personal or professional interest or bias that could influence their judgment or compromise their integrity.

The standard also allows the organization to outsource the internal audit function to a third party, as long as the criteria of objectivity and impartiality are met.

Outsourcing the internal audit function to a third party can be a better option for small organizations that may not have enough resources, skills, or experience to perform an internal audit by themselves. By hiring an external auditor, the

organization can benefit from the following advantages:

The external auditor can provide a fresh and independent perspective on the organization\\'s ISMS, identifying strengths, weaknesses, opportunities, and threats that may not be apparent to the internal staff.

The external auditor can bring in specialized knowledge, expertise, and best practices from other organizations and industries, helping the organization to improve its ISMS and achieve its objectives.

The external auditor can reduce the risk of conflict of interest, bias, or influence that may arise when the internal staff audit their own work or the work of their colleagues.

The external auditor can save the organization time and money by conducting the internal audit more efficiently and effectively, avoiding duplication of work or unnecessary delays.

Therefore, outsourcing the internal audit function to a third party is acceptable and often preferable for small organizations that are implementing an ISMS based on ISO/IEC 27001.

References:

ISO/IEC 27001:2022, Information technology -- Security techniques -- Information security management systems -- Requirements, Clause 9.2, Internal audit ISO/IEC 27007:2023, Information technology -- Security techniques -- Guidelines for information security management systems auditing PECB, ISO/IEC 27001 Lead Implementer Course, Module 12, Internal audit A Complete Guide to an ISO 27001 Internal Audit - Sprinto

LEAD-IMPLEMENTER Practice Test

LEAD-IMPLEMENTER Exam Questions

LEAD-IMPLEMENTER Braindumps