Latest Version: 6.0

Question: 1

Why should the security testing processes be defined and implemented in the development life cycle?

A. To protect the production environment and data from compromise by development and test activities
B. To validate if information security requirements are met when applications are deployed to the production environment
C. To Identify organizational assets and define appropriate protection responsibilities

Answer: C

Question: 2

What is the main purpose of Annex A 7.1 Physical security perimeters of ISO/IEC 27001?

A. To prevent unauthorized physical access, damage, and interference to the organization's information and other associated assets
B. To maintain the confidentiality of information that is accessible by personnel or external parties
C. To ensure access to information and other associated assets is defined and authorized

Answer: A

Explanation:
Annex A 7.1 of ISO/IEC 27001 : 2022 is a control that requires an organization to define and implement security perimeters and use them to protect areas that contain information and other associated assets. Information and information security assets can include data, infrastructure, software, hardware, and personnel. The main purpose of this control is to prevent unauthorized physical access, damage, and interference to these assets, which could compromise the confidentiality, integrity, and availability of the information. Physical security perimeters can include fences, walls, gates, locks, alarms, cameras, and other barriers or devices that restrict or monitor access to the facility or area. The organization should also consider the environmental and fire protection of the assets, as well as the disposal of any waste or media that could contain sensitive information.
Reference:
ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Section 5.3.1.7, page 101
ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 17
ISO/IEC 27002 : 2022, Control 7.1 – Physical Security Perimeters 1 2 3

Question: 3

Some of the issues being discussed in the awareness session were too technical for the participants. What does this situation indicate? Refer to scenario 6.

A. Employees are equipped with information security expertise, therefore. they do not represent a potential risk
B. TradeB did not evaluate the competence of the trainer
C. TradeB did not determine the type and level of competence needed

Answer: C

Question: 4

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

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 findings 1 . 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, respectively 2 .

Reference: 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 15

Question: 5

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 scenario 8. does SunDee comply with ISO/IEC 27001 requirements regarding the monitoring and measurement process?

A. Yes. because the standard does not Indicate when the monitoring and measurement phase should be performed
B. Yes, because the standard requires that the monitoring and measurement phase be conducted every two years
C. No, because even though the standard does not imply when such a process should be performed, the company must have a monitoring and measurement process in place

Answer: C

Explanation:
According to ISO/IEC 27001:2022, clause 9.1, the organization shall determine:
what needs to be monitored and measured, including information security processes and controls, as well as information security performance and the effectiveness of the ISMS;
the methods for monitoring, measurement, analysis and evaluation, to ensure valid and reliable results;
when the monitoring and measurement shall be performed;
who shall monitor and measure;
who shall analyze and evaluate the monitoring and measurement results; and
how the results shall be communicated and used for decision making and improvement.
The organization shall retain documented information as evidence of the monitoring and measurement results.
The standard does not prescribe a specific frequency or method for monitoring and measurement, but it requires the organization to have a defined and documented process that is appropriate to its context, objectives, risks, and opportunities. The organization should also ensure that the monitoring and

measurement results are analyzed and evaluated to determine the performance and effectiveness of the ISMS, and to identify any nonconformities, gaps, or improvement opportunities.
In the scenario, SunDee did not comply with these requirements, as it did not have a monitoring and measurement process in place, and did not monitor or measure the performance and effectiveness of its ISMS regularly. It also did not use valid and reliable methods, or communicate and use the results for improvement. Therefore, SunDee's negligence of ISMS performance evaluation was a major nonconformity, as Tessa correctly identified.
Reference: ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, clause 9.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 9: Monitoring, Measurement, Analysis and Evaluation.

Question: 6

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

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.
Reference:
ISO/IEC 27001:2022 Lead Implementer Course Guide 1
ISO/IEC 27001:2022 Lead Implementer Info Kit 2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements 3
ISO/IEC 27002:2022 Code of Practice for Information Security Controls 4
Understanding Cryptographic Controls in Information Security 5

Question: 7

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

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.
Reference:
ISO/IEC 27001:2022 Lead Implementer Course Guide 1
ISO/IEC 27001:2022 Lead Implementer Info Kit 2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements 3
ISO/IEC 27002:2022 Code of Practice for Information Security Controls 4
What are Information Security Controls? - SecurityScorecard 4
What Are the Types of Information Security Controls? - RiskOptics 2
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 27001:2022 1 ; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 3.7: Integrity 2

Question: 8

Which of the following practices Indicates that Company A has Implemented clock synchronization?

A. Logs that record activities and other relevant events are stored and analyzed
B. Information processing systems are coordinated according to an approved time source
C. Suspected information security events are reported in a timely manner through an appropriate channel

Answer: B

Question: 9

What is the most important asset to Socket Inc. associated with the use of cloud storage? Refer to scenario 5.

A. IT provided network drives

B. Employees with access to cloud storage files
C. Customers' personal data

Answer: C

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.

Based on this scenario, answer the following question:

Based on his tasks, which team is Bob part of?

A. Security architecture team
B. Forensics team
C. Incident response team

Answer: C

Explanation:

Based on his tasks, Bob is part of the incident response team (IRT) of InfoSec. According to ISO/IEC 27035-2:2023, the IRT is a team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way 1 . One of the tasks of the IRT is to conduct an evaluation of the nature of an unexpected event, including the details on how the event happened and what or whom it might affect 1 . This is consistent with Bob’s responsibility of ensuring that a thorough evaluation of the nature of an unexpected event is conducted. Therefore, Bob belongs to the incident response team.

Reference:
ISO/IEC 27035-2:2023 (en), Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response 1
Response to Information Security Incidents | ISMS.online 2