Question #1 *Topic 1*

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 the scenario above, answer the following question:

Which of the following indicates that the confidentiality of information was compromised?

A. Service interruptions due to the increased number of users

B. Invasion of patients' privacy

C. Modification of patients' medical reports

Correct Answer: *B*

freddyflex 3 months, 2 weeks ago

B. Confidentiality, right answer

upvoted 1 times

ali3534223 5 months, 2 weeks ago

D. compromise of patient information

upvoted 1 times

Question #2 *Topic 1*

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*

Community vote distribution

B (100%)

Cutiedupc 4 months, 2 weeks ago

Selected Answer: B

Incomplete data show loss of intergrity

upvoted 2 times

Question #3 *Topic 1*

Intrinsic vulnerabilities, such as the ___________, are related to the characteristics of the asset. Refer to scenario 1.

A. Software malfunction

B. Service interruptions

C. Complicated user interface

Correct Answer: *C*

freddyflex 3 months, 2 weeks ago

C. The software is the asset

upvoted 1 times

Question #4 *Topic 1*

Which situation described in scenario 1 represents a threat to HealthGenic?

A. HealthGenic did not train its personnel to use the software

B. The software company modified information related to HealthGenic's patients

C. HealthGenic used a web-based medical software for storing patients' confidential information

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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*

freddyflex 3 months, 2 weeks ago

A. Service disruption - availability

upvoted 1 times

Question #6 *Topic 1*

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 gained 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*

Community vote distribution

C (50%) A (50%)

Everfaithful1 2 months, 3 weeks ago

Selected Answer: C

C. Corrective

Beauty's decision to install new anti-malware software after the security incident is a corrective control. Corrective controls are implemented to respond to and fix issues after a security event has occurred, aiming to mitigate the impact of the incident and prevent recurrence. In this case, the new anti-malware software was installed to address the issue and prevent future breaches by automatically removing malicious code.

upvoted 2 times

Everfaithful1 2 months, 3 weeks ago

Selected Answer: C

The answer is C because the solution was implemented after an incidence had occurred. Any action taken after an incidence is a corrective action, even if it would prevent a recurrence.

upvoted 1 times

Winbe 3 months, 1 week ago

Selected Answer: A

Why is the answer C, and not A?

upvoted 2 times

Question #7 *Topic 1*

Which statement below suggests that Beauty has implemented a managerial control that helps avoid the occurrence of incidents? Refer to scenario 2.

A. Beauty's employees signed a confidentiality agreement

B. Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information

C. Beauty updated the segregation of duties chart

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

According to scenario 2, Beauty has reviewed all user access rights. What type of control is this?

A. Detective and administrative

B. Corrective and managerial

C. Legal and technical

Correct Answer: *A*

Community vote distribution

B (100%)

Everfaithful1 2 months, 3 weeks ago

Selected Answer: B

B. Corrective and managerial

This is because Beauty implemented corrective controls (installing new anti-malware software and updating it) to fix the issue after the incident occurred. Additionally, the actions of updating policies, conducting security awareness sessions, and managing user access rights fall under managerial controls, which are focused on oversight, administration, and policy management to ensure compliance and security.

upvoted 1 times

Everfaithful1 2 months, 3 weeks ago

I had a second look at the question, the answer is A. I would like to withdraw my initial answer.

upvoted 1 times

Question #9 *Topic 1*

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*

Community vote distribution

A (100%)

Everfaithful1 2 months, 3 weeks ago

Selected Answer: A

Based on the options provided, the best fit for each is:

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

(1) Access control software is used to manage who can access what resources, ensuring that only authorized users have access.
(2) Patches are software updates designed to fix vulnerabilities and security issues in a system.
This pairing makes sense because it lists specific technical measures (access control software and patches) related to securing systems and addressing vulnerabilities.

upvoted 1 times

Question #10 *Topic 1*

Based on scenario 2, which information security principle is the IT team aiming to ensure by establishing a user authentication process that requires user identification and password when accessing sensitive information?

A. Integrity

B. Confidentiality

C. Availability

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

FinanceX, a well-known financial institution, uses an online banking platform that enables clients to easily and securely access their bank accounts. To log in, clients are required to enter the one-time authorization code sent to their smartphone. What can be concluded from this scenario?

A. FinanceX has implemented a security control that ensures the confidentiality of information

B. FinanceX has implemented an integrity control that avoids the involuntary corruption of data

C. FinanceX has incorrectly implemented a security control that could become a vulnerability

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Which of the following statements regarding information security risk is NOT correct?

A. Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats

B. Information security risk cannot be accepted without being treated or during the process of risk treatment

C. Information security risk can be expressed as the effect of uncertainty on information security objectives

Correct Answer: *B*

Community vote distribution

B (100%)

Everfaithful1 2 months, 3 weeks ago

Selected Answer: B

The incorrect statement is:

B. Information security risk cannot be accepted without being treated or during the process of risk treatment

This statement is NOT correct because according to ISO 27001, risk acceptance is one of the possible risk treatment options. Organizations may accept certain risks if the cost of mitigation is higher than the potential impact of the risk or if the risk is deemed to be at an acceptable level. Therefore, information security risks can be accepted without being treated, as part of the risk treatment process.

upvoted 1 times

Question #14 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

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 case?

A. Availability

B. Confidentiality

C. Integrity

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

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 the scenario above, answer the following question:
Which security control does NOT prevent information security incidents from recurring?

A. Segregation of networks

B. Privileged access rights

C. Information backup

Correct Answer: *C*

⊟ **c827257** 3 weeks, 4 days ago

Selected Answer: C

because the backup is not a preventive controls

upvoted 1 times

Question #17 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Can Socket Inc. find out that no persistent backdoor was placed and that the attack was initiated from an employee inside the company by reviewing event logs that record user faults and exceptions? Refer to scenario 3.

A. Yes, Socket Inc. can find out that no persistent backdoor was placed by only reviewing user faults and exceptions logs

B. No, Socket Inc. should also have reviewed event logs that record user activities

C. No, Socket Inc. should have reviewed all the logs on the syslog server

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19

Topic 1

Based on scenario 3. what would help Socket Inc. address similar information security incidents in the future?

A. Using the MongoDB database with the default settings

B. Using cryptographic keys to protect the database from unauthorized access

C. Using the access control system to ensure that only authorized personnel is granted access

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

An organization documented each security control that it implemented by describing their functions in detail. Is this compliant with ISO/IEC 27001?

A. No, the standard requires to document only the operation of processes and controls, so no description of each security control is needed

B. No, because the documented information should have a strict format, including the date, version number and author identification

C. Yes, but documenting each security control and not the process in general will make it difficult to review the documented information

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which security controls must be implemented to comply with ISO/IEC 27001?

A. Those designed by the organization only

B. Those included in the risk treatment plan

C. Those listed in Annex A of ISO/IEC 27001, without any exception

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

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

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24

Topic 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 implement?

A. Use of privileged utility programs

B. Clock synchronization

C. Installation of software on operational systems

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

The incident management process of an organization enables them to prepare for and respond to information security incidents. In addition, the organization has procedures in place for assessing information security events. According to ISO/IEC 27001, what else must an incident management process include?

A. Processes for using knowledge gained from information security incidents

B. Establishment of two information security incident response teams

C. Processes for handling information security incidents of suppliers as defined in their agreements

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 Topic 1

Who should be involved, among others, in the draft, review, and validation of information security procedures?

A. An external expert

B. The information security committee

C. The employees in charge of ISMS operation

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

An organization has implemented a control that enables the company to manage storage media through their life cycle of use, acquisition, transportation and disposal. Which control category does this control belong to?

A. Organizational

B. Physical

C. Technological

Correct Answer: *B*

EwomaZno 1 month, 1 week ago

C, Control 8.12 data leakage prevention. so the answer is C.

upvoted 2 times

tovich 2 months ago

C, storage refers to Backup which is included in the 34 security controls divided in five caegory : Malware protection, Backups, Logging and monitoring, Network security and Segregation and lastly Development and Coding practices

upvoted 2 times

Question #28

Topic 1

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 the scenario above, answer the following question:

The decision to treat only risks that were classified as high indicates that TradeB has:

A. Evaluated other risk categories based on risk treatment criteria

B. Accepted other risk categories based on risk acceptance criteria

C. Modified other risk categories based on risk evaluation criteria

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Based on scenario 4, what type of assets were identified during risk assessment?

A. Supporting assets

B. Primary assets

C. Business assets

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Which of the actions presented in scenario 4 is NOT compliant with the requirements of ISO/IEC 27001?

A. TradeB selected only ISO/IEC 27001 controls deemed applicable to the company

B. The Statement of Applicability was drafted before conducting the risk assessment

C. The external experts selected security controls and drafted the Statement of Applicability

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 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 testing 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*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Based on scenario 5, after migrating to cloud, Operaze's IT team changed the ISMS scope and implemented all the required modifications. Is this acceptable?

A. Yes, because the ISMS scope should be changed when there are changes to the external environment

B. No, because the company has already defined the ISMS scope

C. No, because any change in ISMS scope should be accepted by the management

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

Based on scenario 5, in which category of the interested parties does the HR manager of Operaze belong?

A. Positively influenced interested parties, because the ISMS will increase the effectiveness and efficiency of the HR Department

B. Negatively influenced interested parties, because the HR Department will deal with more documentation

C. Both A and B

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Based on scenario 5, which committee should Operaze create to ensure the smooth running of the ISMS?

A. Information security committee

B. Management committee

C. Operational committee

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

What is the next step that Operaze's ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.

A. Implement the information security policy

B. Obtain top management's approval for the information security policy

C. Communicate the information security policy to all employees

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 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*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

“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*

Currently there are no comments in this discussion, be the first to comment!

Question #41

Topic 1

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*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

Which statement is an example of risk retention?

A. An organization has decided to release the software even though some minor bugs have not been fixed yet

B. An organization has implemented a data loss protection software

C. An organization terminates work in the construction site during a severe storm

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Which option below should be addressed in an information security policy?

A. Actions to be performed after an information security incident

B. Legal and regulatory obligations imposed upon the organization

C. The complexity of information security processes and their interactions

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Which approach should organizations use to implement an ISMS based on ISO/IEC 27001?

A. An approach that is suitable for organization’s scope

B. Any approach that enables the ISMS implementation within the 12 month period

C. Only the approach provided by the standard

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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 the scenario above, answer the following question:

How should Colin have handled the situation with Lisa?

A. Extend the duration of the training and awareness session in order to be able to achieve better results

B. Promise Lisa that future training and awareness sessions will be easily understandable

C. Deliver training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

Based on the last paragraph of scenario 6, which principles of an effective communication strategy did Colin NOT follow?

A. Transparency and credibility

B. Credibility and responsiveness

C. Appropriateness and clarity

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #50

Topic 1

What is the difference between training and awareness? Refer to scenario 6.

A. Training helps acquire certain skills, whereas awareness develops certain habits and behaviors

B. Training helps acquire a skill, whereas awareness helps apply it in practice

C. Training helps transfer a message with the intent of informing, whereas awareness helps change the behavior toward the message

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 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 (DMZ) 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

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

According to scenario 7, a demilitarized zone (DMZ) is deployed within InfoSec's network. What type of control has InfoSec implemented in this case?

A. Detective

B. Preventive

C. Corrective

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

Based on scenario 7, what should Anna be aware of when gathering data?

A. The use of the buffer zone that blocks potential attacks coming from malicious websites where data can be collected

B. The type of data that helps prevent future occurrences of information security incidents

C. The collection and preservation of records

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

Kyte, a company that has an online shopping website, has added a Q&A 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: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

What should an organization allocate to ensure the maintenance and improvement of the information security management system?

A. The appropriate transfer to operations

B. Sufficient resources, such as the budget, qualified personnel, and required tools

C. The documented information required by ISO/IEC 27001

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

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

A. Operating system and virtualization

B. Servers and storage

C. Application and data

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

A company decided to use an algorithm that analyzes various attributes of customer behavior, such as browsing patterns and demographics, and groups customers based on their similar characteristics. This way, the company will be able to identify frequent buyers and trend-followers, among others. What type of machine learning is the company using?

A. Decision tree machine learning

B. Supervised machine learning

C. Unsupervised machine learning

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

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 ISO/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: *C*

Soke_Ikay 1 month, 2 weeks ago

A.

This choice directly addresses the root cause of the problem. SunDee's failure to regularly monitor and evaluate its ISMS led to a last-minute rush to prepare for the recertification audit. This sudden surge in workload, particularly in the Production Department, resulted in workforce disruption and decreased stock.

upvoted 1 times

Question #61 *Topic 1*

Based on scenario 8, did the nonconformity report include all the necessary aspects?

A. Yes, the report included all the necessary aspects

B. No, the report must also specify the root cause of the nonconformity

C. No, the report must also specify the audit criteria

Correct Answer: *B*

durolusegun 3 months, 3 weeks ago

The answer is supposed to be c. which is the audit criteria

upvoted 1 times

Question #62 *Topic 1*

How does SunDee's negligence affect the ISMS certificate? Refer to scenario 8.

A. SunDee will renew the ISMS certificate, because it has conducted an internal audit to evaluate the ISMS effectiveness

B. SunDee might not be able to renew the ISMS certificate, because it has not conducted management reviews at planned intervals

C. SunDee might not be able to renew the ISMS certificate, because the internal audit lasted longer than planned

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

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

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

An organization has decided to conduct information security awareness and training sessions on a monthly basis for all employees. Only 45% of employees who attended these sessions were able to pass the exam. What does the percentage represent?

A. Measurement objective

B. Attribute

C. Performance indicator

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

A small organization that is implementing an ISMS based on ISO/IEC 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*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

An organization that has an ISMS in place conducts management reviews at planned intervals, but does not retain documented information on the results. Is this in accordance with the requirements of ISO/IEC 27001?

A. Yes, ISO/IEC 27001 does not require organizations to document the results of management reviews

B. No, ISO/IEC 27001 requires organizations to document the results of management reviews

C. Yes, ISO/IEC 27001 requires organizations to document the results of management reviews only if they are conducted ad hoc

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!