PECB

ISO-IEC-27001-Lead-Implementer

PECB Certified ISO /IEC 27001 : 2022 Lead Implementer exam

Version: 6.2

[Total Questions: 215]

Web: www.marks4sure.com

Email: support@marks4sure.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@marks4sure.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@marks4sure.com and our technical experts will provide support within 24 hours.

Copyright

Question #:1

Based on ISO/IEC 27001, what areas within the organization require establishing rules, procedures, and agreements for information transfer?

A. Internal file-sharing platforms and shared drives

B. Public and private cloud services and partner collaboration platforms

C. All transfer facilities within the organization

Answer: C

Question #:2

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on the scenario above, answer the following question:

Based on scenario 2. which principle of information security was NOT compromised by the attack?

A. Confidentiality

B. integrity

C. Availability

Answer: B

Question #:3

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 9.3.3, the organization must retain documented information as evidence of the results of management reviews. The results of management reviews must include decisions and actions related to the ISMS policy, objectives, risks, opportunities, resources, and communication. Documenting the results of management reviews is important to ensure the accountability, traceability, and effectiveness of the ISMS. It also helps the organization to monitor and measure the performance and improvement of the ISMS, and to demonstrate compliance with the requirements of ISO/IEC 27001:2022. Therefore, an organization that has an ISMS in place and conducts management reviews at planned intervals, but does not retain documented information on the results, is not in accordance with the requirements of ISO /IEC 27001. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 107)

Question #:4

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. did the ISMS project manager complete the corrective action process appropriately?

A. Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions

B. No, the corrective action did not address the root cause of the nonconformity

C. No, the corrective action process should also include the review of the implementation of the selected actions

Answer: C

Explanation

According to ISO/IEC 27001:2022, the corrective action process consists of the following steps12:

- Reacting to the nonconformity and, as applicable, taking action to control and correct it and deal with the consequences
- Evaluating the need for action to eliminate the root cause(s) of the nonconformity, in order that it does not recur or occur elsewhere
- Implementing the action needed
- Reviewing the effectiveness of the corrective action taken
- Making changes to the information security management system, if necessary

In scenario 9, the ISMS project manager did not complete the last step of reviewing the effectiveness of the corrective action taken. This step is important to verify that the corrective action has achieved the intended results and that no adverse effects have been introduced. The review can be done by using various methods, such as audits, tests, inspections, or performance indicators3. Therefore, the ISMS project manager did not complete the corrective action process appropriately.

Question #:5

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

Answer: C

Explanation

According to ISO/IEC 27001:2022, clause 7.5, an organization is required to maintain documented information to support the operation of its processes and to have confidence that the processes are being carried out as planned. This includes documenting the information security policy, the scope ofthe ISMS, the risk assessment and treatment methodology, the statement of applicability, the risk treatment plan, the information security objectives, and the results of monitoring, measurement, analysis, evaluation, internal audit, and management review. However, the standard does not specify the level of detail or the format of the documented information, as long as it is suitable for the organization's needs and context. Therefore, documenting each security control that is implemented by describing their functions in detail is not a violation of the standard, but it may not be the most efficient or effective way to document the ISMS. Documenting each security control separately may make it harder to review, update, and communicate the documented information, and may also create unnecessary duplication or inconsistency. A better approach would be to document the processes and activities that involve the use of security controls, and to reference the relevant controls from Annex A or other sources. This way, the documented information would be more aligned with the process approach and the Plan-Do-Check-Act cycle that the standard promotes.

Question #:6

Which of the following traits is NOT associated with an external audit?

A. It is always conducted in a planned and timely manner

B. It assesses the effectiveness and efficiency of ISMS

C. It has no advisory role within the organization

Answer: C

Question #:7

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

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.

Question #:8

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:

According to scenario 1, which of the following controls implemented by Antiques is a detective and administrative control?

A. Enable the automatic update feature of the new software

B. Review of all user access rights

C. Review of the information security policy

Answer: B

Question #:9

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

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.

Question #:10

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. 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

Answer: B

Explanation

According to ISO/IEC 27001:2022, a nonconformity report is a document that records the details of any deviation from the audit criteria that is identified during an audit2. The audit criteria are the set of policies, procedures, requirements, or specifications that are used as a reference against which audit evidence is compared3. Therefore, a nonconformity report must include the following aspects:

- The description of the nonconformity, which should clearly state what the deviation is, where it occurred, and when it was detected
- The audit findings, which should provide the objective evidence that supports the identification of the nonconformity
- The audit criteria, which should specify the reference document or standard that the nonconformity deviates from
- The recommendations, which should suggest the possible corrective actions or improvements that can be taken to address the nonconformity

In scenario 8, Tessa's nonconformity report included the description of the nonconformity, the audit findings, and the recommendations, but it did not specify the audit criteria. Therefore, the report did not include all the necessary aspects and was incomplete.

Question #:11

Question:

Which of the following would be an acceptable justification for excluding the Annex A 6.1**Screening**control?

A. The organization considers background verification checks unnecessary for its operations

B. A collective agreement with employees prohibits security checks

C. The organization voluntarily performs comprehensive criminal background checks on all employees

Answer: B

Explanation

Annex A Control A.6.1 of ISO/IEC 27001:2022 (and ISO/IEC 27002:2022 Clause 6.1) covers**Screening**:

"Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks."

If**collective agreements**(e.g., labor union agreements) or**local labor laws**prohibit such checks, this is a valid justification for**exclusion**in the Statement of Applicability (SoA), per ISO/IEC 27001:2022 Clause 6.1.3 (d), which allows exclusions when**properly justified**.

Question #:12

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

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

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

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

Answer: C

Explanation

According to the ISO/IEC 27001 : 2022 Lead Implementer course, the steps required by ISO/IEC 27001 that an organization must take when a nonconformity is detected are as follows1:

- React to the nonconformity, take action to control and correct it, and deal with its consequences
- Evaluate the need for action to eliminate the causes of the nonconformity so that it does not recur or occur elsewhere
- Implement any action needed
- Review the effectiveness of the corrective action
- Make changes to the information security management system (ISMS) if necessary

Therefore, communicating the details of the nonconformity to every employee of the organization and suspending the employee that caused the nonconformity is not part of the steps required by ISO/IEC 27001. This option is not only unnecessary, but also potentially harmful, as it could violate the principles of confidentiality, integrity, and availability of information, as well as the human rights and dignity of the employee involved2. Instead, the organization should follow the established procedures for reporting, recording, and analyzing nonconformities, and ensure that the corrective actions are appropriate, proportional, and fair3.

Question #:13

Scenario 9:

OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan 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."

However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.

Did Julia's approach to submitting action plans for addressing nonconformities align with best practices?

A. Yes, as action plan submission can be flexible

B. No, as action plans are typically expected to meet specified deadlines

C. Yes, Julia revised the action plan to ensure alignment with best practices

Answer: B

Question #:14

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives.

Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

Based on scenario 2, which information security requirement was NOT assessed by Beauty?

A. Alignment of the risk assessment with the organization's strategy

B. Compliance with legal, regulatory, and contractual obligations

C. Principles and objectives for the information life cycle

Answer: C

Question #:15

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 anddecided 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

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.

Question #:16

Scenario 1:

HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canada. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.

As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.

When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

However, HealthGenic also uncovered unauthorized changes to user access controls. Consequently, some medical reports were altered, resulting in incomplete and inaccurate medical records. The company swiftly acknowledged and corrected the unintentional changes to user access controls. When analyzing the root cause of these changes, HealthGenic identified a vulnerability related to the segregation of duties within the IT department, which allowed individuals with system administration access also to manage user access controls. Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

In response to the consequences of the service interruptions, the software development company revamped its infrastructure by adopting a scalable architecture hosted on a cloud platform, enabling dynamic resource allocation based on demand. Rigorous load testing and performance optimization were conducted to identify and address potential bottlenecks, ensuring the system could handle increased user loads seamlessly. Additionally, the company promptly assessed the unauthorized access and data alterations.

To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data, HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.

In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.

Which information security principle was impacted by the alteration of medical records?

A. Availability

B. Confidentiality

C. Integrity

Answer: C

Question #:17

An organization uses Platform as a Service (PaaS) to host its cloud-based services. As such, the cloud provider manages the majority of the services provided to the organization. What does the organization still need to manage when using PaaS?

A. Operating system and virtualization

B. Servers and storage

C. Application and data

Answer: C

Question #:18

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.

Question #:19

Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which serves as a structured framework and a guideline that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its 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 a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

Then, they evaluated the risks based on the risk evaluation criteria, where they decided to treat only the risks of the high-risk category. Additionally, they focused primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted.

Based on the scenario above, answer the following question:

Which implementation approach did TradeB initially choose to implement its information security management system (ISMS)?

A. The systematic approach

B. The iterative approach

C. The systems approach

Answer: B

Question #:20

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

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.

Question #:21

An employee from Reyae Ltd. unintentionally sent an email containing critical business strategies to a competitor. Which information security principle was compromised in this case?

A. Integrity

B. Availability

C. Confidentiality

Answer: C

Question #:22

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on the scenario above, answer the following question:

According to scenario 2, Solena decided to issue a press release in which its representatives denied the attack. What does this situation present?

A. Lack of communication strategies

B. Lack of transparency toward their users

C. Lack of availability toward their users

Answer: B

Question #:23

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

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. Thisalso 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 processfor 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 #:24

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

A. Operating system and visualization

B. Servers and storage

C. Application and data

Answer: C

Question #:25

Scenario 7: Incident Response at Texas H&H Inc.

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

According to scenario 7, the team prevented a potential attack based on knowledge gained from previous incidents. Is this acceptable?

A. No, before responding to an information security incident, an information security incident management policy must be established

B. No, every information security incident is different, hence knowledge gained from previous incidents cannot prevent potential attacks

C. Yes, in the absence of an information security incident management policy, lessons learned can be applied

Answer: C

Question #:26

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 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

Answer: C

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, an effective communication strategy should follow some principles, such as transparency, credibility, appropriateness, clarity, responsiveness, and consistency. These principles help to ensure that the communication is relevant, accurate, understandable, timely, and coherent. Based on the last paragraph of scenario 6, it seems that Colin did not follow the principles of appropriateness and clarity. Appropriateness means that the communication should be tailored to the needs, expectations, and level of understanding of the audience. Clarity means that the communication should be simple, concise, and precise, avoiding ambiguity and jargon. However, Colin explained the information security issues in a too technical manner, which made Lisa confused and unable to comprehend the session. Therefore, Colin should have adapted his communication style and content to suit the HR personnel, who may not have the same technical background as him.

Question #:27

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization’s topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and

documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. Theimplementation was based on all relevant agreements, legislation, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Which of the following controls did Socket Inc. implement by conducting pre-employment background checks? Refer to scenario 3.

A. Annex A 6.1 Screening

B. Annex A 6.7 Remote working

C. Annex A 6.4 Disciplinary process

Answer: A

Question #:28

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

Answer: B

Explanation

According to the ISO/IEC 27001:2022 standard, an information security policy is a high-level document that defines the management approach and objectives for information security within the organization. It should include, among other things, the legal and regulatory obligations imposed upon the organization, such as compliance with laws, contracts, agreements, and standards that are relevant to information security. The information security policy should also provide the basis for establishing, implementing, maintaining, and continually improving the information security management system (ISMS).

Question #:29

What is the purpose of an internal audit charter?

A. To outline how the organization benefits from internal audits, especially in achieving its objectives

B. To outline the assessment of collected audit evidence against predefined audit criteria

C. To outline the audit results, considering the audit objectives and all findings

Answer: A

Question #:30

Scenario 10: ProEBank

ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leaverages the city's advanced technological and financial ecosystem To enhance its security posture, ProEBank has implementied an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.

To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.

During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential conflict of interest with one of the auditors, who had previously worked for ProEBank's mein competitor in the banking industry To ensure the integrity of the audit process. ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team

After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.

Three weeks later, the team conducted an on-site visit to the auditee’s location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001. was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected The audit team leader then issued a recommendation for certification.

After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body.

The certification body’s final decision for certification was made by a**committee**that included**one auditor from the audit team**and two other experts.

Question:

Is this acceptable?

A. No – the certification body must ensure that persons that make the decision for certification are different from those who carried out the audit

B. No – the committee should have included only members from the audit team and not other experts that were not part of the audit

C. Yes – the committee must include one member from the audit team and other individuals working for the certification body

Answer: A

Explanation

ISO/IEC 17021-1:2015 Clause 7.2.7 clearly states:

“The personnel making the certification decision shall not have participated in the audit.”

This separation of duties ensures impartiality. Including an**auditor from the same audit team**in the decision-making process is a**violation**of this clause, regardless of intent.

Question #:31

Question:

What action should an organization take to ensure the security of information when it is transferred or treated by an external party?

A. Rely on external parties to implement their own security measures

B. Include security clauses in a contractual agreement with the external party

C. Exclude external parties from the ISMS scope to limit risk exposure

Answer: B

Explanation

ISO/IEC 27002:2022 Clause 5.20 –**Addressing information security within supplier agreements**states:

“Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and products provided by suppliers.”

Further emphasized in Clause 5.19 –**Information security in supplier relationships**, which mandates managing supplier-related risks.

This means**contracts must include clauses**addressing information security expectations, responsibilities, access rights, compliance, audits, and breach response mechanisms.

Question #:32

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:

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

A. (1) Patches. (2) an access control software

B. (1) Intrusions on networks. (?) an intrusion detection system

C. (1) Technical vulnerabilities. (2) network intrusions

Answer: B

Question #:33

Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues

Based on scenario 6. when should Colin deliver the next training and awareness session?

A. After he ensures that the group of employees targeted have satisfied the organization's needs

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

C. After he determines the employees' availability and motivation

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 7.2.3, the organization shall conduct a competence needs analysis to determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization shall also evaluate the effectiveness of the actions taken to acquire the necessary competence and retain appropriate documented information as evidence of competence. Therefore, Colin should deliver the next training and awareness session after he conducts a competence needs analysis and records the competence related issues, such as the level of understanding, the gaps in knowledge, and the feedback from the participants.

Question #:34

Which of the situations below can negatively affect the internal audit process?

A. Restricting the internal auditor's access to offices and documentation

B. Conducting internal audit interviews with all employees of the organization

C. Reporting the internal audit results to the top management

Answer: A

Explanation

According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the factors that can negatively affect the internal audit process is the lack of cooperation from the auditees, which can manifest as restricting the internal auditor’s access to offices and documentation1. This can hinder the auditor’s ability to collect sufficient and appropriate audit evidence, verify the conformity of the information security management system (ISMS) with the audit criteria, and identify any nonconformities or opportunities for improvement2. Therefore, the auditees should be informed of the audit objectives,scope, criteria, and schedule in advance, and should provide the auditor with all the necessary information and resources to conduct the audit effectively3.

Question #:35

Scenario 7: Incident Response at Texas H&H Inc.

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Texas H&H Inc. decided to assign an internal expert for their forensic analysis. Is this acceptable? Refer lo scenario 7.

A. Yes. forensic analysis can be done by cither an internal or external expert

B. Yes. hiring an external expert for forensic analysis Is a requirement of the standard

C. No. the company's forensic analysis should be based on the conclusion of Its cloud storage provide investigation

Answer: A

Question #:36

Scenario 10: ProEBank

ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leaverages the city's advanced technological and financial ecosystem To enhance its security posture, ProEBank has implementied an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.

To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.

During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential conflict of interest with one of the auditors, who had previously worked for ProEBank's mein competitor in the banking industry To ensure the integrity of the audit process. ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team

After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.

Three weeks later, the team conducted an on-site visit to the auditee’s location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001. was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected The audit team leader then issued a recommendation for certification.

After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body.

After the Stage 2 audit, minor nonconformities were found. Despite this, the audit team leader issued a **positive recommendation**for certification.

Question:

Is this acceptable?

A. No – the auditor should have issued an unfavorable recommendation for certification because minor nonconformities were identified

B. Yes – a recommendation for certification should be issued when only minor nonconformities are identified

C. No – the auditor should have issued a recommendation for certification conditional upon the filing of corrective action plans for the minor nonconformities

Answer: B

Explanation

ISO/IEC 17021-1:2015 Clause 9.4.5.2 states:

“A certification recommendation can be made when only minor nonconformities are identified, provided a corrective action plan is submitted and accepted.”

So long as the auditee commits to corrective actions within an agreed time, certification can proceed. Therefore, issuing a positive recommendation is**compliant**, assuming the organization has plans in place for resolution.

Question #:37

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.

Which situation presented in scenario 8 is not in compliance with ISO/IEC 27001 requirements?

A. Emma has an operational role in the HealthGenic's management system

B. The recodification audit Is planned to be conducted two years after HealthGenic implemented the ISMS

C. Emma had access to all offices and documentation of HealthGenic

Answer: A

Question #:38

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.

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

Answer: B

Explanation

Event logs are records of events that occur in a system or network, such as user actions, faults, exceptions, errors, warnings, or security incidents. They can provide valuable information for monitoring, auditing, and troubleshooting purposes. Event logs can be categorized into different types, depending on the source and nature of the events. For example, user activity logs record the actions performed by users, such as login, logout, file access, or command execution. User fault and exception logs record the errors oranomalies that

occur due to user input or behavior, such as invalid data entry, unauthorized access attempts, or system crashes. In scenario 3, Socket Inc. used a syslog server to centralize all logs in one server, which is a good practice for log management. However, to find out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company, Socket Inc. should have reviewed not only the user fault and exception logs, but also the user activity logs. The user activity logs could reveal any suspicious or malicious actions performed by the hackers or the employees, such as creating, modifying, or deleting files, executing commands, or installing software. By reviewing both types of logs, Socket Inc. could have a more complete picture of the incident and its root cause. Reviewing all the logs on the syslog server might not be necessary or feasible, as some logs might be irrelevant or too voluminous to analyze.

Question #:39

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 7.5.1, the organization shall ensure that the documented information required by the ISMS and by this document is controlled to ensure that it is available and suitable for use, where and when it is needed, and that it is adequately protected. This includes ensuring that the documented information is reviewed and approved for suitability and adequacy. The information security procedures are part of the documented information that supports the operation ofthe ISMS processes and the implementation of the information security controls. Therefore, they should be drafted, reviewed, and validated by the information security committee, which is the group of people responsible for overseeing the ISMS and ensuring its alignment with the organization's objectives and strategy. The information security committee should include representatives from different functions and levels of the organization, as well as external experts if needed. The information security committee should also ensure that the information security procedures are communicated to the relevant employees and other interested parties, and that they are periodically reviewed and updated as necessary.

Question #:40

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, the control that enables the organization to manage storage media through their life cycle of use, acquisition, transportation and disposal belongs to the category of physical and environmental security. This category covers the controls that prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. The specific control objective for this control is A.11.2.7 Secure disposal or reuse of equipment1, which states that "equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse."2

Question #:41

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

Answer: C

Explanation

According to the ISO/IEC 27001:2022 standard, the organization should determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization should also ensure that these persons are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming with the ISMS requirements, and the benefits of improved information security performance. The organization should also provide information security awareness, education, and training to all employees and, where relevant, contractors and third-party users, as relevant for their job function. The awareness, education, and training programs should be planned, implemented, and maintained according to the needs of the organization and the results of the risk assessment and risk treatment.

Therefore, Colin should have handled the situation with Lisa by delivering training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company. This would ensure that the content and the language of the sessions are appropriate and understandable for the target audience, and that the sessions are effective and efficient in achieving the desired learning outcomes. By doing so, Colin would also avoid wasting time and resources on delivering sessions that are too technical or too basic for some employees, and that do not address their specific information security challenges and responsibilities.

Question #:42

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body

Based on the scenario above, answer the following question:

Does NetworkFuse fulfill the prerequisites for a certification audit?

A. Yes, because the certification body has been selected

B. Yes, because internal audits and management reviews have been performed

C. Yes, because the ISMS must be operational for at least one year prior to the certification audit

Answer: B

Explanation

According to ISO/IEC 27006:2015, the prerequisites for a certification audit are:

- The ISMS must be operational for a period of time that is sufficient to demonstrate its effectiveness and performance.
- The organization must have conducted at least one internal audit and one management review of the ISMS prior to the certification audit.
- The organization must provide the certification body with access to all the relevant documented information, records, personnel, and facilities related to the ISMS.

In the scenario, NetworkFuse has fulfilled these prerequisites, as it has had an operational ISMS for approximately two years, and it has performed internal audits and management reviews. Therefore, the correct answer is B.

Question #:43

Question:

How should the level of detail in risk identification evolve over time?

A. It should be refined gradually through iterative assessments, increasing the level of detail over time

B. It should be performed in full detail only when significant changes occur in the organization

C. It should focus on highly detailed assessments conducted on an ad-hoc basis rather than broad risk assessments

Answer: A

Explanation

ISO/IEC 27005:2022 (Clause 8.2.1 – Risk Identification Process) and the ISMS Implementation Toolkit emphasize that risk identification is a**cyclical and iterative**process:

“Risk identification should evolve with organizational maturity and environmental change, becoming more detailed and effective through each cycle.”

This aligns with Clause 10.1 of ISO/IEC 27001:2022, which requires continual improvement:

“The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.”

Refining detail over time allows organizations to adjust to new threats and better understand their environment, promoting**resilience and continual improvement**.

Question #:44

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.

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

Answer: B

Explanation

A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, such as the Internet. It is used to host public services that need to be accessible from outside the organization, such as web servers, email servers, or DNS servers. A DMZ provides a layer of protection for the internal network by limiting the exposure of the public services and preventing unauthorized access from the external network. A DMZ is an example of a preventive control, which is a type of control that aims to prevent or deter the occurrence of an information security incident. Preventive controls reduce the likelihood of a threat exploiting a vulnerability and causing harm to the organization’s information assets. Other examples of preventive controls are encryption, authentication, firewalls, antivirus software, and security awareness training.

Question #:45

The purpose of control 7.2 Physical entry of ISO/IEC 27001 is to ensure only authorized access to, the organization's information and other associated assets occur. Which action below does NOT fulfill this purpose?

A. Verifying items of equipment containing storage media

B. Using appropriate entry controls

C. Implementing access points

Answer: A

Question #:46

Scenario 8: BioVitalis

BioVitalis is a biopharmaceutical firm headquartered in California, the US Renowned for its pioneering work in the field of human therapeutics, BioVitalis places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation BioVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit. BioVitalis conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment. Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader

BioVitalis's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow up action plans, which were then approved by top management.

In response to the review outcomes. BioVitalis promptly implemented corrective actions, strengthening its Information security measures Additionally, dashboard tools were Introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities.

Furthermore. BioVitalis embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities

BioVitalis is a biopharma company with an ISMS certified under ISO/IEC 27001. For recertification, itreviewed ISMS performance, created dashboards to monitor KPIs such as incident cost, vulnerability tests, and resolution times.

Question:

What type of dashboards did BioVitalis utilize?

A. Operational

B. Tactical

C. Strategic

Answer: C

Explanation

Strategic dashboards focus on**high-level KPIs**and long-term objectives, as per ISO/IEC 27004:2016 – Monitoring, measurement, analysis, and evaluation.

“Strategic dashboards provide an overview of organizational performance and help top management in decision-making.”

BioVitalis used dashboards that track ISMS effectiveness across key performance indicators (incidents, costs, etc.), aligning with**strategic objectives**and management reviews under Clause 9.3.

Question #:47

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 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

Answer: A

Explanation

According to ISO/IEC 27001:2022, clause 5.1, the top management of an organization is responsible for ensuring the leadership and commitment for the ISMS. However, the top management may delegate some of its responsibilities to an information security committee, which is a group of people who oversee the ISMS and provide guidance and support for its implementation and operation. The information security committee may include representatives from different departments, functions, or levels of the organization, as well as external experts or consultants. The information security committee may have various roles and responsibilities, such as:

- Establishing the information security policy and objectives
- Approving the risk assessment and risk treatment methodology and criteria
- Reviewing and approving the risk assessment and risk treatment results and plans
- Monitoring and evaluating the performance and effectiveness of the ISMS
- Reviewing and approving the internal and external audit plans and reports
- Initiating and approving corrective and preventive actions
- Communicating and promoting the ISMS to all interested parties
- Ensuring the alignment of the ISMS with the strategic direction and objectives of the organization
- Ensuring the availability of resources and competencies for the ISMS
- Ensuring the continual improvement of the ISMS

Therefore, in scenario 5, Operaze should create an information security committee to ensure the smooth running of the ISMS, as this committee would provide the necessary leadership, guidance, and support for the ISMS implementation and operation.

Question #:48

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on 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

Answer: A

Explanation

In the scenario described, Beauty's decision to install new anti-malware software after a security incident is aPreventivecontrol. This type of control is aimed at preventing future security incidents by removing malicious code and protecting against malware infections. The purpose of the new anti-malware software is to proactively protect the company's systems and data from potential threats, thus it falls under the category of preventive measures.

Question #:49

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.

Question #:50

Upon the risk assessment outcomes. Socket Inc. decided to:

• Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

• Require the change of passwords at least once every 60 days

• Keep backup copies of files on IT-provided network drives

• Assign users to a separate network when they have access to cloud storage files storing customers' personal data.

Based on the scenario above, answer the following question:

Which of the following options indicate that Socket Inc. used risk modification to treat risks?

A. Conducting a risk assessment before deciding to use third-party services

B. Requiring the change of passwords at least once every 60 days

C. Storing customers' personal data in a cloud-based storage

Answer: B

Question #:51

Scenario 10: ProEBank

ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leaverages the city's advanced technological and financial ecosystem To enhance its security posture, ProEBank has implementied an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.

To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.

During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential conflict of interest with one of the auditors, who had previously worked for ProEBank's mein competitor in the banking industry To ensure the integrity of the audit process. ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team

After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.

Three weeks later, the team conducted an on-site visit to the auditee’s location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001. was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected The audit team leader then issued a recommendation for certification.

After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body.

To prepare for their ISO/IEC 27001 certification audit, ProEBank trained employees, prepared documentation, and identified key personnel to support the audit. However, they did not conduct a**self-assessment**before the audit.

Question:

Did ProEBank follow all of the best practices while preparing for the certification audit?

A. Yes – the company followed all of the best practices in preparation for the certification audit

B. No – the company should have also conducted a self-assessment to prepare for the audit

C. No – the company should not have informed its employees regarding the upcoming audit

Answer: B

Explanation

While ISO/IEC 27001:2022 doesn't require a formal**self-assessment**, it is a widely recognized**best practice** found in implementation guides, such as ISO/IEC 27003 and the ISMS Implementation Toolkit. A self-assessment or**internal audit simulation**:

"Helps organizations identify gaps, test readiness, and build auditor confidence prior to formal audit stages."

ProEBank took several good steps, but**omitting a self-assessment**leaves a potential gap in preparedness and can delay certification if unexpected issues arise.

Question #:52

Refer to Scenario 4 (FinSecure)

Finsecure is a financial institution based in Finland, providing services to a diverse clientele, encompassing retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, FinSecure has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of experts, FinSecure opted for a methodological framework, which serves as a structured framework that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts conducted a risk assessment, identifying all the supporting assets, which were the most tangible ones. They assessed the potential consequences and likelihood of various risks, determining the level of risks using a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process. These risks were categorized into nonnumerical levels (e g., very low, low. moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

After completing the risk assessment, the experts reviewed a selected number of the security controls from Annex A of ISO/IEC 27001 to determine which ones were applicable to the company's specific context. The decision to implement security controls was justified by the risk assessment results. Based on this review, they drafted the Statement of Applicability (SoA). They focused on treating only the high-risk category particularly addressing unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted

Question:

Did the experts draft the Statement of Applicability (SoA) in accordance with ISO/IEC 27001?

A. Yes – because they reviewed a selected number of the controls from Annex A of ISO/IEC 27001

B. No – because they did not review all of the controls from Annex A of ISO/IEC 27001

C. No – because the SoA should have been drafted just before the risk assessment was finalized

Answer: A

Explanation

ISO/IEC 27001:2022 Clause 6.1.3 (c) states:

"Compare the controls determined in 6.1.3 b) with those in Annex A and verify that**no necessary controls have been omitted**."

Clause 6.1.3 (d) continues:

"Produce a Statement of Applicability that contains the necessary controls, justification for inclusion, whether implemented, and justification for exclusion."

The SoA does**not require selection of all controls**, but rather only those that are applicable based on the context, risk assessment, and needs of the organization. FinSecure's experts complied by**selecting relevant controls**and documenting justifications—thus aligning with the standard.

Question #:53

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.

Question #:54

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

Answer: B

Explanation

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

Question #:55

Scenario 1:

HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canada. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.

As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.

When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

However, HealthGenic also uncovered unauthorized changes to user access controls. Consequently, some medical reports were altered, resulting in incomplete and inaccurate medical records. The company swiftly acknowledged and corrected the unintentional changes to user access controls. When analyzing the root cause of these changes, HealthGenic identified a vulnerability related to the segregation of duties within the IT department, which allowed individuals with system administration access also to manage user access controls. Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

In response to the consequences of the service interruptions, the software development company revamped its infrastructure by adopting a scalable architecture hosted on a cloud platform, enabling dynamic resource allocation based on demand. Rigorous load testing and performance optimization were conducted to identify and address potential bottlenecks, ensuring the system could handle increased user loads seamlessly. Additionally, the company promptly assessed the unauthorized access and data alterations.

To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data, HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.

In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.

Based on scenario 1, has HealthGenic implemented physical access controls?

A. Yes, it included physical access controls in its strategy

B. No, its primary focus has been on digital access controls

C. No, its primary focus has been on legal access controls

Answer: B

Question #:56

A tech company has implemented a security measure to confirm the secure removal or overwriting of sensitive data and licensed software on equipment before disposal or reuse. What type of security control was implemented?

A. Physical control

B. Technological control

C. Organizational control

Answer: B

Question #:57

Question:

What is the purpose of ISO/IEC 27002:2022 Clause 8.28?

A. To ensure all security requirements are addressed during application development

B. To ensure software is written securely to reduce information security vulnerabilities

C. To ensure secure system design principles are followed

Answer: C

Explanation

Clause 8.28 of ISO/IEC 27002:2022 addresses “Secure system architecture and engineering principles,” which includes secure design principles throughout the system lifecycle.

The purpose is:

“To ensure that security is built into systems and processes by following recognized engineering and design principles, minimizing vulnerabilities.”

This clause ensures secure system architecture is embedded early, aligning with secure-by-design practices.

Question #:58

Why is the power/interest matrix used for?

A. Define the information security and physical boundaries

B. identify business requirements

C. Determine and manage interested parties

Answer: C

Question #:59

Scenario 7: Incident Response at Texas H&H Inc.

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was notdesigned tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Based on scenario 7. what else should Texas H&H Inc. do when responding to the incident?

A. Decide to stop using cloud services in order to eliminate the risk of similar incidents happening in the future

B. Record and document the incident which serves as input for future corrective actions

C. Communicate the updated Information security policy only to the top management of the company

Answer: B

Question #:60

Question:

During a security audit, analysts discover that an attacker repeatedly queried a black-box ML model to infer if specific data points were in the training set. The attacker could determine if an individual's data was used during training. What threat does this attack represent?

A. Backdoor in the training set

B. Data poisoning

C. Membership inference attack

Answer: C

Explanation

ISO/IEC 23894:2023 (Artificial Intelligence Risk Management) and NIST SP 800-207A define**Membership Inference Attacks (MIA)**as:

"An adversary attempts to determine whether specific data was used in the training phase of a machine learning model."

This is a**privacy threat**and can lead to**data breaches**, especially with personally identifiable information (PII). It differs from**data poisoning**, which manipulates the training process, and**backdoors**, which alter behavior intentionally.

Question #:61

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body

According to scenario 10, NetworkFuse requested from the certification body to review all the documentation only on-site. Is this acceptable?

A. Yes, the auditee may request that the review of the documentation takes place on-site

B. Yes, only if a confidentiality agreement is formerly signed by the audit team

C. No, the certification body decides whether the documentation review takes place on-site or off-site

Answer: A

Explanation

According to the ISO/IEC 27001:2022 standard, the certification body is responsible for planning and conducting the audit, including the review of the documented information. The certification body may decide to review the documentation on-site or off-site, depending on the audit objectives, scope, criteria, and risks. The auditee may not impose any restrictions on the access to the documentation, unless there are valid reasons for confidentiality or security. However, such restrictions should be agreed upon before the audit and should not compromise the effectiveness and impartiality of the audit.

Question #:62

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company identified issues in its IT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, OperazelT implemented an information security managementsystem (ISMS) based on ISO/IEC 27001.

In a collaborative effort involving the implementation team, OperazelT thoroughly assessed its business requirements and internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties to establish the preliminary scope of the ISMS. Following this, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to in clause 4.1, the requirements in clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting OperazelT’s commitment to information security.

OperazelT's information security team created a comprehensive information security policy that aligned with the company's strategic direction and legal requirements, informed by risk assessment findings and business strategies. This policy, alongside specific policies detailing security issues and assigning roles and responsibilities, was communicated internally and shared with external parties. The drafting, review, and approval of these policies involved active participation from top management, ensuring a robust framework for safeguarding information across all interested parties.

As OperazelT moved forward, the company entered the policy implementation phase, with a detailed plan encompassing security definition, role assignments, and training sessions. Lastly, the policy monitoring and maintenance phase was conducted, where monitoring mechanisms were established to ensure the company's information security policy is enforced and all employees comply with its requirements.

To further strengthen its information security framework, OperazelT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazelT decided to involve the services of external consultants to assess the state of its ISMS. The company

collaborated with external consultants, which brought a fresh perspective and valuable insights to the gap analysis process, enabling OperazelT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazelT created a committee whose mission includes ensuring the proper operation of the ISMS, overseeing the company's risk assessment process, managing information security-related issues, recommending solutions to nonconformities, and monitoring the implementation of corrections and corrective actions.

Based on the scenario above, answer the following question:

Was there any issue with how OperazelT determined its current ISMS state?

A. Yes, as the ISMS state must be determined by the implementation team

B. Yes, as it is the top management’s responsibility to determine the ISMS state

C. No, as the ISMS state can be determined by outsourced external consultants

Answer: C

Question #:63

Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts 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 implement 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 a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.

On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for 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.

As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.

Furthermore, while implementing the communication plan for information security, InfoSec’s top management was responsible for creating a roadmap for new product development. This approach helps the

company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.

InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Based on this scenario, answer the following question:

Does InfoSec adhere to the requirements of ISO/IEC 27001 when conducting information security risk assessments?

A. Yes, it adhered to ISO/IEC 27001 requirements

B. No, as it should perform them at planned intervals as well

C. No, as it should perform them twice a year, regardless of significant changes

Answer: B

Question #:64

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

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

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

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

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

Answer: C

Explanation

An intrusion detection system (IDS) is a device or software application that monitors network activities, looking for malicious behaviors or policy violations, and reports their findings to a management station. An IDS can help an organization to detect intrusions on networks, which are unauthorized attempts to access, manipulate, or harm network resources or data. In the scenario, Beauty should have implemented an IDS to detect intrusions on networks, such as the one that exposed customers' information due to the out-of-date anti-malware software. An IDS could have alerted the IT team about thesuspicious network activity and helped them to respond faster and more effectively. Therefore, the correct answer is C.

Question #:65

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affectingthe ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the

progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Did SunDee define the roles for measurement activities correctly?

A. Yes, the information owner can also be responsible for conducting measurement activities

B. No, as the information owner cannot perform different measurement-related roles and responsibilities

C. No, as the responsibility for conducting measurement activities should have been assigned to the information communicator

Answer: A

Question #:66

Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swiftimplementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which serves as a structured framework and a guideline that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its 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 a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

Then, they evaluated the risks based on the risk evaluation criteria, where they decided to treat only the risks of the high-risk category. Additionally, they focused primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted.

Based on the scenario above, answer the following question:

According to scenario 4, what type of assets were identified during the risk assessment?

A. Supporting assets

B. Financial assets

C. Business assets

Answer: A

Question #:67

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

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

Answer: B

Explanation

Managerial controls are administrative actions that are designed to prevent or reduce the likelihood of security incidents by influencing human behavior. They include policies, procedures, guidelines, standards, training, and awareness programs. In scenario 2, Beauty has implemented a managerial control by conducting information security awareness sessions for the IT team and other employees that have access to confidential information. These sessions aim to educate the staff on the importance of system and network security, the potential threats and vulnerabilities, and the best practices to follow to avoid the occurrence of incidents. By raising the level of awareness andknowledge of the employees, Beauty can reduce the human errors and negligence that might compromise the security of the information assets.

Question #:68

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Texas M&H Inc. decided to integrate the incident management policy to the existent information security policy. How do you define this situation?

A. Acceptable, the incident management policy may be integrated into the overall information security policy of the organization

B. Acceptable, but only if the incident management policy addresses environmental, or health and safety issues

C. Unacceptable, the incident management policy should be drafted as a separate document in order to be clear and effective

Answer: A

Question #:69

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

A. Availability

B. Confidentiality

C. Integrity

Answer: C

Explanation

According to ISO/IEC 27001:2022, information security controls are measures that are implemented to protect the confidentiality, integrity, and availability of information assets1. Controls can be preventive, detective, or corrective, depending on their purpose and nature2. Preventive controls aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Detective controls aim to detect or discover the occurrence of a security incident or its symptoms. Corrective controls aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact2.

In this scenario, Socket Inc. implemented several security controls to prevent information security incidents from recurring, such as:

- Segregation of networks: This is a preventive and technical control that involves separating different parts of a network into smaller segments, using devices such as routers, firewalls, or VPNs, to limit the access and communication between them3. This can enhance the security and performance of the network, as well as reduce the administrative efforts and costs3.
- Privileged access rights: This is a preventive and administrative control that involves granting access to information assets or systems only to authorized personnel who have a legitimate need to access them, based on their roles and responsibilities4. This can reduce the risk of unauthorized access, misuse, or modification of information assets or systems4.
- Cryptographic controls: This is a preventive and technical control that involves the use of cryptography, which is the science of protecting information by transforming it into an unreadable format, to protect the confidentiality, integrity, and authenticity of information assets or systems. This can prevent unauthorized access, modification, or disclosure of information assets or systems.
- Information security threat management: This is a preventive and administrative control that involves the identification, analysis, and response to information security threats, which are any incidents that could negatively affect the confidentiality, integrity, or availability of information assets or systems. This can help the organization to anticipate, prevent, or mitigate the impact of information security threats.
- Information security integration into project management: This is a preventive and administrative control that involves the incorporation of information security requirements and controls into the planning, execution, and closure of projects, which are temporary endeavors undertaken to create a unique product, service, or result. This can ensure that information security risks and opportunities are identified and addressed throughout the project life cycle.

However, information backup is not a preventive control, but a corrective control. Information backup is a corrective and technical control that involves the creation and maintenance of copies of information assets or systems, using dedicated software and utilities, to ensure that they can be recovered in case of data loss, corruption, accidental deletion, or cyber incidents. This can help the organization to restore the normal state of

information assets or systems after a security incident or mitigate its impact. Therefore,information backup does not prevent information security incidents from recurring, but rather helps the organization to recover from them.

Question #:70

Scenario 6: Skyver manufactures electronic products, such as 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 ISO/IEC 27001.

Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware. and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well informed by security principles and practices.

One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained the existing Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues In a supportive manner, Colin suggested Lisa to consider attending the session again.

Skyver has been exploring the implementation of Al solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize Al technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver's commitment to improving the customer experience through data-driven insights.

Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.

According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.

Based on the scenario above, answer the following question:

How should Colin have handled the situation with Lisa?

A. Assign an individual the responsibility to provide Lisa with personalized explanations for her technical issues

B. Organize separate technical training sessions exclusively for Lisa

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

Answer: C

Question #:71

Scenario:

Evergreen tailored the format and naming convention of their information security policy to align with their internal structure and needs.

Question:

Is this acceptable?

A. No – the policy must adhere to the predefined template set by ISO/IEC 27001

B. Yes – the organization can determine the formats and names of these policy documents that meet the organization's needs

C. No – the policy format and naming conventions must be approved by an external auditor before being implemented

Answer: B

Explanation

ISO/IEC 27002:2022 Clause 5.1 (Policies for information security) states:

"The organization can determine the**formats and names**of these policy documents that meet the organization' s needs. In some organizations, the information security policy and topic-specific policies can be in a single document."

There is no requirement to use a universal or predefined template. What's important is that the policies are documented, communicated, approved by top management, and support the ISMS objectives.

Question #:72

According to ISO/IEC 27001 controls, when planning audit tests and assurance activities involving operational systems, who should be involved in the agreement process except the tester?

A. The top management

B. The appropriate management

C. The board of directors

Answer: B

Question #:73

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 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

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 8.2.3, the organization shall establish and maintain an incident response process that includes the following activities:

- a) planning and preparing for incident response, including defining roles and responsibilities, establishing communication channels, and providing training and awareness;
- b) detecting and reporting information security events and weaknesses;
- c) assessing and deciding on information security incidents;
- d) responding to information security incidents according to predefined procedures;

- e) learning from information security incidents, including identifying root causes, taking corrective actions, and improving the incident response process;

- f) collecting evidence, where applicable.

The standard does not specify whether the incident response process should be performed internally or externally, as long as the organization ensures that the process is effective and meets the information security objectives. Therefore, the organization may decide to use external consultants for forensic investigation, as long as they comply with the organization's policies and procedures, and protect the confidentiality, integrity, and availability of the information involved.

Question #:74

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked withconducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Based on scenario 8, which of the following performance indicators was NOT established by SunDee?

A. Information security cases

B. Training

C. ISMS weaknesses

Answer: B

Question #:75

Scenario 10: ProEBank

ProEBank, an Austrian financial institution, implemented an ISMS and prepared for ISO/IEC 27001 certification. During planning, the company identified a**conflict of interest**with one auditor, who had previously worked with their main competitor. ProEBank**refused to undergo the audit**until a new audit team was assigned. The certification body acknowledged the issue and replaced the team.

ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leaverages the city's advanced technological and financial ecosystem To enhance its security posture, ProEBank has implementied an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.

To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.

During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential conflict of interest with one of the auditors, who had previously worked for ProEBank's mein competitor in the banking industry To ensure the integrity of the audit process. ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team

After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.

Three weeks later, the team conducted an on-site visit to the auditee’s location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001. was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected The audit team leader then issued a recommendation for certification.

After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body.

Question:

Is ProEBank's decision to require a new audit team due to a perceived conflict of interest acceptable?

A. No – they should have requested only the replacement of the auditor

B. No – the auditee does not have the right to reject the auditors selected by the certification body

C. Yes – the auditee is allowed to refuse to undergo the audit until a new audit team is established

Answer: C

Explanation

According to ISO/IEC 17021-1:2015 Clause 9.1.3 and ISO/IEC 27006:2015 Clause 7.1.2:

“The certification body shall ensure the objectivity and impartiality of the audit team... The auditee has the right to raise concerns over any conflict of interest.”

ProEBank acted within its rights to maintain audit integrity. Requesting an entirely new team—especially when trust is compromised—is acceptable. This ensures**independence and impartiality**, which are core to a valid certification process.

Question #:76

Which of the following represents an example of The Open Security Architecture (TOGAF) framework?

A. Classifying techniques that ensure the integrity of software

B. Choosing specific security architecture requirements

C. Defining components for security architecture

Answer: C

Question #:77

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company identified issues in its IT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, OperazelT implemented an information security management system (ISMS) based on ISO/IEC 27001.

In a collaborative effort involving the implementation team, OperazelT thoroughly assessed its business requirements and internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties to establish the preliminary scope of the ISMS. Following this, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to

in clause 4.1, the requirements in clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting OperazelT's commitment to information security.

OperazelT's information security team created a comprehensive information security policy that aligned with the company's strategic direction and legal requirements, informed by risk assessment findings and business strategies. This policy, alongside specific policies detailing security issues and assigning roles and responsibilities, was communicated internally and shared with external parties. The drafting, review, and approval of these policies involved active participation from top management, ensuring a robust framework for safeguarding information across all interested parties.

As OperazelT moved forward, the company entered the policy implementation phase, with a detailed plan encompassing security definition, role assignments, and training sessions. Lastly, the policy monitoring and maintenance phase was conducted, where monitoring mechanisms were established to ensure the company's information security policy is enforced and all employees comply with its requirements.

To further strengthen its information security framework, OperazelT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazelT decided to involve the services of external consultants to assess the state of its ISMS. The company collaborated with external consultants, which brought a fresh perspective and valuable insights to the gap analysis process, enabling OperazelT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazelT created a committee whose mission includes ensuring the proper operation of the ISMS, overseeing the company's risk assessment process, managing information security-related issues, recommending solutions to nonconformities, and monitoring the implementation of corrections and corrective actions.

Based on the scenario above, answer the following question:

Which phase of information security policy development at OperazelT did NOT encompass all the necessary components?

A. Risk assessment

B. Policy construction

C. Policy implementation

Answer: B

Question #:78

In the SABSA framework, which layer is concerned with viewing the services at a high level?

A. Physical security architecture

B. Logical security architecture

C. Component security architecture

Answer: B

Question #:79

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on scenario 2, 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

Answer: B

Explanation

Confidentiality is one of the three information security principles, along with integrity and availability, that form the CIA triad. Confidentiality means protecting information from unauthorized access or disclosure, and

ensuring that only those who are authorized to view or use it can do so. Confidentiality is essential for preserving the privacy and trust of the information owners, such as customers, employees, or business partners.

The IT team of Beauty is aiming to ensure confidentiality by establishing a user authentication process that requires user identification and password when accessing sensitive information. User authentication is a security control that verifies the identity and credentials of the users who attempt to access a system or network, and grants or denies them access based on their authorization level. User authentication helps to prevent unauthorized users, such as hackers, competitors, or malicious insiders, from accessing confidential information that they are not supposed to see or use. User authentication also helps to create an audit trail that records who accessed what information and when, which can be useful for accountability and compliance purposes.

Question #:80

Who is responsible for ensuring that the information security management system (ISMS) achieves its intended outcome(s)?

A. The organization's IT department

B. The top management of the organization

C. The ISMS project manager

Answer: B

Question #:81

Scenario 1:

HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canada. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.

As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.

When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

However, HealthGenic also uncovered unauthorized changes to user access controls. Consequently, some medical reports were altered, resulting in incomplete and inaccurate medical records. The company swiftly acknowledged and corrected the unintentional changes to user access controls. When analyzing the root cause

of these changes, HealthGenic identified a vulnerability related to the segregation of duties within the IT department, which allowed individuals with system administration access also to manage user access controls. Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

In response to the consequences of the service interruptions, the software development company revamped its infrastructure by adopting a scalable architecture hosted on a cloud platform, enabling dynamic resource allocation based on demand. Rigorous load testing and performance optimization were conducted to identify and address potential bottlenecks, ensuring the system could handle increased user loads seamlessly. Additionally, the company promptly assessed the unauthorized access and data alterations.

To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data, HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.

In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.

According to scenario 1, what is the possible threat associated with the vulnerability discovered by HealthGenic when analyzing the root cause of unauthorized changes?

A. Theft

B. Lawsuit

C. Fraud

Answer: C

Question #:82

Scenario 6: GreenWave

GreenWave, a manufacturer of sustainable and energy efficient home appliances, specializes in solar-powered devices, EV chargers, and smart thermostats. To ensure the protection of customer data and internal operations against digital threats, the company has implemented an ISO/IEC 27001-based information security management system (ISMS). GreenWave is also exploring innovative loT solutions to further improve energy efficiency in buildings

GreenWave is committed to maintaining a high standard of information security within its operations As part of its continuous improvement approach, the company is in the process of determining the competence levels required to manage its ISMS. GreenWave considered various factors when defining these competence requirements, including technological advancements, regulatory requirements, the company's mission, strategic objectives, available resources, as well as the needs and expecations of its customers

Furthermore, the company remained committed to complying with ISO/IEC 27001's communication requirements. It established clear guidelines for internal and external communication related to the ISMS,

defining what information to share, when to share it. with whom, and through which channels. However, not all communications were formally documented; instead, the company classified and managed communication based on its needs, ensuring that documentation was maintained only to the extent necessary for the ISMS effectiveness .

GreenWave has been exploring the implementation of Al solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize Al technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with GreenWave's commitment to improving the customer experience through data-driven insights.

Additionally, GreenWave looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for GreenWave's electronic product development

According to GreenWave, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. GreenWave assigned Colin the responsibility of determining the materiality of this change within the company.

Question:

Is GreenWave’s approach to documenting communication acceptable?

A. No – as ISO/IEC 27001 requires all ISMS-related communication to be formally documented

B. No – as ISO/IEC 27001 provides a predefined structure for all ISMS communication

C. Yes – as the organization can determine the extent and format of documented communication based on what is necessary for the effectiveness of its ISMS

Answer: C

Explanation

ISO/IEC 27001:2022 Clause 7.4 –**Communication**states:

“The organization shall determine the need for internal and external communications... including:

(a) what to communicate;

(b) when to communicate;

(c) with whom to communicate;

(d) how to communicate.”

There is**no mandate that all communication must be documented**. The organization has the freedom to decide what is documented, based on necessity for the**effectiveness of the ISMS**(as also supported by Clause 7.5 – Documented Information).

Question #:83

An organization has established a policy that provides the personnel with the information required to effectively deploy encryption solutions in order to protect organizational confidential data. What type of policy is this?

A. High-level general policy

B. High-level topic-specific policy

C. Topic-specific policy

Answer: C

Question #:84

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, information security risk can be accepted as one of the four possible options for risk treatment, along with avoiding, modifying, or sharing the risk12. Risk acceptance means that the organization decides to tolerate the level of risk without taking any further action to reduce it3. Risk acceptance can be done before, during, or after the risk treatment process, depending on the organization's risk criteria and the residual risk level4.

Question #:85

Levo Corporation has implemented a demilitarized zone (DMZ) and virtual private network (VPN) to secure its network. What controls did Levo Corporation implement in this case?

A. Preventive controls

B. Detective controls

C. Corrective controls

Answer: A

Question #:86

Scenario 7: CyTekShield

CyTekShield based in Dublin. Ireland, is a cybersecurity consulting provider specializing in digital risk management and enterprise security solutions. After facing multiple security incidents. CyberTekShield formed expanded its information security team by bringing in Sadie and Niamh as part of the team. This team is structured into three key divisions: incident response, security architecture and forensics

Sadie will separate the demilitarized zone from CyTekShield's private network and publicly accessible resources, as part of implementing a screened subnet network architecture. In addition, Sadie will carry out comprehensive evaluations of any unexpected incidents, analyzing their causes and assessing their potential impact. She also developed security strategies and policies. Whereas Niamh. a specialized expert in forensic investigations, will be responsible for creating records of different data for evidence purposes To do this effectively, she first reviewed the company's information security incident management policy, which outlines the types of records to be created, their storage location, and the required format and content for specific record types.

To support the process of handling of evidence related to information security events. CyTekShield has established internal procedures. These procedures ensure that evidence is properly identified, collected, and preserved within the company CyTekShield's procedures specify how to handle records in various storage mediums, ensuring that all evidence is safeguarded in its original state, whether the devices are powered on or off.

As part of CyTekShield's initiative to strengthen information security measures, Niamh will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments Upon completion of the risk assessment process, Niamh is responsible to develop and implement a plan for treating information security risks and document the risk treatment results.

Furthermore, while implementing the communication plan for information security, the CyTekShield's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Niamh, the forensics expert, conducted information security risk assessments upon significant changes and developed a**risk treatment plan**. The results of both were**documented**.

Question:

Does CyTekShield comply with ISO/IEC 27001 requirements regarding the information security risk treatment plan?

A. Yes – by implementing a risk treatment plan and documenting risk treatment results

B. No – it should only retain documented information for risk assessment results

C. No – the information security risk treatment plan should be developed only by the top management

Answer: A

Explanation

ISO/IEC 27001:2022 Clause 6.1.3 (e) requires organizations to:

“Formulate an information security risk treatment plan and obtain risk owners’ approval...

The organization shall retain documented information about the information security risk treatment process.”

Niamh’s role aligns with ISO expectations. There is**no restriction**that only top management must develop this plan, as long as risk owners approve it (6.1.3(f)). Documentation of**both assessment and treatment**is required.

Question #:87

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 scenario 5. in which category of the interested parties does the MR 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

Answer: B

Explanation

According to ISO/IEC 27001, interested parties are those who can affect, be affected by, or perceive themselves to be affected by the organization's information security activities, products, or services. Interested parties can be classified into four categories based on their influence and interest in the ISMS:

- Positively influenced interested parties: those who benefit from the ISMS and support its implementation and operation
- Negatively influenced interested parties: those who are adversely affected by the ISMS and oppose its implementation and operation
- High-interest interested parties: those who have a strong interest in the ISMS and its outcomes, regardless of their influence
- Low-interest interested parties: those who have a weak interest in the ISMS and its outcomes, regardless of their influence

In scenario 5, the HR manager of Operaze belongs to the category of negatively influenced interested parties, because he/she perceives that the ISMS will create more paperwork and documentation for the HR Department, and therefore opposes its implementation and operation. The HR manager does not benefit from the ISMS and does not support its objectives and requirements.

Question #:88

Scenario 6: GreenWave

GreenWave, a manufacturer of sustainable and energy efficient home appliances, specializes in solar-powered devices, EV chargers, and smart thermostats. To ensure the protection of customer data and internal operations against digital threats, the company has implemented an ISO/IEC 27001-basedinformation security management system (ISMS). GreenWave is also exploring innovative loT solutions to further improve energy efficiency in buildings

GreenWave is committed to maintaining a high standard of information security within its operations As part of its continuous improvement approach, the company is in the process of determining the competence levels required to manage its ISMS. GreenWave considered various factors when defining these competence requirements, including technological advancements, regulatory requirements, the company's mission, strategic objectives, available resources, as well as the needs and expecations of its customers

Furthermore, the company remained committed to complying with ISO/IEC 27001's communication requirements. It established clear guidelines for internal and external communication related to the ISMS, defining what information to share, when to share it. with whom, and through which channels. However, not all communications were formally documented; instead, the company classified and managed communication based on its needs, ensuring that documentation was maintained only to the extent necessary for the ISMS effectiveness .

GreenWave has been exploring the implementation of Al solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize Al technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with GreenWave's commitment to improving the customer experience through data-driven insights.

Additionally, GreenWave looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for GreenWave's electronic product development

According to GreenWave, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. GreenWave assigned Colin the responsibility of determining the materiality of this change within the company.

Question:

Did GreenWave appropriately determine the competence levels required to support their ISMS?

A. Yes – because GreenWave considered only the internal factors, which are the most important for its operations

B. No – because GreenWave did not consider external issues, which are relevant to the ISMS

C. Yes – because GreenWave considered external issues, internal factors, and needs and expectations of relevant interested parties

Answer: C

Explanation

ISO/IEC 27001:2022 Clause 7.2 –**Competence**states:

“The organization shall determine the necessary competence of persons... considering**internal and external issues**, and the needs and expectations of interested parties relevant to the ISMS.”

GreenWave followed this clause by factoring in both internal and external influences, including regulatory and customer requirements. This comprehensive view ensures that assigned personnel are adequately equipped to manage ISMS functions.

Question #:89

Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts 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 implement 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 a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.

On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for 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.

As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.

Furthermore, while implementing the communication plan for information security, InfoSec's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.

InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Based on this scenario, answer the following question:

Does InfoSec comply with ISO/IEC 27001 requirements regarding the information security risk treatment plan?

A. Yes, it complies with ISO/IEC 27001 requirements by implementing a risk treatment plan and documenting risk treatment results

B. No, it should only retain documented information for risk assessment results

C. No, the information security risk treatment plan should be developed only by the top management

Answer: A

Question #:90

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body

NetworkFuse should_____to ensure that employees are prepared for the audit. Refer to scenario 10.

A. Conduct practice interviews

B. Observe the technologies used

C. Select a certification body that provides combined audits

Answer: A

Explanation

One of the ways to prepare employees for an ISO/IEC 27001 audit is to conduct practice interviews with them. This can help them to familiarize themselves with the audit process, the types of questions they might be asked, and the evidence they need to provide to demonstrate compliance with the standard. Practice interviews can also help employees to identify any gaps or weaknesses in their knowledge or performance, and to address them before the actual audit. Practice interviews can be conducted by internal auditors, managers, or consultants, and should cover the relevant scope, objectives, and criteria of the audit. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113)

Question #:91

TradeB communicated the information security processes and procedures to employees. Which principle of efficient communication strategy did they use?

A. Transparency

B. Appropriateness

C. Responsiveness

Answer: A

Question #:92

Question:

Whom should an organization interview to obtain information regarding information security risks in their respective fields?

A. Experts who are directly responsible for information security only

B. Employees involved in information security activities and tasks only

C. All interested parties' members, whether they are experts or not

Answer: C

Explanation

ISO/IEC 27001:2022 Clause 4.2 –**Understanding the needs and expectations of interested parties**states:

"The organization shall determine:

a) interested parties that are relevant to the ISMS;

b) the relevant requirements of these interested parties."

Risk identification must incorporate input from**all relevant stakeholders**, including but not limited to experts. In fact,**ISO/IEC 27005:2022**emphasizes**stakeholder engagement**in risk assessments to improve understanding of risk context and ensure comprehensive input.

Question #:93

A tech company rapidly expanded its operations over the past few years. Its information system, consisting of servers, databases, and communication tools, is a critical part of its daily operations. However, due to the rapid growth and increased data flow, the company is now facing a saturation of its information system. This saturation has led to slower response times, increased downtime, and difficulty in managing the overwhelming volume of data. In which category does this threat fall into?

A. Infrastructure failures

B. Technical failures

C. Compromise of functions

Answer: A

Question #:94

Invalid Electric, a manufacturer of electrical components, is preparing for its upcoming ISO 27001 certification audit. This is the first time the company has undergone such an audit, and many of itsemployees are not familiar with the process. The management team is concerned that employees may not be adequately prepared for interviews and the scrutiny of documentation during the audit.

To ensure that employees are ready for the audit, the management team is considering several options to help them understand what to expect and how to handle the auditor's questions confidently.

Based on scenario 10. did invalid Electric provide a valid reason for requesting the replacement of the audit learn leader?

A. No, because Issuing a recommendation for certification lo a main competitor is not a conflict of interest situation

B. No, because the auditee can request the replacement of an auditor only if the auditor has worked for the auditee

C. Yes, because the auditee can request to replace an auditor that has worked for one of its major competitors

Answer: C

Question #:95

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 way1. 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 affect1. 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.

Question #:96

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 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.

Question #:97

Question:

Who is responsible for ensuring that the ISMS achieves its intended outcomes?

A. IT Department

B. Top management

C. ISMS project manager

Answer: B

Explanation

According to ISO/IEC 27001:2022 Clause 5.1 –**Leadership and Commitment**:

"Top management shall demonstrate leadership and commitment with respect to the information security management system by:

e) ensuring that the ISMS achieves its intended outcomes."

Top management must not only provide resources but also**integrate ISMS into organizational processes**, promote awareness, and support roles like the ISMS manager. While the**ISMS project manager**supports implementation,**top management bears ultimate accountability**.

Question #:98

Scenario:

Jane is a developer deploying an application using a language supported by her cloud provider. Shedoesn't manage the underlying infrastructure but needs control over the application and its environment.

Question:

Which cloud service model does Jane need?

A. Infrastructure as a Service

B. Platform as a Service

C. Software as a Service

Answer: B

Explanation

ISO/IEC 17788:2014 (Cloud Computing Overview and Vocabulary) defines:

- **Platform as a Service (PaaS):**

"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications... The consumer does not manage or control the underlying infrastructure."

Jane's requirements precisely match the**PaaS model**, where she controls the app and environment (runtime, storage) but not the infrastructure (servers, OS).

Question #:99

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

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

Answer: A

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, residual risk is the risk remaining after risk treatment. Residual risk should be compared with the acceptable level of risk, which is the level of risk that the organization is willing to tolerate. If the residual risk is below the acceptable level of risk, then the risk can be accepted. If the residual risk is above the acceptable level of risk, then additional risk treatment options should be considered. Therefore, TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment, which is the difference between the initial risk and the residual risk. This will help TradeB to determine whether the risk treatment was effective and whether the residual risk is acceptable or not.

Question #:100

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

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.

Question #:101

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

Answer: B

Explanation

Confidentiality of information is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. In other words, confidentiality ensures that only those who are authorized to access the information can do so. In the scenario, the confidentiality of information was compromised when the software company modified some files that contained sensitive information related to HealthGenic's patients. This modification resulted in the invasion of patients' privacy, which means that their personal and medical information was exposed to unauthorized parties. Therefore, the correct answer is B.

Question #:102

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body

Based on scenario 10. NetworkFuse did not conduct a self-evaluation of the ISMS before the audit. Is this compliant to ISO/IEC 27001?

A. No, the auditee must review the requirements of clauses 4 to 10 before the conduct of a certification audit

B. Yes, the standard indicates that the auditee shall rely only on internal audit and management review reports to prepare for the certification audit

C. Yes, the standard does not require to conduct a self-evaluation before the audit but it is a good practice to follow

Answer: C

Explanation

According to the ISO/IEC 27001:2022 standard, the organization is responsible for establishing, implementing, maintaining and continually improving the information security management system (ISMS) in accordance with the requirements of the standard (section 4.1). The standard does not explicitly require the organization to conduct a self-evaluation of the ISMS before the certification audit, which is an external audit performed by an independent certification body to verify the conformity of the ISMS with the standard and to grant the certification (section 9.3.2). However, the standard does require the organization to conduct internal audits (section 9.2) and management reviews (section 9.3) of the ISMS at planned intervals to ensure its

effectiveness, suitability and adequacy, and to identify opportunities for improvement and corrective actions. Therefore, conducting a self-evaluation of the ISMS before the certification audit is a good practice to follow, as it can help the organization to prepare for the audit, to identify any gaps or nonconformities, and to demonstrate its commitment and readiness for the certification.

Question #:103

Scenario 9: CoreBit Systems

CoreBit Systems, with its headquarters m San Francisco, specializes in information and communication technology (ICT) solutions, its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients a smooth transition into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently. John, the internal auditor of CoreBit Systems, conducted an internal audit which uncovered nonconformities related to their monitoring procedures and system vulnerabilities, in response to the identified nonconformities. CoreBit Systems decided to employ a comprehensive problem-solving approach to solve these issues systematically. The method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of issues. This approach involves several steps. First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root cause of the nonconformities, CoreBit Systems's ISMS project manager. Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective action for addressing a nonconformity, Julia identified the issue as significant and assessed a high likelihood of its reoccurrence Consequently, she chose to implement temporary corrective actions. Afterward. Julia combined all the nonconformities Into a single action plan and sought approval from the top management.

The submitted action plan 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.

However. Julia's submitted action plan was not approved by top management The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process, and notably, the revised action plans lacked a defined schedule for execution.

Julia, the ISMS project manager, developed a combined action plan for all nonconformities. However, it was rejected, revised, and resubmitted late—without defined execution schedules.

Question:

Did CoreBit Systems have a plan in place to implement permanent corrective action to address the identified nonconformities?

A. Yes – CoreBit Systems had a comprehensive plan in place to implement permanent corrective actions

B. No – CoreBit Systems did not have a clear plan to implement a permanent corrective action

C. No – CoreBit Systems decided not to pursue this course of action

Answer: B

Explanation

ISO/IEC 27001:2022 Clause 10.2 –**Nonconformity and corrective action**requires:

“Corrective actions shall be implemented without undue delay and include:

— evaluating the need for action to eliminate the cause;

— implementing the necessary actions;

— reviewing the effectiveness;

— updating risks and SoA if needed.”

Although Julia drafted an action plan, it was not approved initially, was**resubmitted late**, and**lacked scheduling**—failing to meet key requirements of a “clear and actionable plan.”

Question #:104

Question:

Which of the following statements best represents The Open Security Architecture (OSA) framework?

A. A framework that explains the functionality and technical controls of security, presenting a holistic view of crucial security concerns

B. A framework that assists organizations in determining the objectives of developing their security architecture, focusing on the initial stages of security architecture

C. A framework that helps organize enterprise architecture artifacts, including documents, specifications, and models, by considering the impact of these artifacts on various stakeholders

Answer: A

Explanation

The Open Security Architecture (OSA) provides free, vendor-neutral security architecture patterns and guidance for implementing security controls. It is intended to:

“Present a holistic view of essential security components and technical measures to assist organizations in securing their IT environments.”

This aligns best with Option A, as it reflects the comprehensive and practical nature of OSA in cybersecurity architecture planning.

Question #:105

Scenario 6: Skyver manufactures electronic products, such as 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 ISO/IEC 27001.

Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware, and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well-informed by security principles and practices.

One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues. In a supportive manner, Colin suggested Lisa consider attending the session again.

Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver’s commitment to improving the customer experience through data-driven insights.

Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.

According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.

Based on the scenario above, answer the following question:

Which cloud computing model best aligns with Skyver's requirements?

A. Public cloud

B. Private cloud

C. Hybrid cloud

Answer: C

Question #:106

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 this the company using?

A. Decision tree machine learning

B. Supervised machine learning

C. Unsupervised machine learning

Answer: C

Explanation

According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the objectives of information security incident management is to collect and preserve records that can be used as evidence for disciplinary and legal action, as well as for learning and improvement purposes1. Therefore, Anna should be aware of the collection and preservation of records when gathering data for the forensics team. She should follow the guidelines and procedures specified in the information security incident management policy of InfoSec, which defines the type, format, content, and location of the records to be created and maintained2. The records should be accurate, complete, consistent, and reliable, and should be protected from unauthorized access, modification, or deletion3.

Question #:107

Scenario 6: Skyver manufactures electronic products, such as 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 ISO/IEC 27001.

Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware, and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well-informed by security principles and practices.

One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues. In a supportive manner, Colin suggested Lisa consider attending the session again.

Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver’s commitment to improving the customer experience through data-driven insights.

Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.

According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.

Based on the scenario above, answer the following question:

Did Skyver assign the adequate person for determining the materiality of the transition into operational mode of the ISMS?

A. Yes, the materiality of this change should be decided by the information security manager

B. No, the top management should be responsible for this decision

C. No, the ISMS implementation team should be responsible for this decision

Answer: A

Question #:108

Who should verily the effectiveness of the corrective actions taken by the auditee after an internal audit?

A. An Independent auditor should be contracted to perform this evaluation

B. The internal auditor

C. The information security manager

Answer: B

Question #:109

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, andcommunicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

In scenario 1, HealthGenic experienced a number of service interruptions due to the loss of functionality of the software. Which principle of information security has been affected in this case?

A. Availability

B. Confidentiality

C. Integrity

Answer: A

Explanation

Availability of information is the property of being accessible and usable upon demand by an authorized entity. In other words, availability ensures that the information and the systems that support it are always ready for use when needed. In the scenario, the availability of information was affected when HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. This means that the software was not able to handle the demand and provide the required functionality to the users. Therefore, the correct answer is A.

Question #:110

What supports the continual improvement of an ISMS?

A. The update of documented information

B. The update of action plans

C. The update of eternal audit reports

Answer: A

Explanation

According to the ISO/IEC 27001:2022 standard, the organization should establish, implement and maintain a process to manage changes that affect the information security management system (ISMS) and to continually improve the suitability, adequacy and effectiveness of the ISMS (section 8.1.3 and 10.2). The standard also states that the organization should update the documented information of the ISMS as necessary to reflect the changes and the results of the improvement process (section 8.1.3.2 and 10.2.2). Therefore, the update of documented information supports the continual improvement of the ISMS by ensuring that the ISMS is aligned with the current and future needs and expectations of the organization and its interested parties.

Question #:111

Invalid Electric, a manufacturer of electrical components, is preparing for its upcoming ISO 27001 certification audit. This is the first time the company has undergone such an audit, and many of its employees are not familiar with the process. The management team is concerned that employees may not be adequately prepared for interviews and the scrutiny of documentation during the audit.

To ensure that employees are ready for the audit, the management team is considering several options to help them understand what to expect and how to handle the auditor's questions confidently.

How can Invalid Electric's ensure that Us employees are prepared for the audit?

A. By conducting practice Interviews with the employees

B. By allowing the employees to observe the technologies used

C. By showing the employees the internal audit reports so they can anticipate the questions asked by the auditor

Answer: A

Question #:112

Scenario 8: BioVitalis

BioVitalis is a biopharmaceutical firm headquartered in California, the US Renowned for its pioneering work in the field of human therapeutics, BioVitalis places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation BioVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit. BioVitalis conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment. Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader

BioVitalis's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvementDecisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow up action plans, which were then approved by top management.

In response to the review outcomes. BioVitalis promptly implemented corrective actions, strengthening its Information security measures Additionally, dashboard tools were Introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests,

nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities.

Furthermore. BioVitalis embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities

Top management decided that the**information owner**would also be responsible for executing measurement activities across ISMS processes.

Question:

Did BioVitalis define the roles for measurement activities correctly?

A. Yes – the information owner can also be responsible for conducting measurement activities

B. No – as the information owner cannot perform different measurement-related roles and responsibilities

C. No – as the responsibility for conducting measurement activities should have been assigned to the information communicator

Answer: A

Explanation

ISO/IEC 27004:2016 Clause 6.2 states:

“Measurement roles can be assigned to**information owners**, system administrators, or process managers, as long as accountability and expertise are ensured.”

There is**no restriction**preventing information owners from also conducting measurements, provided competency and authority are documented. This is supported by ISO/IEC 27001:2022 Clause 5.3 – Organizational roles and responsibilities.

Question #:113

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company identified issues in its IT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, OperazelT implemented an information security management system (ISMS) based on ISO/IEC 27001.

In a collaborative effort involving the implementation team, OperazelT thoroughly assessed its business requirements and internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties to establish the preliminary scope of the ISMS. Following this, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to in clause 4.1, the requirements in

clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting OperazelT's commitment to information security.

OperazelT's information security team created a comprehensive information security policy that aligned with the company's strategic direction and legal requirements, informed by risk assessment findings and business strategies. This policy, alongside specific policies detailing security issues and assigning roles and responsibilities, was communicated internally and shared with external parties. The drafting, review, and approval of these policies involved active participation from top management, ensuring a robust framework for safeguarding information across all interested parties.

As OperazelT moved forward, the company entered the policy implementation phase, with a detailed plan encompassing security definition, role assignments, and training sessions. Lastly, the policy monitoring and maintenance phase was conducted, where monitoring mechanisms were established to ensure the company's information security policy is enforced and all employees comply with its requirements.

To further strengthen its information security framework, OperazelT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazelT decided to involve the services of external consultants to assess the state of its ISMS. The company collaborated with external consultants, which brought a fresh perspective and valuable insights to the gap analysis process, enabling OperazelT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazelT created a committee whose mission includes ensuring the proper operation of the ISMS, overseeing the company's risk assessment process, managing information security-related issues, recommending solutions to nonconformities, and monitoring the implementation of corrections and corrective actions.

Based on the scenario above, answer the following question:

Which ISMS boundaries did OperazelT include in its ISMS scope?

A. Solely information system boundaries

B. Physical boundaries only

C. Organizational and physical boundaries

Answer: C

Question #:114

Question:

An organization has compared its actual performance against predetermined performance targets. What is the primary purpose of this action?

A. To verify that all security incidents are resolved

B. To assess whether the organization's security objectives are being met

C. To eliminate the need for manual tracking and reporting

Answer: B

Explanation

ISO/IEC 27001:2022 Clause 9.1 –**Monitoring, measurement, analysis, and evaluation**:

"The organization shall evaluate the performance and effectiveness of the information security management system. The evaluation shall include... comparison against performance indicators and security objectives."

The purpose is to ensure that**security objectives**(Clause 6.2) are being met. Measuring performance allows organizations to determine whether controls and processes are effective and aligned with strategic goals.

Option A is too narrow, and Option C is incorrect because manual tracking may still be required in some cases.

Question #:115

Scenario:

A manufacturing company faced a risk of production delays due to potential supply chain disruptions. After assessing the potential impact, the company concluded the disruption was unlikely to significantly affect operations. The company decided to accept the risk.

Question:

Which risk treatment option did the company select in this case?

A. Risk avoidance

B. Risk retention

C. Risk deflection

Answer: B

Explanation

According to ISO/IEC 27001:2022 Clause 6.1.3 (a), an organization must determine appropriate**risk treatment options**. ISO 27005:2022 (Clause 8.2.2) defines**risk retention**as:

"The decision to accept the risk without taking any action to reduce it, often because the cost of mitigation is greater than the benefit."

The company assessed the likelihood and impact of the risk and decided**not to mitigate**, which qualifies as **risk retention**(also known as risk acceptance in ISO 27001 Clause 6.1.3(f)).

Question #:116

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's topmanagement appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Is Alex suitable for the position of internal auditor within the company?

A. Yes, Alex's recent experience in the day-to-day operations of the Compliance Department would benefit the internal auditor role

B. No, Alex should wait for a reasonable period of time to pass before transitioning to the internal auditor position

C. No, the internal audit can be conducted only by individuals who have not had operational roles

Answer: C

Question #:117

Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.

Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.

Based on the scenario above, answer the following question:

Which situation described in scenario 7 Indicates that Texas H&H Inc. implemented a detective control?

A. Texas H&H Inc. integrated the incident management policy in Its information security policy

B. Texas H&H Inc. tested its system for malicious activity and checked cloud based email settings

C. Texas H&H Inc. hired an expert to conduct a forensic analysis

Answer: C

Question #:118

Question:

Which statement regarding organizational roles, responsibilities, and authorities is**NOT**correct?

A. Top management is responsible for reporting on the performance of the ISMS and cannot assign this responsibility to someone else

B. A project manager can have information security responsibilities as well

C. Top management must assign the responsibility for ensuring that the ISMS conforms to ISO/IEC 27001

Answer: A

Explanation

ISO/IEC 27001:2022 Clause 5.3 –**Organizational roles, responsibilities, and authorities**clearly states:

"Top management shall assign the responsibility and authority for:

a) ensuring that the ISMS conforms to the requirements of this document;

b) reporting on the performance of the ISMS to top management."

This means top management is**not solely responsible**for directly reporting on performance—it can assign this responsibility to a qualified individual (such as an ISMS manager, CISO, or another responsible party). Therefore,**Option A is incorrect**and violates the intent of Clause 5.3.

Question #:119

Scenario 10:

NetworkFuse is a leading company that specializes in the design, production, and distribution of network hardware products. Over the past two years, NetworkFuse has maintained an operational Information Security Management System (ISMS) based on ISO/IEC 27001 requirements and a Quality Management System (QMS) based on ISO 9001. These systems are designed to ensure the company's commitment to both information security and the highest quality standards.

To further demonstrate its dedication to best practices and industry standards, NetworkFuse recently scheduled a combined certification audit. This audit seeks to validate NetworkFuse's compliance with both ISO/IEC 27001 and ISO 9001, showcasing the company's strong commitment to maintaining high standards in information security management and quality management. The process began with the careful selection of a certification body. NetworkFuse then took steps to prepare its employees for theaudit, which was crucial for ensuring a smooth and successful audit process. Additionally, NetworkFuse appointed individuals to manage the ISMS and the QMS.

NetworkFuse decided not to conduct a self-evaluation before the audit, a step often taken by organizations to proactively identify potential areas for improvement. The company's top management believed such an evaluation was unnecessary, confident in their existing systems and practices. This decision reflected their trust in the robustness of their ISMS and QMS. As part of the preparations, NetworkFuse took careful measures to ensure that all necessary documented information—including internal audit reports, management reviews, technological infrastructure, and the overall functioning of the ISMS and QMS—was readily available for the audit. This information would be vital in demonstrating their compliance with the ISO standards.

During the audit, NetworkFuse requested that the certification body not carry documentation off-site. This request stemmed from their commitment to safeguarding sensitive and proprietary information, reflecting their desire for maximum security and control during the audit process. Despite meticulous preparations, the actual audit did not proceed as scheduled. NetworkFuse raised concerns about the assigned audit team leader and requested a replacement. The company asserted that the same audit team leader had previously issued a recommendation for certification to one of NetworkFuse's main competitors. This potential conflict of interest raised concerns among the company's top management. However, the certification body rejected NetworkFuse's request for a replacement, and the audit process was canceled.

Which of the following actions is NOT a requirement for NetworkFuse in preparing for the certification audit?

A. Identifying subject matter experts

B. Preparing the personnel

C. Gathering documented information

Answer: A

Question #:120

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

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.

Question #:121

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 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

Answer: C

Explanation

According to ISO/IEC 27001:2022, clause 4.3, the organization shall determine the scope of the ISMS by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organizations. The scope shall be available as documented information and shall state what is included and what is excluded from the ISMS. The scope shall be reviewed and updated as necessary, and any changes shall be approved by the top management. Therefore, it is not acceptable for the IT team to change the ISMS scope and implement the required modifications without the approval of the management.

Question #:122

Question:

Which statement best describes an organization that has achieved the “Defined” maturity level?

A. The organization has implemented some processes, but there is no standardized procedure

B. The organization has fully automated and integrated its workflows for continuous improvement

C. The organization has standardized, documented, and communicated its procedures through training sessions

Answer: C

Explanation

According to the**ISO/IEC 27003:2017**and various ISMS implementation maturity models (e.g., COBIT, CMMI), a “Defined” maturity level implies:

“Processes are well-characterized and understood, and are described in standards, procedures, tools, and methods. These are communicated through training and organizational policy.”

This level ensures repeatability and consistency. It is higher than “initial” or “basic” maturity where ad hoc approaches dominate but does not yet include automation (which would fall under "Managed" or "Optimized").

Question #:123

Upon the risk assessment outcomes. Socket Inc. decided to:

• Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

• Require the change of passwords at least once every 60 days

• Keep backup copies of files on IT-provided network drives

• Assign users to a separate network when they have access to cloud storage files storing customers' personal data.

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 #:124

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 this scenario, answer the following question:

OpenTech has decided to establish a new version of its access control policy. What should the company do when such changes occur?

A. Identify the change factors to be monitored

B. Update the information security objectives

C. Include the changes in the scope

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 6.2, the organization shall establish information security objectives at relevant functions and levels. The information security objectives shall be consistent with the information security policy and relevant to the information security risks. The organization shall update the information security objectives as changes occur. Therefore, when OpenTech decides to establish a new version of its access control policy, it should update its information security objectives accordingly to reflect the changes and ensure alignment with the policy.

Question #:125

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives.

Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that

an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

What type of controls did Beauty implement to ensure the safety of products and unique formulas stored in the warehouse?

A. Administrative

B. Legal

C. Technical

Answer: C

Question #:126

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company identified issues in its IT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, OperazelT implemented an information security management system (ISMS) based on ISO/IEC 27001.

In a collaborative effort involving the implementation team, OperazelT thoroughly assessed its business requirements and internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties to establish the preliminary scope of the ISMS. Followingthis, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to in clause 4.1, the requirements in

clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting OperazelT's commitment to information security.

OperazelT's information security team created a comprehensive information security policy that aligned with the company's strategic direction and legal requirements, informed by risk assessment findings and business strategies. This policy, alongside specific policies detailing security issues and assigning roles and responsibilities, was communicated internally and shared with external parties. The drafting, review, and approval of these policies involved active participation from top management, ensuring a robust framework for safeguarding information across all interested parties.

As OperazelT moved forward, the company entered the policy implementation phase, with a detailed plan encompassing security definition, role assignments, and training sessions. Lastly, the policy monitoring and maintenance phase was conducted, where monitoring mechanisms were established to ensure the company's information security policy is enforced and all employees comply with its requirements.

To further strengthen its information security framework, OperazelT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazelT decided to involve the services of external consultants to assess the state of its ISMS. The company collaborated with external consultants, which brought a fresh perspective and valuable insights to the gap analysis process, enabling OperazelT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazelT created a committee whose mission includes ensuring the proper operation of the ISMS, overseeing the company's risk assessment process, managing information security-related issues, recommending solutions to nonconformities, and monitoring the implementation of corrections and corrective actions.

Based on the scenario above, answer the following question:

Did OperazelT include all the necessary factors when determining its scope?

A. Yes, the company adhered to the requirements of ISO/IEC 27001

B. No, it should have included the interfaces and dependencies between activities performed by other organizations as well

C. No, it should have only considered external issues referred to in 4.1 and the requirements referred to in 4.2

Answer: A

Question #:127

Which of the following statements is accurate regarding the methodology for managing the implementation of an ISMS?

A. Organizations must strictly follow a specific methodology to meet the minimum requirements

B. The sequence of steps must remain fixed throughout the ISMS implementation

C. Organizations can adapt the methodology to their specific context, and steps can be modified as needed

Answer: C

Question #:128

What risk treatment option has Company A Implemented If it has decided not to collect information from users so that It is not necessary to implement information security controls?

A. Risk avoidance

B. Risk retention

C. Risk modification

Answer: A

Question #:129

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 #:130

Which of the following is the information security committee responsible for?

A. Ensure smooth running of the ISMS

B. Set annual objectives and the ISMS strategy

C. Treat the nonconformities

Answer: B

Question #:131

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensiveinformation security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives.

Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

Under which category does the vulnerability identified by Maya during the incident fall into?

A. Network

B. Site

C. Organization

Answer: C

Question #:132

Scenario:

An employee at Reyae Ltd unintentionally sent an email containing critical business strategies to a competitor due to an autofill email suggestion error. The email included proprietary trade secrets and confidential client data. Upon receiving the email, the competitor altered the information and attempted to use it to mislead clients into switching services.

Question:

Which of the following statements correctly describes the security principles affected in this situation?

A. Reyae Ltd's confidentiality was compromised first, while the competitor's actions led to an integrity violation

B. Reyae Ltd's integrity was compromised first, while the competitor's actions led to an availability violation

C. Reyae Ltd's availability was compromised first, while the competitor’s actions led to an integrity violation

Answer: A

Explanation

According to ISO/IEC 27002:2022, information security is based on the principles of confidentiality, integrity, and availability (CIA). Confidentiality refers to preventing unauthorized disclosure, integrity ensures information accuracy and trustworthiness, and availability ensures information is accessible when needed.

In this case:

- **Confidentiality**was compromised when the sensitive email was mistakenly sent to the competitor.
- The**integrity**was violated when the competitor altered the proprietary data to mislead clients.

This directly aligns with the definitions in ISO/IEC 27002:2022, clause 3.1.7 (Confidential Information) and 3.1.13 (Information Security Breach).

Question #:133

Scenario 1:

HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canada. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.

As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.

When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

However, HealthGenic also uncovered unauthorized changes to user access controls. Consequently, some medical reports were altered, resulting in incomplete and inaccurate medical records. The company swiftly acknowledged and corrected the unintentional changes to user access controls. When analyzing the root cause of these changes, HealthGenic identified a vulnerability related to the segregation of duties within the IT department, which allowed individuals with system administration access also to manage user access controls. Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

In response to the consequences of the service interruptions, the software development company revamped its infrastructure by adopting a scalable architecture hosted on a cloud platform, enabling dynamic resource allocation based on demand. Rigorous load testing and performance optimization were conducted to identify and address potential bottlenecks, ensuring the system could handle increased user loads seamlessly. Additionally, the company promptly assessed the unauthorized access and data alterations.

To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data, HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.

In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.

Based on scenario 1, what type of controls did HealthGenic decide to prioritize?

A. Technical controls

B. Administrative controls

C. Managerial controls

Answer: B

Question #:134

According to ISO/IEC 270G1. why shall organizations document nonconformities?

A. To provide evidence of the requirements set by internal audit after reviewing their audit reports

B. To provide evidence of the results of the corrective actions and the nature of the nonconformities

C. To provide evidence of regulations set by external sources that need to be followed by the organization

Answer: B

Question #:135

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

Answer: C

Explanation

Information backup is a corrective control that aims to restore the information in case of data loss, corruption, or deletion. It does not prevent information security incidents from recurring, but rather mitigates their impact.

The other options are preventive controls that reduce the likelihood of information security incidents by limiting the access to authorized personnel, segregating the networks, and using cryptography. These controls can help Socket Inc. avoid future attacks on its MongoDB database by addressing the vulnerabilities that were exploited by the hackers.

Question #:136

What does the organization still need to manage when using Platform as a Service (PaaS)?

A. Operating system and virtualization

B. Servers and storage

C. Application and data

Answer: C

Question #:137

Upon the risk assessment outcomes. Socket Inc. decided to:

• Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

• Require the change of passwords at least once every 60 days

• Keep backup copies of files on IT-provided network drives

• Assign users to a separate network when they have access to cloud storage files storing customers' personal data.

Based on scenario 5. Socket Inc. decided to assign users lo a separate network when accessing cloud storage tiles. What does this ensure?

A. Belter security when using cloud storage files

B. Elimination of risks related to the use of cloud storage services

C. Creation of backup copies of files

Answer: A

Question #:138

If an organization wants to monitor operations in real time and notify users about deviations, which type of dashboard should be used?

A. Strategic dashboard

B. Tactical dashboard

C. Operational dashboard

Answer: C

Question #:139

Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which serves as a structured framework and a guideline that outlines thehigh-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its 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 a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

Then, they evaluated the risks based on the risk evaluation criteria, where they decided to treat only the risks of the high-risk category. Additionally, they focused primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted.

Based on the scenario above, answer the following question:

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. TradeB drafted the Statement of Applicability before conducting the risk assessment

C. TradeB decided to treat only the risks of the high-risk category

Answer: B

Question #:140

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

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

Answer: B

Explanation

According to ISO/IEC 27001:2013, clause 9.3, the top management of an organization must review the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review must consider the status of actions from previous management reviews, changes in external and internal issues, the performance and effectiveness of the ISMS, feedback from interested parties, results of risk assessment and treatment, and opportunities for continual improvement. The management review must also result in decisions and actions related to the ISMS policy and objectives, resources, risks and opportunities, and improvement. The management review is a critical process that demonstrates the commitment and involvement of the top management in the ISMS and its alignment with the strategic direction of the organization. The management review also provides input for the internal audit and the certification audit.

SunDee has neglected to conduct management reviews regularly, which means that it has not fulfilled the requirement of clause 9.3. This is a major nonconformity that could jeopardize the renewal of the ISMS

certificate. The certification body will verify whether SunDee has conducted management reviews and whether they have been effective and documented. If SunDee cannot provide evidence of management reviews, it will have to take corrective actions and undergo a follow-up audit before the certificate can be renewed. Alternatively, the certification body may decide to suspend or withdraw the certificate if SunDee fails to address the nonconformity within a specified time frame.

Question #:141

Scenario 9: CoreBit Systems

CoreBit Systems, with its headquarters m San Francisco, specializes in information and communication technology (ICT) solutions, its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients a smooth transition into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently. John, the internal auditor of CoreBit Systems, conducted an internal audit which uncovered nonconformities related to their monitoring procedures and system vulnerabilities, in response to the identified nonconformities. CoreBit Systems decided to employ a comprehensive problem-solving approach to solve these issues systematically. The method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of issues. This approach involves several steps. First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root cause of the nonconformities, CoreBit Systems's ISMS project manager. Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective action for addressing a nonconformity, Julia identified the issue as significant and assessed a high likelihood of its reoccurrence Consequently, she chose to implement temporary corrective actions. Afterward. Julia combined all the nonconformities Into a single action plan and sought approval from the top management.

The submitted action plan 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.

However. Julia's submitted action plan was not approved by top management The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process, and notably, the revised action plans lacked a defined schedule for execution.

Question:

Which method did CoreBit Systems use to address and prevent reoccurring problems after identifying the nonconformities?

A. The Eight Disciplines Problem Solving (8Ds) method

B. DMAIC (Define, Measure, Analyze, Improve, Control) method

C. Lean Six Sigma method

Answer: A

Explanation

The described process matches the**8D (Eight Disciplines) method**, commonly used for quality and compliance management. The method includes:

- Forming a team
- Describing the problem
- Implementing containment
- Identifying root causes
- Choosing corrective actions
- Implementing actions
- Preventing recurrence
- Recognizing contributions

This aligns exactly with CoreBit's approach.

Question #:142

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Which of the following physical controls was NOT included in Socket Inc.'s strategy?

A. Annex A 7.2 Physical entry

B. Annex A 7.9 Security of assets off-premises

C. Annex A 7.11 Supporting utilities

Answer: C

Question #:143

Upon the risk assessment outcomes. Socket Inc. decided to:

• Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

• Require the change of passwords at least once every 60 days

• Keep backup copies of files on IT-provided network drives

• Assign users to a separate network when they have access to cloud storage files storing customers' personal data.

Based on scenario 5, what can be considered as a residual risk to Socket Inc.?

A. Files arc decrypted once the user is authenticated

B. Users with access to cloud storage files are segregated on a separate network

C. The use of passwords with at least 12 characters containing a mixture of uppercase and lowercase letters, symbols, and numbers

Answer: A

Question #:144

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

Answer: B

Explanation

ISO/IEC 27001:2022 does not prescribe a specific set of security controls that must be implemented by all organizations. Instead, it allows organizations to select and implement the controls that are appropriate for their context, based on the results of a risk assessment and a risk treatment plan. The risk treatment plan is a document that specifies the actions to be taken to address the identified risks, including the selection of controls from Annex A or other sources, the allocation of responsibilities, the expected outcomes, the priorities and the resources. Therefore, the security controls that must be implemented to comply with ISO /IEC 27001 are those that are included in the risk treatment plan, which may vary from one organization to another.

Question #:145

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site

However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body

The certification body rejected NetworkFuse's request to change the audit team leader. Is this acceptable? Refer to scenario 10.

A. No, because an auditee cannot request the rejection of an audit team member

B. Yes, because NetworkFuse did not give a valid reason to support their claims

C. No, auditee's requests for the replacement of auditors must be accepted

Answer: B

Explanation

According to the ISO/IEC 27001 : 2022 Lead Implementer course, the certification body is responsible for selecting and appointing the audit team members, taking into account the competence, impartiality, and objectivity of the auditors1. The auditee can request the replacement of an audit team member only if there is a valid reason to doubt their competence or impartiality, such as a personal or professional conflict of interest, a lack of relevant experience or qualifications, or a previous involvement in the auditee's activities2. However, NetworkFuse did not give a valid reason to support their claims, as the fact that the audit team leader issued a recommendation for certification to their main competitor does not imply a conflict of interest or a bias. Therefore, the certification body rejected NetworkFuse's request to change the audit team leader, which is acceptable.

Question #:146

Question:

According to ISO/IEC 27001 controls, why should the use of privileged utility programs be restricted and tightly controlled?

A. To ensure that utility programs are compatible with existing system software

B. To prevent misuse of utility programs that could override system and application controls

C. To enable the correlation and analysis of security-related events

Answer: B

Explanation

ISO/IEC 27002:2022 Clause 8.11 addresses "Use of privileged utility programs":

"The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled to prevent misuse."

Such tools can provide powerful access or modification capabilities, which if misused can compromise the integrity and confidentiality of systems.

Question #:147

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

Answer: A

Explanation

Risk modification is one of the four risk treatment options defined by ISO/IEC 27001, which involves applying controls to reduce the likelihood and/or impact of the risk. By requiring its employees to change their email passwords at least once every 60 days, Company A has implemented a risk modification option to reduce the risk of unauthorized access to its email accounts. Changing passwords frequently can make it harder for attackers to guess or crack the passwords, and can limit the damage if a password is compromised.

The other three risk treatment options are:

- Risk avoidance: This option involves eliminating the risk source or discontinuing the activity that causes the risk. For example, Company A could avoid the risk of email compromise by not using email at all, but this would also mean losing the benefits of email communication.
- Risk retention: This option involves accepting the risk and its consequences, either because the risk is too low to justify any treatment, or because the cost of treatment is too high compared to the potential loss. For example, Company A could retain the risk of email compromise by not implementing any security measures, but this would expose the company to potential breaches and reputational damage.
- Risk transfer: This option involves sharing or transferring the risk to a third party, such as an insurer, a supplier, or a partner. For example, Company A could transfer the risk of emailcompromise by outsourcing its email service to a cloud provider, who would be responsible for the security and availability of the email accounts.

Question #:148

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and

associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Based on scenario 3, did Socket Inc. comply with ISO/IEC 27001 organizational controls regarding its operating procedures?

A. Yes, it did comply with ISO/IEC 27001 requirements

B. No, operating procedures for information processing facilities should have been specifically provided to personnel who require them

C. No, operating procedures for information processing facilities should have been exclusively available to the Information Technology Department or a similar unit within the company

Answer: A

Question #:149

What is the main difference between an audit program and an audit plan?

A. An audit program outlines the activities and arrangements for a particular audit, while an audit plan provides an overarching framework for a series of audits with specific timelines and purposes

B. An audit program outlines the overarching framework for a series of audits with specific timelines and purposes, while an audit plan outlines the activities and arrangements for a particular audit

C. An audit program outlines policies, procedures, or requirements for reference in audit evidence comparison, while an audit plan provides an overarching framework for a series of audits with specific timelines and purposes

Answer: B

Question #:150

Following a repotted event, an Information security event ticket has been completed and its priority has been assigned. Then, the event has been evaluated to determine If it is an information security incident, which phase of the incident management has been completed?

A. initial assessment and decision

B. Detection and reporting

C. Evaluation and confirmation

Answer: C

Question #:151

Scenario 5: Evergreen

Evergreen is undergoing ISMS implementation. In their structure, there exists an Information Security Committee (ISC), which leads and governs security operations.

Question:

Can the information security committee at Evergreen take on the role of the emergency committee in the event of a major incident?

A. No – no one should assume the role of the emergency committee to prevent the mismanagement of major incidents

B. Yes – can assume the role of the emergency committee in the event of a major incident

C. No – only the steering committee can assume the role of the emergency committee

Answer: B

Explanation

ISO/IEC 27002:2022 Clause 5.17 – Information Security in Project Management, and Clause 5.2 – Roles and Responsibilities, support role flexibility provided responsibilities are clear and documented.

The**same group**can assume multiple roles, provided:

- The roles are defined
- Competency is proven
- There is no conflict of interest

It’s acceptable and sometimes encouraged for an established, competent committee like the ISC to assume emergency roles during incidents, enhancing response efficiency.

Question #:152

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

Answer: A

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, eitherbecause the bugs are not critical or because the cost of fixing them would outweigh the benefits.

Question #:153

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

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

Answer: A

Explanation

- Preventive controls: These are controls that aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Examples of preventive controls are encryption, firewalls, locks, policies, etc.
- Detective controls: These are controls that aim to detect or discover the occurrence of a security incident or its symptoms. Examples of detective controls are logs, alarms, audits, etc.
- Corrective controls: These are controls that aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact. Examples of corrective controls are backups, recovery plans, incident response teams, etc.
- Administrative controls: These are controls that involve the management and governance of information security, such as policies, procedures, roles, responsibilities, awareness, training, etc.
- Technical controls: These are controls that involve the use of technology or software to implement information security, such as encryption, firewalls, anti-malware, authentication, etc.
- Physical controls: These are controls that involve the protection of physical assets or locations from unauthorized access, damage, or theft, such as locks, fences, cameras, guards, etc.
- Legal controls: These are controls that involve the compliance with laws, regulations, contracts, or agreements related to information security, such as privacy laws, data protection laws, confidentiality agreements, etc.

In scenario 2, the action of Beauty reviewing all user access rights is best described as a "Preventive and Administrative" control.

- Preventive Control: The review of user access rights is a preventive measure. It is designed to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to specific files. By controlling access rights, the organization aims to prevent potential security breaches and protect sensitive data.

- Administrative Control: This action also falls under administrative controls, sometimes referred to as managerial controls. These controls involve policies, procedures, and practices related to the management of the organization and its employees. In this case, the review of access rights is a part of the company's administrative procedures to manage the security of information systems.

Question #:154

Scenario 1:

HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canada. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.

As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.

When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

However, HealthGenic also uncovered unauthorized changes to user access controls. Consequently, some medical reports were altered, resulting in incomplete and inaccurate medical records. The company swiftly acknowledged and corrected the unintentional changes to user access controls. When analyzing the root cause of these changes, HealthGenic identified a vulnerability related to the segregation of duties within the IT department, which allowed individuals with system administration access also to manage user access controls. Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

In response to the consequences of the service interruptions, the software development company revamped its infrastructure by adopting a scalable architecture hosted on a cloud platform, enabling dynamic resource allocation based on demand. Rigorous load testing and performance optimization wereconducted to identify and address potential bottlenecks, ensuring the system could handle increased user loads seamlessly. Additionally, the company promptly assessed the unauthorized access and data alterations.

To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data,

HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.

In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.

During which of the following processes did HealthGenic notice a critical gap in its capacity planning and infrastructure resilience?

A. Risk evaluation

B. Risk treatment

C. Risk acceptance

Answer: A

Question #:155

Scenario 6: Skyver manufactures electronic products, such as 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 ISO/IEC 27001.

Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware, and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well-informed by security principles and practices.

One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues. In a supportive manner, Colin suggested Lisa consider attending the session again.

Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver’s commitment to improving the customer experience through data-driven insights.

Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.

According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.

Based on the scenario above, answer the following question:

As part of its strategic initiative to improve customer experiences, Skyver is exploring the implementation of advanced AI solutions. Which type of AI is the company likely considering for this purpose?

A. Weak AI

B. Machine learning

C. Strong AI

Answer: B

Question #:156

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization’s topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Based on scenario 3, did Socket Inc. adhere to the requirements of ISO/IEC 27001 regarding ISMS documented information?

A. No, Socket Inc. consolidated all controls of a group into a single document while the standard requires the controls to be documented in four groups

B. Yes, the standard requires that all security controls be included in a single document

C. Yes, there is no mandatory requirement on how to document processes or security controls in the standard

Answer: C

Question #:157

Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flowcontrol services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization’s topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and

documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control 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, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.

Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.

Based on the scenario above, answer the following question:

Which security function has Socket Inc. considered when implementing data flow control services to prevent unauthorized access between departments and external networks? Refer to scenario 3.

A. Access control services

B. Boundary control services

C. Integrity services

Answer: B

Question #:158

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

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.

Question #:159

Del&Co has decided to improve their staff-related controls to prevent incidents. Which of the following is NOT a preventive control related to the Del&Co's staff?

A. Authentication and authorization

B. Control of physical access to the equipment

C. Video cameras

Answer: C

Explanation

According to ISO/IEC 27001:2022, Annex A.7, the objective of human resource security is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, and to reduce the risk of human error, theft, fraud, or misuse of facilities. The standard specifies eight controls in this domain, which are:

- A.7.1 Prior to employment: This control covers the screening, terms and conditions, and roles and responsibilities of employees and contractors before they are hired.
- A.7.2 During employment: This control covers the awareness, education, and training, disciplinary process, and management responsibilities of employees and contractors during their employment.

- A.7.3 Termination and change of employment: This control covers the return of assets, removal of access rights, and exit interviews of employees and contractors when they leave or change their roles.

The other controls in Annex A are related to other aspects of information security, such as organizational, physical, and technological controls. For example:

- A.9.2 User access management: This control covers the authentication and authorization of users to access information systems and services, based on their roles and responsibilities.
- A.11.1 Secure areas: This control covers the control of physical access to the equipment and information assets, such as locks, alarms, guards, etc.
- A.13.2 Information transfer: This control covers the protection of information during its transfer, such as encryption, digital signatures, secure protocols, etc.

Therefore, video cameras are not a preventive control related to the staff, but rather a physical control related to the equipment and assets. Video cameras can be used to monitor and record the activities of the staff, but they cannot prevent them from causing incidents. They can only help to detect and investigate incidents after they occur.

Question #:160

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 Trade B 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

Answer: B

Explanation

According to ISO/IEC 27001 : 2022, risk acceptance criteria are the criteria used to decide whether a risk can be accepted or not1. Risk acceptance criteria are often based on a maximum level of acceptable risks, on cost-benefits considerations, or on consequences for the organization2. In the scenario, TradeB decided to treat only the high risk category, which implies that

Question #:161

Which of the following is the most suitable option for presenting raw data in a user-friendly, easy-to-read format?

A. Scorecards

B. Reports

C. Gages

Answer: A

Question #:162

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, clause 10.2.2, the organization shall define and apply an information security incident management process that includes the following activities:

- reporting information security events and weaknesses;
- assessing information security events and classifying them as information security incidents;
- responding to information security incidents according to their classification;

- learning from information security incidents, including identifying causes, taking corrective actions and preventive actions, and communicating the results and actions taken;

- collecting evidence, where applicable.

The standard does not specify who should perform these activities, as long as they are done in a consistent and effective manner. Therefore, the organization may choose to conduct forensic investigation internally or by using external consultants, depending on its needs, resources, and capabilities. However, the organization should ensure that the external consultants are competent, trustworthy, and comply with the organization's policies and procedures.

Question #:163

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affectingthe ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Does SunDee's approach align with the best practices for evaluating and maintaining the effectiveness of an ISMS?

A. Yes, because comprehensive coverage is essential to achieve ISMS objectives

B. Yes, because a diverse set of measures minimizes the likelihood of overlooking any potential security risks

C. No, as an excessive number of measures may distort SunDee’s focus and obscure what is genuinely important

Answer: B

Question #:164

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

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.

Question #:165

What should an organization demonstrate through documentation?

A. That the complexity of processes and their interactions is documented

B. That the distribution of paper copies is regularly complete

C. That Its security controls are implemented based on risk scenarios

Answer: C

Question #:166

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

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

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 SoA should be drafted after conducting the risk assessment, not before. Drafting the SoA before the risk assessment may lead to inappropriate or incomplete selection of controls, as the organization may not have a clear understanding of its information security risks and their impact.

Question #:167

Scenario 9:

OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan 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."

However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.

Did Julia make an appropriate decision regarding the nonconformities with a high likelihood of reoccurrence?

A. Yes, Julia's decision to implement temporary corrective actions was consistent with best practices

B. No, as temporary corrective actions are not allowed in the evaluation phase

C. No, implementing temporary actions during the corrective action process is not recommended

Answer: A

Question #:168

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 8. how does the HealthGenic’s negligence affect the ISMS certificate?

A. HealthGenic will be able to renew the ISMS certificate, as they did not detect any information security incident in the past two years

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

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

Answer: B

Question #:169

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.

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

Answer: C

Explanation

Intrinsic vulnerabilities are related to the characteristics of the asset that make it susceptible to threats, regardless of the presence or absence of controls. In scenario 1, the complicated user interface of the web-based medical software is an intrinsic vulnerability, as it is a feature of the software that makes it difficult to use and increases the likelihood of human errors. The software malfunction and the service interruptions are not intrinsic vulnerabilities, but rather incidents that occurred due to external factors, such as the increased number of users or the software company’s actions.

Question #:170

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-lime authorization code sent to their smartphone. What can be concluded from this scenario?

A. FinanceX has implemented a securityControl 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

Answer: A

Explanation

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. A security control is a measure that is put in place to protect the confidentiality, integrity, and availability of informationassets. In this scenario, FinanceX has implemented a security control that ensures the confidentiality of information by requiring clients to enter a one-time authorization code sent to their smartphone when they log in to their online banking platform. This control prevents unauthorized

access to the clients' bank accounts and protects their sensitive information from being disclosed to third parties. The one-time authorization code is a form of two-factor authentication, which is a security technique that requires two pieces of evidence to verify the identity of a user. In this case, the two factors are something the user knows (their username and password) and something the user has (their smartphone). Two-factor authentication is a recommended security control for online banking platforms, as it provides a higher level of security than single-factor authentication, which relies only on one piece of evidence, such as a password.

Question #:171

Which of the following processes may involve increasing risk in order to pursue an opportunity?

A. Risk analysis

B. Risk treatment

C. Risk identification

Answer: B

Question #:172

The purpose of control 5.9 inventory of Information and other associated assets of ISO/IEC 27001 is to identify organization's information and other associated assets in order to preserve their information security and assign ownership. Which of the following actions docs NOT fulfill this purpose?

A. Conducting regular reviews of identified information and other associated assets

B. Establishing rules to control physical and logical access to Information and other associated assets

C. Assigning the responsibility for appropriately classifying and protecting information and other associated assets to the asset owners

Answer: B

Question #:173

Scenario 7: InfoSec is a multinational corporation headquartered in Boston, MA, which provides professional electronics, gaming, and entertainment services. After facing numerous informationsecurity 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 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

Answer: C

Explanation

According to the ISO/IEC 27001 : 2022 standard, information security incident management is the process of ensuring a consistent and effective approach to the management of information security incidents, events and weaknesses. One of the objectives of this process is to collect and preserve evidence that can be used for disciplinary and legal action, as well as for learning and improvement. Therefore, Anna should be aware of the collection and preservation of records when gathering data for the forensics team. She should follow the information security incident management policy of InfoSec, which specifies the type, format, content and location of the records to be created and maintained. She should also ensure that the records are protected from unauthorized access, modification, deletion or disclosure, and that they are retained for an appropriate period of time.

Question #:174

What is the primary requirement for the documented information of an ISMS?

A. It must exist solely in a digital format to ensure modern compatibility

B. It must be sufficiently flexible to adapt to any identified change triggers

C. It must be accessible to the public at all times to maintain transparency

Answer: B

Question #:175

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 informationsecurity-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

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

Answer: A

Explanation

According to ISO/IEC 27001, training and awareness are two different but complementary activities that aim to enhance the information security competence and performance of the organization’s personnel. Training is the process of providing instruction and guidance to help individuals acquire certain skills, knowledge, or abilities related to information security. Awareness is the process of raising the level of consciousness and understanding of the importance and benefits of information security, and developing certain habits and behaviors that support the information security objectives and requirements.

In scenario 6, Colin is holding a training and awareness session for the personnel of Skyver, which means he is combining both activities to achieve a more effective and comprehensive information security education. The training part of the session covers topics such as Skyver’s information security policies and procedures, and techniques for mitigating phishing and malware. The awareness part of the session covers topics such as Skyver’s information security approaches and challenges, and the benefits of information security for the organization and its customers. The purpose of the session is to help the personnel acquire the necessary skills to perform their information security roles and responsibilities, and to develop the appropriate habits and behaviors to protect the information assets of the organization.

Question #:176

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company identified issues in its IT systems, including improperuser permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance

information security, OperazelT implemented an information security management system (ISMS) based on ISO/IEC 27001.

In a collaborative effort involving the implementation team, OperazelT thoroughly assessed its business requirements and internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties to establish the preliminary scope of the ISMS. Following this, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to in clause 4.1, the requirements in clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting OperazelT's commitment to information security.

OperazelT's information security team created a comprehensive information security policy that aligned with the company's strategic direction and legal requirements, informed by risk assessment findings and business strategies. This policy, alongside specific policies detailing security issues and assigning roles and responsibilities, was communicated internally and shared with external parties. The drafting, review, and approval of these policies involved active participation from top management, ensuring a robust framework for safeguarding information across all interested parties.

As OperazelT moved forward, the company entered the policy implementation phase, with a detailed plan encompassing security definition, role assignments, and training sessions. Lastly, the policy monitoring and maintenance phase was conducted, where monitoring mechanisms were established to ensure the company's information security policy is enforced and all employees comply with its requirements.

To further strengthen its information security framework, OperazelT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazelT decided to involve the services of external consultants to assess the state of its ISMS. The company collaborated with external consultants, which brought a fresh perspective and valuable insights to the gap analysis process, enabling OperazelT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazelT created a committee whose mission includes ensuring the proper operation of the ISMS, overseeing the company's risk assessment process, managing information security-related issues, recommending solutions to nonconformities, and monitoring the implementation of corrections and corrective actions.

Based on the scenario above, answer the following question:

What committee did OperazelT establish to guarantee the proper operation of the ISMS?

A. Information security committee

B. Management committee

C. Operational committee

Answer: A

Question #:177

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives.

Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team andother employees with access to confidential information, emphasizing the importance of system and network security.

Based on scenario 2, what type of controls did Beauty use during incident investigation?

A. Preventive controls

B. Detective controls

C. Corrective controls

Answer: B

Question #:178

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, 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

Answer: B

Explanation

In Scenario 3, the measure that would help Socket Inc. address similar information security incidents in the future is "B. Using cryptographic keys to protect the database from unauthorized access." Implementing cryptographic controls, including cryptographic key management, is a proactive measure to secure the data in the MongoDB database against unauthorized access. It ensures that even if attackers gain access to the database, they cannot read or misuse the data without the appropriate cryptographic keys. This approach aligns with best practices for securing sensitive data and is part of a comprehensive security strategy.

Question #:179

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on the scenario above, answer the following question:

Which situation described in scenario 2 Indicates service unavailability?

A. Lucas was no! able to access the website with his credentials

B. Attackers still had access to the data when Solena delivered a press release

C. Lucas was asked to change his password weekly

Answer: A

Question #:180

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

Answer: C

Explanation

According to the ISO/IEC 27001:2022 standard, a performance indicator is “a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization” (section 3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.

Question #:181

Scenario 2:

Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care productsthat enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential threats and vulnerabilities associated with its new e-commerce venture, aligned with its business strategy and objectives.

Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.

After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

What type of assets were compromised in Beauty's incident?

A. Personal virtual assets

B. Organizational virtual assets

C. Organizational physical assets

Answer: A

Question #:182

'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

Answer: B

Explanation

The statement describes the organizational boundaries of the ISMS scope, which define which parts of the organization are included or excluded from the ISMS. The organizational boundaries can be based on criteria such as departments, functions, processes, activities, or locations. In this case, the statement specifies that the ISMS covers all departments within Company XYZ that have access to customers' data, and excludes the ones that do not. The statement also explains the purpose of the ISMS, which is to ensure the confidentiality, integrity, and availability of customers' data, and ensure compliance with the applicable regulatory requirements regarding information security.

The statement does not describe the information systems boundary of the ISMS scope, which defines which information systems are included or excluded from the ISMS. The information systems boundary can be based on criteria such as hardware, software, networks, databases, or applications. The statement does not mention any specific information systems that are covered by the ISMS.

The statement also does not describe the physical boundary of the ISMS scope, which defines which physical locations are included or excluded from the ISMS. The physical boundary can be based on criteria such as buildings, rooms, cabinets, or devices. The statement does not mention any specific physical locations that are covered by the ISMS.

Question #:183

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

Answer: B

Explanation

According to the ISO/IEC 27001:2022 Lead Implementer objectives and content, the maturity levels of information security controls are based on the ISO/IEC 15504standard, which defines five levels of process capability: incomplete, performed, managed, established, and optimized1. Each level has a set of attributes that describe the characteristics of the process at that level. The level of defined corresponds to the attribute of process performance, which means that the process achieves its expected outcomes2. In this case, the control of two-factor authentication has been documented, standardized, and communicated, which implies that it has a clear purpose and expected outcomes. However, the control is not consistently implemented, monitored, or measured, which means that it does not meet the attributes of the higher levels of managed, established, or optimized. Therefore, the control is at the level of defined, which is the second level of maturity.

Question #:184

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

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.

Question #:185

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

Answer: A

Explanation

According to ISO/IEC 27001, an incident management process must include processes for using knowledge gained from information security incidents to reduce the likelihood or impact of future incidents, and to improve the overall level of information security. This means that the organization should conduct a root cause analysis of the incidents, identify the lessons learned, and implement corrective actions to prevent recurrence or mitigate consequences. The organization should also document and communicate the results of the incident management process to relevant stakeholders, and update the risk assessment and treatment plan accordingly. (Must be taken from ISO/IEC 27001 : 2022 Lead Implementer resources)

Question #:186

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 12month period

C. Only the approach provided by the standard

Answer: A

Explanation

ISO/IEC 27001:2022 does not prescribe a specific approach for implementing an ISMS, but rather provides a set of requirements and guidelines that can be adapted to the organization’s context, scope, and objectives. Therefore, organizations can use any approach that is suitable for their scope, as long as it meets the requirements of the standard and enables the achievement of the intended outcomes of the ISMS. The approach should also consider the needs and expectations of the interested parties, the risks and opportunities related to information security, and the legal and regulatory obligations of the organization.

Question #:187

A healthcare organization needs to ensure that patient records are available to the medical staff whenever needed. Which measure should it prioritize to achieve this?

A. Implementing multi-factor authentication

B. Establishing record retention policies

C. Using version control systems for data management

Answer: B

Question #:188

Org Y. a well-known bank, 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. Org Y has implemented an integrity control that avoids the involuntary corruption of data

B. Org Y has incorrectly implemented a security control that could become a vulnerability

C. Org Y has implemented a security control that ensures the confidentiality of information

Answer: C

Question #:189

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, what type of assets were identified during risk assessment?

A. Supporting assets

B. Primary assets

C. Business assets

Answer: A

Explanation

According to ISO/IEC 27005:2021, there are three types of assets in information security risk management: primary assets, supporting assets, and business assets. Primary assets are the information and business processes that support the organization's objectives and operations. Supporting assets are the resources that enable the primary assets to function, such as hardware, software, networks, people, facilities, etc. Business assets are the outcomes or benefits that the organization expects from the primary assets, such as reputation, market share, customer satisfaction, etc. (Must be taken from ISO/IEC 27001 : 2022 Lead Implementer resources)

In scenario 4, the assets that were identified during risk assessment are hardware, software, and networks, which are examples of supporting assets. These assets are necessary for the information and business processes of TradeB to operate, but they are not the main focus of the risk assessment. The risk assessment should also consider the primary assets and the business assets, as well as the threats and vulnerabilities that affect them, and the potential impacts and likelihood of information security incidents.

Question #:190

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.

Question #:191

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

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.

Question #:192

Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts 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 implement 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 a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.

On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for 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.

As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.

Furthermore, while implementing the communication plan for information security, InfoSec's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.

InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Based on this scenario, answer the following question:

Which of the following cloud service models did InfoSec use?

A. Infrastructure as a Service

B. Platform as a Service

C. Software as a Service

Answer: C

Question #:193

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

Answer: B

Explanation

In the scenario described, Kyte's failure to provide answers to users' questions in the Q&A section of its online shopping website demonstrates a lack of responsiveness. Responsiveness is a key principle of an effective communication strategy, especially in customer service. It involves timely and appropriate reactions to inquiries and feedback, ensuring that customers' concerns and queries are addressed promptly. By not responding, Kyte is not adhering to this principle, potentially affecting customer satisfaction and trust.

Question #:194

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.

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

Answer: B

Explanation

According to ISO/IEC 27001:2022, a threat is any incident that could negatively affect the confidentiality, integrity or availability of an asset1. In this scenario, the asset is the information related to HealthGenic’s patients, which is stored and processed by the web-based medical software. The software company’s modification of some files that comprised sensitive information related to HealthGenic’s patients is an incident that could negatively affect the confidentiality and integrity of the asset, as it resulted in incomplete and incorrect medical reports and invaded the patients’ privacy. Therefore, this situation represents a threat to HealthGenic.

Question #:195

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.

During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.

SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.

In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.

Based on the scenario above, answer the following question:

Based on scenario 8, which of the following dashboards did SunDee utilize?

A. Operational dashboards

B. Tactical dashboards

C. Strategic dashboards

Answer: C

Question #:196

Scenario 9:

OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The

company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan 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."

However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.

Which method did OpenTech choose to use for addressing and preventing reoccurring problems after identifying the nonconformities?

A. The Eight Disciplines Problem Solving (8Ds) method

B. DMAIC (Define, Measure, Analyze, Improve, Control) method

C. Lean Six Sigma method

Answer: A

Question #:197

Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts 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 implement 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 a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.

On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for 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.

As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.

Furthermore, while implementing the communication plan for information security, InfoSec’s top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.

InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Based on this scenario, answer the following question:

Is the responsibility of InfoSec’s top management appropriately established in implementing the communication plan for information security?

A. No, the top management is responsible for allocating resources for communication activities

B. Yes, the top management is responsible for creating a new product development roadmap as an activity during the communication plan implementation

C. No, the top management is responsible for communicating only technical specifications for products

Answer: B

Question #:198

Question:

An organization has implemented additional controls from other sources alongside the ISO/IEC 27001 Annex A controls. Is this acceptable?

A. Yes, organizations can incorporate additional controls from other sources

B. No, organizations must only implement the controls listed in Annex A

C. Yes, but only if the additional controls replace existing Annex A controls

Answer: A

Explanation

ISO/IEC 27001:2022 clause 6.1.3 (Information Security Risk Treatment) explicitly states:

"Organizations can design controls as required or identify them from any source."

Annex A provides a reference list, but it is not exhaustive. Organizations are encouraged to adopt additional controls if they are needed based on the results of risk assessment or contextual relevance. This supports flexibility and context-based tailoring of the ISMS.

Question #:199

An organization that is implementing the ISMS based on ISO/IEC 27001 has defined and communicated secure system architecture and engineering principles. However, there is no documented information related to these principles. Is this acceptable?

A. Yes, the standard requires organizations to only communicate secure system architecture and engineering principles

B. Yes, documented information related to secure system architecture and engineering principles is not directly required by the standard

C. No, documenting secure system architecture and engineering principles is required by the standard

Answer: B

Question #:200

Scenario 7: CyTekShield

CyTekShield based in Dublin. Ireland, is a cybersecurity consulting provider specializing in digital risk management and enterprise security solutions. After facing multiple security incidents. CyberTekShield formed expanded its information security team by bringing in Sadie and Niamh as part of the team. This team is structured into three key divisions: incident response, security architecture and forensics

Sadie will separate the demilitarized zone from CyTekShield's private network and publicly accessible resources, as part of implementing a screened subnet network architecture. In addition, Sadie will carry out comprehensive evaluations of any unexpected incidents, analyzing their causes and assessing their potential

impact. She also developed security strategies and policies. Whereas Niamh. a specialized expert in forensic investigations, will be responsible for creating records of different data for evidence purposes To do this effectively, she first reviewed the company's information security incident management policy, which outlines the types of records to be created, their storage location, and the required format and content for specific record types.

To support the process of handling of evidence related to information security events. CyTekShield has established internal procedures. These procedures ensure that evidence is properly identified, collected, and preserved within the company CyTekShield's procedures specify how to handle records in various storage mediums, ensuring that all evidence is safeguarded in its original state, whether the devices are powered on or off.

As part of CyTekShield's initiative to strengthen information security measures, Niamh will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments Upon completion of the risk assessment process, Niamh isresponsible to develop and implement a plan for treating information security risks and document the risk treatment results.

Furthermore, while implementing the communication plan for information security, the CyTekShield's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.CyTekShield uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by CyTekShield This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.

Question:

Has CyTekShield appropriately addressed the handling of evidence related to information security events?

A. No – as it does not include proper training for staff involved in evidence handling

B. Yes – it has appropriately addressed the handling of evidence

C. No – because the process of evidence acquisition was not fully detailed

Answer: B

Explanation

ISO/IEC 27037:2012 and ISO/IEC 27002:2022 Clause 8.16 –**Monitoring activities**and Clause 6.8 – **Information security event reporting**emphasize that:

“Evidence must be appropriately identified, collected, preserved, and protected to ensure it remains reliable and admissible in investigations.”

CyTekShield's approach covers all major evidence handling practices, including safeguarding devices in powered/unpowered states and defining content format/location, meeting accepted standards.

Question #:201

Question:

Which audit phase was conducted after the issue with the audit team was resolved?

A. Stage 1

B. Stage 2

C. Audit follow-up

Answer: B

Explanation

ISO/IEC 17021-1:2015 (used by certification bodies) defines:

- **Stage 1:**Review of documentation, readiness, scope
- **Stage 2:**On-site audit to assess effectiveness and implementation
- **Follow-up:**Only done post-audit if there are nonconformities requiring verification

In Scenario 10 (ProEBank), once the**auditor conflict was resolved**, the audit team**visited the site**to evaluate implementation—this is a clear**Stage 2 audit**activity.

Question #:202

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

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.

Question #:203

Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which serves as a structured framework and a guideline that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its 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 a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

Then, they evaluated the risks based on the risk evaluation criteria, where they decided to treat only the risks of the high-risk category. Additionally, they focused primarily on the unauthorized use of administrator rights

and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted.

Based on the scenario above, answer the following question:

Which risk analysis technique did the experts use to determine the level of risk? Refer to scenario 4.

A. Qualitative risk analysis

B. Semi-quantitative analysis

C. Quantitative risk analysis

Answer: A

Question #:204

Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which serves as a structured framework and a guideline that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its 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 a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

Then, they evaluated the risks based on the risk evaluation criteria, where they decided to treat only the risks of the high-risk category. Additionally, they focused primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted.

Based on the scenario above, answer the following question:

Based on scenario 4, from which source did TradeB's ISMS implementation draw its methodological framework?

A. ISO/IEC 27003

B. ISO 10006

C. COBIT 5

Answer: A

Question #:205

Company X restricted the access of the internal auditor of some of its documentation taking into account its confidentiality. Is this acceptable?

A. Yes. it is up to the company to determine what an internal auditor can access

B. Yes. confidential information should not be increased by internal auditors

C. No. restricting the internal auditor's access to offices and documentation can negatively affect the internal audit process

Answer: C

Question #:206

Scenario 9:

OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan 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."

However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.

Did OpenTech have a plan in place to implement permanent corrective action to address the identified nonconformities?

A. Yes, OpenTech had a comprehensive plan in place to implement permanent corrective actions

B. No, OpenTech did not have a clear plan to implement a permanent corrective action

C. No, OpenTech decided not to pursue this course of action

Answer: B

Question #:207

Scenario 9:

OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.

Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list

to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan 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."

However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.

Based on scenario 9, was it acceptable that the top management rejected the action plan submitted by Julia?

A. Yes, an action plan must be submitted to address each nonconformity separately

B. No, top management should have approved the action plan submitted by Julia

C. No, a general action plan can be submitted to address all nonconformities at once

Answer: A

Question #:208

Upon the risk assessment outcomes. Socket Inc. decided to:

• Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers

• Require the change of passwords at least once every 60 days

• Keep backup copies of files on IT-provided network drives

• Assign users to a separate network when they have access to cloud storage files storing customers' personal data.

Based on scenario 5. Socket Inc. decided to use cloud storage to store customers' personal data considering that the identified risks have low likelihood and high impact, is this acceptable?

A. Yes. because the calculated level of risk is below the acceptable threshold

B. No, because the impact of the identified risks is considered in he high

C. No. because the identified risks fall above the risk acceptable criteria threshold

Answer: B

Question #:209

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 theinformation 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.

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

Answer: B

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, the information security policy is a high-level document that defines the organization’s objectives, principles, and commitments regarding information security. The policy should be aligned with the organization’s strategic direction and context, and should provide a framework for setting information security objectives and establishing the ISMS. The policy should also be approved by top management, who are ultimately responsible for the ISMS and its performance. Therefore, after drafting the information security policy, the next step that Operaze’s ISMS implementation

team should take is to obtain top management's approval for the policy. This will ensure that the policy is consistent with the organization'svision and values, and that it has the necessary support and resources for its implementation and maintenance.

Question #:210

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

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.

Question #:211

The application used by an organization has a complicated user interface. What does the complicated user interface represent in this case?

A. An intrinsic vulnerability, since it is a characteristic of the asset

B. An extrinsic vulnerability, since it is fin external factor that impacts the asset

C. A type of threat, since it may result in an unwanted incident

Answer: A

Question #:212

Question:

Which statement regarding management reviews is correct?

A. Management reviews are carried out at various levels in the organization

B. Management reviews must be carried out monthly

C. Top management can delegate the ultimate responsibility of the management review process to individuals working for the organization

Answer: A

Explanation

ISO/IEC 27001:2022 Clause 9.3 –**Management Review**:

“Top management shall review the organization’s ISMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.”

While the**ultimate responsibility rests with top management**, reviews may be conducted at**multiple organizational levels**for broader visibility and alignment. ISO/IEC 27004 also supports reviews at tactical and operational levels.

There is**no requirement**for monthly reviews. Option C is incorrect, as**top management cannot fully delegate** the ultimate responsibility, only supporting roles.

Question #:213

Scenario 4: FinSecure

Finsecure is a financial institution based in Finland, providing services to a diverse clientele, encompassing retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, FinSecure has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of experts, FinSecure opted for a methodological framework, which serves as a structured framework that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts conducted a risk assessment, identifying all the supporting assets, which were the most tangible ones. They assessed the potential consequences and likelihood of various risks, determining the level of risks using a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process. These risks were categorized into nonnumerical levels (e g., very low, low. moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

After completing the risk assessment, the experts reviewed a selected number of the security controls from Annex A of ISO/IEC 27001 to determine which ones were applicable to the company's specific context. The decision to implement security controls was justified by the risk assessment results. Based on this review, they drafted the Statement of Applicability (SoA). They focused on treating only the high-risk category particularly addressing unauthorized use of administrator rights and system interruptions due to several hardware failures. To address these issues, they established a new version of the access control policy, implemented controls to manage and control user access, and introduced a control for ICT readiness to ensure business continuity.

Their risk assessment report indicated that if the implemented security controls reduce the risk levels to an acceptable threshold, those risks will be accepted

Question:

Did FinSecure identify information system components on which one or several business assets are based?

A. Yes – the company identified all supporting assets as part of the asset identification process

B. No – the company identified only the valuable information and some organizational processes

C. No – the company identified only business assets

Answer: A

Explanation

According to ISO/IEC 27001:2022 Clause 6.1.2 (c), a valid risk assessment must:

"Identify the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for information**within the scope of the ISMS**."

Supporting assets (like systems, devices, people, networks) are vital to identifying threats and assessing the impact on business assets (like data and processes). FinSecure identified all**supporting assets**, which are defined in ISO/IEC 27002:2022 Clause 5.9:

"An inventory of information and other associated assets (supporting assets) should be developed and maintained."

This confirms they met a key requirement of asset identification.

Question #:214

The Incident Response Team (IRT) has been notified of a potential compromise in the organization's network. Which type of services would be most appropriate for the IRT to provide in this situation?

A. Proactive services

B. Reactive services

C. Security quality management services

Answer: B

Question #:215

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

About Marks4sure.com

marks4sure.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@marks4sure.com
- Feedback: feedback@marks4sure.com
- Support: support@marks4sure.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.