PECB.ISO-IEC-27001-Lead-Implementer.v2026-07-14.q147

Exam Code:	ISO-IEC-27001-Lead-Implementer
Exam Name:	PECB Certified ISO/IEC 27001 Lead Implementer Exam
Certification Provider:	PECB
Free Question Number:	147
Version:	v2026-07-14
# of views:	200
# of Questions views:	1470
https://www.freepdfdumps.com/PECB.ISO-IEC-27001-Lead-Implementer.v2026-07-14.q147.html	

NEW QUESTION: 1
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 (LEAVE A REPLY)
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.
ISO/IEC 27006:2015, clauses 9.1.1, 9.1.2, and 9.2.1.

NEW QUESTION: 2
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. Strong AI
C. Machine learning
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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. Yes, Julia revised the action plan to ensure alignment with best practices
C. No, as action plans are typically expected to meet specified deadlines
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
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 (LEAVE A REPLY)
The secure removal or overwriting of data (data sanitization) is a technological control. It involves technical means to ensure that information stored on electronic media is securely erased so that it cannot be recovered.
"Media sanitization and secure erasure are technical measures designed to prevent unauthorized recovery of information from equipment prior to disposal or reuse."
- ISO/IEC 27001:2022, Annex A, Control 8.10 Storage media; ISO/IEC 27002:2022, 8.10

NEW QUESTION: 5
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 (LEAVE A REPLY)
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.
1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, clause 10.1, Nonconformity and corrective action.

NEW QUESTION: 6
Scenario 5: OperazeIT 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, OperazeIT implemented an information security management system (ISMS) based on ISO/IEC 27001.
In a collaborative effort involving the implementation team, OperazeIT 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 OperazeIT's commitment to information security.
OperazeIT'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 OperazeIT 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, OperazeIT initiated a comprehensive gap analysis as part of the ISMS implementation process. Rather than relying solely on internal assessments, OperazeIT 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 OperazeIT to identify vulnerabilities and areas for improvement with a higher degree of objectivity. Lastly, OperazeIT 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 OperazeIT establish to guarantee the proper operation of the ISMS?
A. Information security committee
B. Operational committee
C. Management committee
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
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. No, documenting secure system architecture and engineering principles is required by the standard
C. Yes, documented information related to secure system architecture and engineering principles is not directly required by the standard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
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. No, it should only retain documented information for risk assessment results
B. No, the information security risk treatment plan should be developed only by the top management
C. Yes, it complies with ISO/IEC 27001 requirements by implementing a risk treatment plan and documenting risk treatment results
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
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. Legal
B. Technical
C. Administrative
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
According to ISO/IEC 27000, which of the following best describes the possible scope of a management system?
A. It should cover the entire organization without exceptions
B. It can vary to include the entire organization or specific sections, depending on the needs
C. It is limited to IT infrastructure and cannot include non-technical departments
Answer: B (LEAVE A REPLY)
ISO/IEC 27001 and 27000 both allow organizations to define the scope of the ISMS according to their needs, including the entire organization, specific departments, business units, or locations.
"The scope of the ISMS can be as broad or narrow as the organization chooses, so long as boundaries are clearly defined and justified."
- ISO/IEC 27001:2022, Clause 4.3
- ISO/IEC 27000:2018, Section 2.2

NEW QUESTION: 11

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 (LEAVE A REPLY)

NEW QUESTION: 12
Which statement regarding residual risk is correct?
A. It can consist of unidentified risk.
B. It consists of only retained risk.
C. It excludes any risk that has been transferred through contracts or insurance.
Answer: A (LEAVE A REPLY)
Residual risk is defined in ISO/IEC 27000:2018 as the risk remaining after risk treatment. According to ISO
/IEC 27005:2022, residual risk can include risks that were not identified during the risk assessment process - meaning unidentified risks form part of the residual risk. This is because no risk assessment is exhaustive; unknown or emerging threats may exist outside the assessed scope. Option B is incorrect because residual risk is not limited to retained risk alone; it includes any risk remaining after all treatment options, including modification, sharing, and avoidance. Option C is incorrect because transferred risks (via insurance or contracts) still contribute to residual risk, as the transfer may be partial or incomplete. Therefore, the only fully correct statement is that residual risk can consist of unidentified risk, consistent with ISO/IEC 27005:
2022 risk management guidance.

NEW QUESTION: 13
According to ISO/IEC 27001, what shall the organization determine regarding monitoring and measurement?
Scenario 8: SecureLynx is one Of the largest cybersecurity advisory and consulting companies that helps private sector organizations prevent security threats. improve security systems. and achieve business SecureLynr is committed to complying with national and international standards to enhance the company'S resilience and credibility_ SecureLynx has Started implementing an ISMS based on ISO/IEC 27001 as part of its relentless pursuit of security.
As part of the internal audit activities. the top management reviewed and approved the audit objectives to assess the effectiveness of SecureLynx*s ISMS During the audit, the internal auditor evaluated whether top management Supports activities associated with the ISMS and if the toles and responsibilities Of relevant parties are Clearly defined. This rigorous examination is a testament to SecureLynx'S commitment to continuous improvernent and alignment of security measures with organizational goals.

SecureLynx employs an innovative dashboard that visually represents implemented processes and controls to ensure transparency and accountability within the Organization. This tool Offers stakeholders a real- time overview of security measures. empowering them to make informed decisions and swiftly respond to emerging threats. As part of this initiative, Paula was appointed to a new position entrusted with the responsibility Of collecting, recordlng, and Stoting data to measure the effectiveness Of the ISMS- Furthermore, SecureLynx conducts management reviews every six months to ensure its Systems are robust and continually improving. These reviews serve as a crucial mechanism for assessing the efficacy Of security measures and identifying areas for enhancement. SecureLynx's dedication to implementing and maintaining a robust ISMS exemplifies its commitment to innovation and Client satisfaction.
Based on the scenario above, answer the following question.
A. The number of attributes to be measured
B. The methods for monitoring, measurement, analysis, and evaluation
C. The frequency of analysis and evaluation
Answer: (SHOW ANSWER)
ISO/IEC 27001:2022, Clause 9.1 states that the organization shall determine the methods for monitoring, measurement, analysis, and evaluation as part of performance evaluation. This ensures that measurement results are valid, repeatable, and aligned with ISMS objectives.
"The organization shall determine... the methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results."
- ISO/IEC 27001:2022, Clause 9.1

NEW QUESTION: 14
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: (SHOW ANSWER)
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.
ISO/IEC 27001:2022, Annex A, control A.8.23.1
PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 21

NEW QUESTION: 15
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. integrity
B. Confidentiality
C. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 16

In addition to leading the new project involving sensitive client data, what is Sarah's role within the company? Refer to scenario 6.
Scenario 6: CB Consulting iS a reputable firm based in Dublin, Ireland. providing Strategic business Solutions to diverse clients, With a dedicated team Of professionals, CB Consulting prides itself on its commitment to excellence, integrity, and client satisfaction.
CB Consulting started implementing an ISMS aligned with ISOflEC 27001 as part of its ongoing commitment to enhancing its information security practices. Throughout this process, ensuring effective communication and adherence to establi Shed security protocols is essential.
Sarah, an employee at CB has been appointed as the head Of a new project focused on managing sensitive client data, Additionally, she is responsible for Overseeing activities during the response phase of incident management, including regular reporting to the incident manager of the incident management team and keeping key stakeholders informed. Meanwhile, CB Consulting has reassigned Tom to serve as the company's legal consultant.
CB Consulting has also reassigned Clare. formerly an IT security analyst, as their information security officer to oversee the implementation Of the ISMS and ensure compliance with ISO/IEC 27001. Clare's primary responsibility iS to conduct regular risk assessments. identlfy potential vulnerabilities, and implement appropriate Security measures to mitigate risks effectively. Clare has established a procedure Stating that information security risk assessments are conducted only when significant changes occur. playing a crucial role in strengthening the companys security posture and safeguarding against potential threats.
TO ensure it has a Competent workforce to meet information security Objectives, CB Consulting has implemented a process to and verify that all employees, including Sarah, Tom, and Clare, possess the necessary competence based on their education. training, or experience. Where gaps were identified, the company has taken specific actions such as providing additional training and mentoring. Additionally, CB Consulting retains documented information as evidence of the competencies requ.red and acquired.
CB Consulting has established a robust communication strategy aligned with industry standards to ensure secure and effective information exchange. It identified the requirements for communication on relevant issues. First, the company designated specific toles. Such as a public relations officer for external communication and a Security officer for internal matters, to manage sensitive issues like data breaches. Then. communication triggers, content. and recipients were carefully defined. with messages pre-approved by management where necessary. Lastly, dedicated channels were implemented to ensure the confidentiality and integrity of transmitted information.
Based on the scenario above, answer the following question.
CB Consulting prioritizes transparent and Substantive communication practices to foster trust, enhance Stakeholder engagement, and reinforce its commitment to information

security excellence. Which principle of effective communication is emphasized by this approach?
Transparency
A. CSIRT
B. Incident coordinator
C. Incident manager
Answer: B (LEAVE A REPLY)
Sarah is described as overseeing activities during the response phase of incident management, including regular reporting to the incident manager and keeping stakeholders informed. This fits the incident coordinator role-responsible for coordinating response activities, communication, and reporting.
"The incident coordinator is responsible for overseeing the incident response process, maintaining communications, and ensuring proper reporting and escalation."
- ISO/IEC 27035-1:2016, Section 6.4

NEW QUESTION: 17
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 (LEAVE A REPLY)

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.

1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 14 2: PECB, ISO/IEC

27001 Lead Implementer Course, Module 9: Internal Audit, slide 15

NEW QUESTION: 18

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.
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 (LEAVE A REPLY)
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's vision and values, and that it has the necessary support and resources for its implementation and maintenance.
ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 5.2 Policy
ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 12, Information security policy

NEW QUESTION: 19
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements1 ISO/IEC 27001 Lead Implementer Info Kit Continual Improvement For ISO 27001 Requirement 10.22

NEW QUESTION: 20
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4

NEW QUESTION: 21
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 accessible to the public at all times to maintain transparency
C. It must be sufficiently flexible to adapt to any identified change triggers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
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. Lean Six Sigma method
C. DMAIC (Define, Measure, Analyze, Improve, Control) method
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
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 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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2013, clause 7.2.2: Information security awareness, education and training ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC
27001
ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit ISO 27001 Security Awareness Training and Compliance - InfosecTrain1 ISO/IEC 27001 compliance and cybersecurity awareness training2 ISO 27001 Free Training | Online Course | British Assessment Bureau

NEW QUESTION: 24
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 (LEAVE A REPLY)

NEW QUESTION: 25
BioLooVitalis is a biopharmaceutical firm headquartered in Singapore Renowned for its pioneering work in the fie d of human therapeutics. BioLooVitalis places a strong emphasis on addressing critical healthcare concerns particularly in the domains of cardiovascular diseases, oncology bone health, and inflammation BioLooVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 77001 for the past two years. After noticing an increase m failed login attempts over several weeks. bioLooVitalis IT security learn reviewed log data, correlated it with user behavior patterns, and mapped it against known attach vectors to determine potential causes. Based on their findings, they prepared a technical report detailing the nature of the anomalies and submitted it to the compliance function. The compliance team then summarized the findings and presented them to the executive management during the quarterly ISMS performance review. To proactively track system behavior following the spike n failed login attempts. BioLooVitalis ' s IT security team configured a dashboard showing real time login activity. system response times, and end point availability across departments. This helped the team quickly detect abnormal behavior without waiting formal reporting cycles. Following The implementation of the real time access control dashboard BioLooVitalis internal audit team assessed whether the new processes and tools effectively reduced unauthorized access attempts and met both technical and policy-based requirements. Lastly, the internal auditors collected system-generated access logs, reviewed user access reports, and conducted interviews with IT personnel. These data sources helped them verify whether the new controls were functioning as intended and aligned with internal ISMS objectives.
Based on The scenario above, answer the following question.
Which measurement-related role did the compliance team perform at BioLooVitalis? Refer to scenario 8.
A. Information collector
B. Information analyst
C. Information communicator
Answer: C (LEAVE A REPLY)
In Scenario 8, the compliance team:
Received the technical report from IT security
Summarized the findings
Presented them to executive management during the ISMS review
This role aligns with information communication, not collection or analysis.
ISO/IEC 27001:2022 Clause 9.3 - Management review requires that performance information be communicated to top management in a structured and understandable manner.
Information collectors gather raw data (performed by IT security).
Information analysts interpret technical data (also performed by IT security).

Information communicators translate and present results to decision-makers (performed by compliance).

NEW QUESTION: 26
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 (LEAVE A REPLY)
The primary purpose of comparing actual performance against targets is to assess whether security objectives are being met. This is a direct requirement of ISO/IEC 27001:2022, Clause 9.1, which mandates monitoring, measurement, analysis, and evaluation to determine if objectives are achieved and to support continual improvement.
"The organization shall evaluate the performance and the effectiveness of the information security management system... and compare results with the objectives set."
- ISO/IEC 27001:2022, Clause 9.1

NEW QUESTION: 27
Scenario 9: SkyFleet specializes in air freight services, providing fast and reliable transportation solutions for businesses that need quick delivery of goods across long distances. Given the confidential nature of the information it handles, SkyFleet is committed to maintaining the highest information security standards. To achieve this, the company has had an information security management system (ISMS) based on ISO/IEC 27001 in operation for a year. To enhance its reputation, SkyFleet is pursuing certification against ISO/IEC
27001.
SkyFleet strongly emphasizes the ongoing maintenance of information security. In pursuit of this goal, it has established a rigorous review process, conducting in-depth assessments of the ISMS strategy every two years to ensure security measures remain robust and up to date. In addition, the company takes a balanced approach to nonconformities. For example, when employees fail to follow proper data encryption protocols for internal communications, SkyFleet assesses the nature and scale of this nonconformity. If this deviation is deemed minor and limited in scope, the company does not prioritize immediate resolution. However, a significant action plan was developed to address a major nonconformity involving the revamp of the company's entire data management system to ensure the protection of client data. SkyFleet entrusted the approval of this action plan to the employees directly responsible for implementing the changes. This streamlined approach ensures that those closest to the issues actively engage in the resolution process. SkyFleet's blend of innovation, dedication to information security, and adaptability has built its reputation as a key player in the IT and communications services sector.

Despite initially not being recommended for certification due to missed deadlines for submitting required action plans, SkyFleet undertook corrective measures to address these deficiencies in preparation for the next certification process. These measures involved analyzing the root causes of the delay, developing a corrective action plan, reassessing ISMS implementation to ensure compliance with ISO/IEC 27001 requirements, intensifying internal audit activities, and engaging with a certification body for a follow-up audit.
According to Scenario 9, has SkyFleet accurately established the appropriate frequency for reviewing its ISMS Strategy?
A. Yes. SkyFleet should review its ISMS every two years
B. No. Reviews are only necessary when significant changes in business operations occur
C. No. SkyFleet should conduct at least an annual review of the ISMS
Answer: C (LEAVE A REPLY)
ISO/IEC 27001:2022 requires that the ISMS and its controls are reviewed at planned intervals, and specifically, the management review of the ISMS must occur at least once per year.
Relevant Extracts:
"Top management shall review the organization's information security management system at planned intervals, at least once a year, to ensure its continuing suitability, adequacy and effectiveness."
- ISO/IEC 27001:2022, Clause 9.3 (Management Review)
The purpose of this annual review is to ensure that the ISMS remains aligned with the organization's needs, the context in which it operates, and the ever-evolving threat environment. Reviewing only every two years, as done by SkyFleet, does not meet the minimum frequency required by ISO/IEC 27001:2022.
Further, ISO/IEC 27001:2022 implementation guidelines clarify:
"The management review should be performed at planned intervals, and it is required at least once per year, but more frequent reviews may be needed in case of significant changes or incidents."
- ISO/IEC 27001:2022 Implementation Guidance, Section 9.3
References:
ISO/IEC 27001:2022, Clause 9.3 (Management Review)
ISO/IEC 27001:2022 Implementation Guidance, Section 9.3
Summary:
SkyFleet's current practice of reviewing its ISMS strategy every two years does not meet ISO/IEC 27001:
2022 requirements. The ISMS must be reviewed at least annually; thus, the correct answer is:
C). No. SkyFleet should conduct at least an annual review of the ISMS

NEW QUESTION: 28

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. Boundary control services
B. Integrity services
C. Access control services
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
Scenario 8: SecureLynx is one Of the largest cybersecurity advisory and consulting companies that helps private sector organizations prevent security threats. improve security systems. and achieve business SecureLynr is committed to complying with national and international standards to enhance the company'S resilience and credibility_ SecureLynx has Started implementing an ISMS based on ISO/IEC 27001 as part of its relentless pursuit of security.
As part of the internal audit activities. the top management reviewed and approved the audit objectives to assess the effectiveness of SecureLynx*s ISMS During the audit, the internal auditor evaluated whether top management Supports activities associated with the ISMS and if the toles and responsibilities Of relevant parties are Clearly defined. This rigorous examination is a testament to SecureLynx'S commitment to continuous improvernent and alignment of security measures with organizational goals.
SecureLynx employs an innovative dashboard that visually represents implemented processes and controls to ensure transparency and accountability within the Organization. This tool Offers stakeholders a real- time overview of security measures. empowering them to make informed decisions and swiftly respond to emerging threats. As part of this initiative, Paula was appointed to a new position entrusted with the responsibility Of collecting, recordlng, and Stoting data to measure the effectiveness Of the ISMS-
Furthermore, SecureLynx conducts management reviews every six months to ensure its Systems are robust and continually improving. These reviews serve as a crucial mechanism for assessing the efficacy Of security measures and identifying areas for enhancement. SecureLynx's dedication to implementing and maintaining a robust ISMS exemplifies its commitment to innovation and Client satisfaction.
Based on the scenario above, answer the following question.
Based on scenario 8, which internal audit activity is the internal auditor at SecureLynx performing?
A. Evaluation of the ISMS governance
B. Evaluation of the information security objectives
C. Evaluation of the risk management process
Answer: A (LEAVE A REPLY)

The internal auditor is evaluating whether top management supports ISMS activities and whether roles and responsibilities are clearly defined. This specifically pertains to ISMS governance-assessing the effectiveness of management commitment and the governance structure that supports the ISMS.
"Internal audits should address the governance of the ISMS, including top management commitment, allocation of roles and responsibilities, and organizational support."
- ISO/IEC 27001:2022, Clause 9.2.1; ISO/IEC 27007:2020, Clause 6.2.2

NEW QUESTION: 30
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the
[^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
In scenario 1, HealthGenic experienced a number of service interruptions due to the loss of functionality of the software. Which principle of information security has been affected in this case?
A. Availability
B. Confidentiality
C. Integrity
Answer: A (LEAVE A REPLY)
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.
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.13.

NEW QUESTION: 31

How can SkyFleet demonstrate its ongoing commitment to continual improvement in information security?

A. By letting employees take independent action ensures swift problem resolution

B. By outsourcing its information security responsibilities to a third-party vendor

C. By publishing an annual report on information security performance

Answer: (SHOW ANSWER)

Publishing an annual report on information security performance is a tangible way to demonstrate ongoing commitment to continual improvement. This aligns with ISO/IEC 27001 requirements for continual improvement (Clause 10.2) and transparency regarding ISMS effectiveness.

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

- ISO/IEC 27001:2022, Clause 10.2

NEW QUESTION: 32

NoAVision is a mid-sized cybersecurity solutions provider based in Tartu, Estonia, with satellite offices in Stockholm and Berlin. The company specializes in secure cloud hosting, identity and access management (IAM), and digital certificate lifecycle management. Its clients span the government, financial services, and healthcare sectors. To have a structured approach to safeguarding sensitive information, NoAVision decided to implement an ISMS based on ISO/IEC 27001. During risk assessment, the security team at NoAVision identified two critical vulnerabilities: inadequate maintenance and faulty installation of data storage media, and the absence of mechanisms to confirm the successful transmission and receipt of internal communications. These weaknesses posed threats to data integrity and availability, prompting the company to prioritize remediation.

What category of vulnerabilities did NoAVision identify during its risk assessment?

A. Software and application

B. Hardware and network

C. Legal and compliance

Answer: B (LEAVE A REPLY)

According to ISO/IEC 27005:2022, vulnerabilities are categorized into types such as hardware, software, network, personnel, and organizational. In this scenario, NoAVision identified: (1) inadequate maintenance and faulty installation of data storage media - a hardware vulnerability, and (2) absence of mechanisms to confirm the successful transmission and receipt of communications - a network/communication vulnerability. Both fall squarely within the hardware and network vulnerability category. Software vulnerabilities involve application flaws or coding defects, which are not described here. Legal and compliance vulnerabilities relate to regulatory gaps. The scenario explicitly references physical storage media and communication channel weaknesses, confirming the hardware and network classification per ISO/IEC
27005 vulnerability taxonomy.

NEW QUESTION: 33
Scenario 1: NobleFind is an online retailer specializing in high-end, custom-design furniture. The company offers a wide range of handcrafted pieces tailored to meet the needs of residential and commercial clients.
NobleFind also provides expert design consultation services. Despite NobleFind ' s efforts to keep its online shop platform secure, the company faced persistent issues, including a recent data breach. These ongoing challenges disrupted normal operations and underscored the need for enhanced security measures. The designated IT team quickly responded to resolve the problem. To address these issues, NobleFind decided to implement an Information Security Management System (ISMS) based on ISO/IEC 27001 to improve security, protect customer data, and ensure the stability of its services.
In addition to its commitment to information security, NobleFind focuses on maintaining the accuracy and completeness of its product data. This is ensured by carefully managing version control, checking information regularly, enforcing strict access policies, and implementing backup procedures. Moreover, product details and customer designs are accessible only to authorized individuals, with security measures such as multi- factor authentication and data access policies.
NobleFind has implemented an incident investigation process within its ISMS, as part of its comprehensive approach to information security. Additionally, it has established record retention policies to ensure that online information about each product and client information remains readily accessible and usable on demand for authorized entities.
NobleFind established an information security policy offering clear guidelines for safeguarding historical data. It also insisted that personnel sign confidentiality agreements and were committed to recruiting only qualified individuals. Additionally, NobleFind implemented measures for monitoring the resources used by its systems, reviewing user access rights, and conducting a thorough analysis of audit logs to swiftly identify and address any security anomalies.
With its ISMS in place, NobleFind maintains and safeguards documented information, encompassing a wide range of data, records, and specifications. This documented

information is vital to its operations, ensuring the security and integrity of customer data, historical records, and financial information.
According to scenario 1, which detective control did NobleFind implement?
A. Enforcing strict access policies
B. Conducting a thorough analysis of audit logs
C. Implementing an incident investigation process
D. Implementing backup procedures
Answer: (SHOW ANSWER)
Detective controls are designed to identify and detect undesirable events or incidents that have occurred so that appropriate corrective actions can be taken. ISO/IEC 27001:2022 and its implementation guidance define detective controls as mechanisms that " identify the occurrence of events or incidents and provide evidence or alerts " (see ISO/IEC 27002:2022, Introduction 0.2, and 6.8, " Audit logging ").
Conducting a thorough analysis of audit logs is a classic detective control. By regularly reviewing audit logs, an organization can identify suspicious activities, policy violations, or operational anomalies that may indicate a security incident.
ISO/IEC 27001:2022, Annex A, A.8.15 (Logging):
" Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed. " ISO/IEC 27002:2022, 8.15 (Logging):
" Regular review and analysis of logs should be performed to detect and respond to inappropriate or anomalous activities. " References:
ISO/IEC 27001:2022, Annex A, A.8.15
ISO/IEC 27002:2022, 8.15 and Introduction 0.2

NEW QUESTION: 34
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 (LEAVE A REPLY)

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.

ISO/IEC 27001:2022, clause 6.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 10, slide 8.

NEW QUESTION: 35

NeuroTrustMed is a leading medical technology company based in Seoul, South Korea. The company specializes in developing AI-assisted neuroimaging solutions used in early diagnosis and treatment planning for neurological disorders. As a data-intensive company handling sensitive patient health records and medical research data, NeuroTrustMed places a strong emphasis on cybersecurity and regulatory compliance. The company has maintained an ISO/IEC 27001-certified ISMS for the past three years. It continuously reviews and improves its ISMS to address emerging threats, support innovation in medical diagnostics, and maintain stakeholder trust. As part of its commitment to continual improvement, NeuroTrustMed actively tracks potential nonconformities, performs root-cause analyses, implements corrective and preventive actions, and ensures all changes are documented and aligned with the company's strategic objectives. When a new data protection regulation came into effect affecting cross-regional data handling, the information security team conducted a gap assessment between current policies and the new regulation. Then, it updated relevant documentation and processes to meet compliance. Following these revisions, NeuroTrustMed updated the ISMS documentation and added a new entry in the improvement register. The register, maintained in the form of a structured spreadsheet, included a unique change number, a description of the update, and a high-priority classification due to legal compliance, the dates of initiation and completion, and the sign-off by the information security manager. Around the same period, during a scheduled management review, the information security team also identified a pattern of onboarding errors. While these had not resulted in any data breaches, they posed a risk of unauthorized access. In response, the onboarding procedure was revised and an automated verification step was added to ensure accuracy before access is granted. To understand the underlying cause, the team collected data on the provisioning

process. They analyzed process logs, interviewed onboarding staff, and traced access errors back to a misconfigured step in the HR-to-IT handover workflow. The team validated this finding through test cases before implementing any changes. Once confirmed, the information security team documented the nonconformity in the ISMS log. The documentation included a description of the issue, impacted systems, affected users, and a brief risk assessment of potential consequences related to access management. Based on the scenario above, answer the following question.
Which discipline of the 8D method did the information security team apply in the last paragraph of scenario 9?
A. Develop an interim containment plan
B. D4 - Identify potential root cause(s)
C. D6- Implement detective actions
Answer: B (LEAVE A REPLY)
In the last paragraph of Scenario 9, the information security team at NeuroTrustMed applied Discipline D4 of the 8D (Eight Disciplines) problem-solving method, which focuses on identifying and verifying the root cause (s) of a problem. Therefore, Option B is the correct answer.
The scenario explicitly states that the team:
Collected data on the provisioning process
Analyzed process logs
Interviewed onboarding staff
Traced access errors back to a misconfigured step in the HR-to-IT handover workflow
Validated the finding through test cases before implementing changes These activities are textbook examples of D4 - Root Cause Analysis, where the objective is to move beyond symptoms and determine the true underlying cause of the nonconformity.
This aligns directly with ISO/IEC 27001:2022 Clause 10.2 - Nonconformity and corrective action, which requires organizations to:
"evaluate the need for action to eliminate the cause(s) of nonconformity, in order that it does not recur." Option A (Develop an interim containment plan) corresponds to D3, which would involve temporary measures to limit impact. This is not what the scenario describes. Option C (D6 - Implement corrective actions) occurs later, after root cause identification and validation. The scenario explicitly states that validation happened before implementing any changes, confirming the team was still in D4.

NEW QUESTION: 36
NoAVision is a mid-sized cybersecurity solutions provider based in Tartu, Estonia. The security team identified a threat scenario involving the forging of user rights within the IAM system, which could enable unauthorized individuals to escalate privileges and access restricted data. Recognizing this as a serious threat, the team categorized it under a specific threat type that required targeted mitigation.

According to Scenario 1, what type of risk source does the threat identified by NoAVision have?

A. Accidental

B. Environmental

C. Deliberate

Answer: (SHOW ANSWER)

ISO/IEC 27005:2022 classifies threat sources into three types: accidental (unintentional human errors), environmental (natural events, infrastructure failures), and deliberate (intentional, malicious actions by threat agents). The scenario describes the forging of user rights within the IAM system to escalate privileges and gain unauthorized access to restricted data. Forging is an intentional, calculated act performed by a malicious actor - this clearly qualifies as a deliberate threat source. Accidental threats involve unintended mistakes without malicious intent. Environmental threats involve natural disasters or infrastructure issues. Deliberate threats, as defined in ISO/IEC 27005, include unauthorized access, data theft, sabotage, and manipulation - all applicable to privilege escalation attacks on IAM systems.

NEW QUESTION: 37

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 (LEAVE A REPLY)

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).
References:
ISO/IEC 27002:2022 Clause 3.1.7, 3.1.13
ISO/IEC 27000:2018 definitions of CIA principles==========

NEW QUESTION: 38
Scenario 6: CB Consulting iS a reputable firm based in Dublin, Ireland. providing Strategic business Solutions to diverse clients, With a dedicated team Of professionals, CB Consulting prides itself on its commitment to excellence, integrity, and client satisfaction. CB Consulting started implementing an ISMS aligned with ISOflEC 27001 as part of its ongoing commitment to enhancing its information security practices. Throughout this process, ensuring effective communication and adherence to establi Shed security protocols is essential.
Sarah, an employee at CB has been appointed as the head Of a new project focused on managing sensitive client data, Additionally, she is responsible for Overseeing activities during the response phase of incident management, including regular reporting to the incident manager of the incident management team and keeping key stakeholders informed. Meanwhile, CB Consulting has reassigned Tom to serve as the company's legal consultant.
CB Consulting has also reassigned Clare. formerly an IT security analyst, as their information security officer to oversee the implementation Of the ISMS and ensure compliance with ISO/IEC 27001. Clare's primary responsibility iS to conduct regular risk assessments. identlfy potential vulnerabilities, and implement appropriate Security measures to mitigate risks effectively. Clare has established a procedure Stating that information security risk assessments are conducted only when significant changes occur. playing a crucial role in strengthening the companys security posture and safeguarding against potential threats.
TO ensure it has a Competent workforce to meet information security Objectives, CB Consulting has implemented a process to and verify that all employees, including Sarah, Tom, and Clare, possess the necessary competence based on their education. training, or experience. Where gaps were identified, the company has taken specific actions such as providing additional training and mentoring. Additionally, CB Consulting retains documented information as evidence of the competencies requ.red and acquired.
CB Consulting has established a robust communication strategy aligned with industry standards to ensure secure and effective information exchange. It identified the requirements for communication on relevant issues. First, the company designated specific

toles. Such as a public relations officer for external communication and a Security officer for internal matters, to manage sensitive issues like data breaches. Then. communication triggers, content. and recipients were carefully defined. with messages pre-approved by management where necessary. Lastly, dedicated channels were implemented to ensure the confidentiality and integrity of transmitted information.
Based on the scenario above, answer the following question.
CB Consulting prioritizes transparent and Substantive communication practices to foster trust, enhance Stakeholder engagement, and reinforce its commitment to information security excellence. Which principle of effective communication is emphasized by this approach?
Transparency
CB Consulting prioritizes transparent and substantive communication practices to foster trust, enhance stakeholder engagement, and reinforce its commitment to information security excellence. Which principle of effective communication is emphasized by this approach?
A. Transparency
B. Clarity
C. Timeliness
Answer: A (LEAVE A REPLY)
Transparent communication involves openly sharing relevant information, fostering trust, and enhancing stakeholder engagement. ISO/IEC 27001:2022 (and ISO/IEC 27003:2017, Clause 8.6) emphasize transparency as a best practice in both internal and external communication to reinforce organizational trust and security culture.
"Transparent communication ensures that all relevant information is available to stakeholders, enhancing trust and supporting the objectives of information security."
- ISO/IEC 27001:2022, Clause 7.4; ISO/IEC 27003:2017, Clause 8.6

NEW QUESTION: 39
What service did Auto Tsaab implement to manage and protect information effectively?
A. Cryptographic services
B. Access control services
C. Integrity services
D. Backup services
Answer: C (LEAVE A REPLY)
The scenario states that Auto Tsaab "established automated checking systems that detect and correct corruption... improved its ability to maintain data accuracy and consistency." These features correspond to integrity services, which protect information from unauthorized alteration and ensure accuracy and consistency.
"Integrity: property of accuracy and completeness. Integrity services protect information from unauthorized alteration or destruction."
- ISO/IEC 27000:2018, 3.8;

- ISO/IEC 27001:2022, Clause 6.1.2, Annex A controls on data integrity

NEW QUESTION: 40
In the SABSA framework, which layer is concerned with viewing the services at a high level?
A. Component security architecture
B. Physical security architecture
C. Logical security architecture
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Scenario 4: UX Software, a company specializing in L.JXfUI design. QA and software testing. and mobile application development. recognized the need to improve its information security measures, As such. the company implemented an ISMS based on ISO/IEC 27001- This strategic move aimed to enhance the confidentiality. availability, and integrity Of information shared internally and externally, aligning with industry standards and best practices.
The integration of ISMS into UX Software ' s existing processes and ensuring that these processes are adjusted in accordance with the framework of ISMS signified an important milestone. underscoring the organization ' S commitment to information security. UX Software meticulously tailored these procedures to align with the ISMS framework, ensuring they ate contextually and culturally appropriate while avoiding mismatches. This proactive stance reassured their employees and instilled confidence in their clients, ensuring the protection of sensitive data throughout their operations.
UX Software ' S top management took action to define the Scope Of their ISMS to adhere to ISOflEC 27003 to drive this initiative forward. Sven, a key member Of the top management team at UX Software. assumed the role of project sponsor. a critical position responsible for ensuring the execution of ISMS implementation with adequate resources. Sven ' s leadership was pivotal in steering the project towards compliance with 27001, thus elevating the organization ' s information security posture to the highest level-
In parallel with their dedication to information security. UX Software incorporated the technical specifications Of security controls within the justification section Of their Statement Of Applicability This approach demonstrated their Commitment to meeting ISO/IEC 27001 requirements and ensured thorough documentation and justification Of Security controls, thereby Strengthening the overall Security framework Of the organization. Additionally. UX Software established a committee responsible for ensuring the effectiveness of correctrve actions, managing the ISMS documented information, and continually improving the ISMS while addressing nonconformities.
By implementing an ISMS based on ISO/IEC 27001, UX Software improved its information security and reinforced its position as a reliable partner. This dedication to information security serves as a testament to UX Software ' s commitment to delivering high-quality

software solutions while safeguarding the interests of its internal stakeholders and valued clients.
According to Scenario 4, UX Software decided to use the guidelines of ISO/IEC 27003 to define the scope of the ISMS. Is the scope defined in accordance with these guidelines?
A. Yes, they defined the scope according to ISO/IEC 27003
B. No, they should have followed a multi-step approach involving management representatives and refinement
C. No, they should have determined the final scope first
Answer: (SHOW ANSWER)
The scenario notes that "UX Software's top management took action to define the Scope of their ISMS to adhere to ISO/IEC 27003." ISO/IEC 27003 provides guidance for defining the scope of an ISMS in accordance with ISO/IEC 27001 requirements.
"The organization should establish the ISMS scope based on the guidance in ISO/IEC 27003, ensuring that it reflects the context, interested parties, and business needs."
- ISO/IEC 27003:2017, Clause 6.2; ISO/IEC 27001:2022, Clause 4.3

NEW QUESTION: 42
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 (LEAVE A REPLY)
An internal audit charter is a formal document that defines the purpose, authority, and responsibility of the internal audit function within the organization. Its primary purpose is to explain how the internal audit adds value and supports the organization in achieving its objectives.
"The internal audit charter should define the purpose, authority, and responsibility of the internal audit activity, including its role in helping the organization achieve its objectives."
- ISO/IEC 27001:2022, Clause 9.2; ISO 19011:2018, Clause 5.1; IIA International Standards

NEW QUESTION: 43
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 twice a year, regardless of significant changes
C. No, as it should perform them at planned intervals as well
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Scenario 2: NyvMarketing is a marketing firm that provides different services to clients across various industries. With expertise in digital marketing. branding, and market

research, NyvMarketing has built a solid reputation for delivering innovative and impactful marketing campaigns. With the growing Significance Of data Security and information protection within the marketing landscape, the company decided to implement an ISMS based on 27001.

While implementing its ISMS NyvMarketing encountered a significant challenge; the threat of insufficient resources, This challenge posed a risk to effectively executing its ISMS objectives and could potentially undermine the company'S efforts to safeguard Sensitive information. TO address this threat, NyvMarketing adopted a proactive approach by appointing Michael to manage the risks related to resource Constraints.

Michael was pivotal in identifying and addressing resource gaps. strategizing risk mitigation. and allocating resources effectively for ISMS implementation at NyvMarket*ng, strengthening the company's resilience against resource challenges.

Furthermore, NyvMarketing prioritized industry standards and best practices in information security, diligently following ISOfIEC 27002 guidelines. This commitment, driven by excellence and ISO/IEC 27001 requirements, underscored NyvMafketinq*s dedication to upholding the h*ghest Standards Of information security governance.

While working on the ISMS implementation, NyvMarketing opted to exclude one Of the requirements related to competence (as stipulated in ISO/IEC 27001, Clause 7.2). The company believed that its existing workforce possessed the necessary competence to fulfill ISMS*telated tasks_ However, it did not provide a valid justification for this omission.

Moreover. when specific controls from Annex A Of ISO/IEC 27001 were not implemented. NyvMarketing neglected to provide an acceptable justification for these exclusions.

During the ISMS implementation, NFMarketing thoroughly assessed vulnerabilities that could affect its information Security These vulnerabilities included insufficient maintenance and faulty installation Of storage media, insufficient periodic replacement schemes for equipment, Inadequate software testing. and unprotected communication lines.

Recognizing that these vulnerabilities could pose risks to its data security. NBMarketing took steps to address these specific weaknesses by implementing the necessary controls and countermeasures- Based on the scenario above, answer the following question.

In the scenario 2. NyvMarketing faced the threat of insufficient resources during the ISMS implementation. In which of the following categories does this threat fall?

According to scenario 2, did NyvMarketing take actions that comply with ISO/IEC 27001 regarding the implementation of Annex A controls?

A. Yes, NyvMarketing's actions taken during the implementation of Annex A controls comply with ISO

/IEC 27001

B. No, NyvMarketing's actions did not comply with ISO/IEC 27001 since it excluded one of the Annex A controls without providing justifications

C. No, NyvMarketing's actions did not comply with ISO/IEC 27001 since it should have included all the Annex A controls

D. Yes, because ISO/IEC 27002 allows for exclusions

Answer: (SHOW ANSWER)
ISO/IEC 27001:2022 requires that when an organization excludes any Annex A controls, it must provide a valid justification for each exclusion (Clause 6.1.3.d). Simply omitting a control or a requirement (such as competence, Clause 7.2) without documented justification is a non-conformance with ISO/IEC 27001. All exclusions must be justified and based on the results of the risk assessment and risk treatment process.
"Any controls omitted must be justified, and such justification must be documented as part of the Statement of Applicability."
- ISO/IEC 27001:2022, Clause 6.1.3 d)
"The organization shall produce a Statement of Applicability that... justifies inclusions and exclusions of controls."
- ISO/IEC 27001:2022, Clause 6.1.3 d)

NEW QUESTION: 45
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: (SHOW ANSWER)

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.
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 9.3 PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001 PECB, ISO/IEC 27001 Lead Implementer Exam Preparation Guide, Section 9: Performance evaluation, measurement, and monitoring of an ISMS based on ISO/IEC 27001

NEW QUESTION: 46
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 availability toward their users
B. Lack of communication strategies
C. Lack of transparency toward their users
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022, Clause 7.2 Competence and Clause 7.3 Awareness
ISO/IEC 27002:2022, Clause 7.2.2 Information security awareness, education and training
PECB ISO/IEC 27001 Lead Implementer Course, Module 4: Leadership, Commitment, and Support of Top Management.

NEW QUESTION: 48

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 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: (SHOW ANSWER)

NEW QUESTION: 49
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. Software as a Service
B. Infrastructure as a Service
C. Platform as a Service
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following standards provides the requirements and guidelines for establishing a privacy information management system (PIMS)?
A. ISO/IEC 27701
B. ISO/IEC 27009
C. ISO/IEC 27011
Answer: A (LEAVE A REPLY)
ISO/IEC 27701 is the international standard that extends ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. It specifies the requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).
"ISO/IEC 27701:2019 - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines."
- ISO/IEC 27701:2019, Foreword

NEW QUESTION: 51
What is the first phase in the information security policy development life cycle?
A. Policy construction
B. Policy implementation
C. Risk assessment
D. Policy planning / Needs assessment
Answer: D (LEAVE A REPLY)
(Note: If your actual options are only the three above, then the correct one in the standard framework is usually " Policy planning / Needs assessment " or " Policy planning. " If that ' s not available, " Policy construction " may be the default in your question bank, but it does not align with ISO best practice.) The information security policy development life cycle typically starts with a policy planning or needs assessment phase, where organizational needs, objectives, and requirements are determined before constructing the policy. Risk assessment often occurs during this initial phase to inform policy direction.
"The policy development process should start by identifying needs and requirements before constructing and implementing the policy."
- ISO/IEC 27002:2022, 5.1; ISO/IEC 27003:2017, Clause 8.2

NEW QUESTION: 52
How does the Statement of Applicability (SoA) contribute to the certification audit process?
A. It provides a comprehensive overview of security incidents for external auditors

B. It provides a reference for external auditors, listing pertinent controls relevant to the ISMS
C. It provides a checklist for top management to ensure the implementation of relevant controls to the ISMS
Answer: B (LEAVE A REPLY)
The Statement of Applicability (SoA) serves as the primary reference document for auditors during the certification audit. It lists all Annex A controls, justifies inclusions and exclusions, and documents implementation status for each control.
"The SoA shall include justification for inclusions and exclusions of controls and state their implementation status. The SoA provides auditors with the definitive list of controls relevant to the ISMS."
- ISO/IEC 27001:2022, Clause 6.1.3 d

NEW QUESTION: 53
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 (LEAVE A REPLY)

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

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

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

NEW QUESTION: 54

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 (LEAVE A REPLY)

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.

References:

ISO/IEC 27001:2022 Clause 6.1.3 Note 1 and Note 3

ISO/IEC 27002:2022 Introduction 0.1 and Clause 0.4==========

NEW QUESTION: 55

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. Implementing access points
B. Using appropriate entry controls
C. Verifying items of equipment containing storage media
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Scenario 2: NyvMarketing is a marketing firm that provides different services to clients across various industries. With expertise in digital marketing. branding, and market research, NyvMarketing has built a solid reputation for delivering innovative and impactful marketing campaigns. With the growing Significance Of data Security and information protection within the marketing landscape, the company decided to implement an ISMS based on 27001.
While implementing its ISMS NyvMarketing encountered a significant challenge; the threat of insufficient resources, This challenge posed a risk to effectively executing its ISMS objectives and could potentially undermine the company ' S efforts to safeguard Sensitive information. TO address this threat, NyvMarketing adopted a proactive approach by appointing Michael to manage the risks related to resource Constraints.
Michael was pivotal in identifying and addressing resource gaps. strategizing risk mitigation. and allocating resources effectively for ISMS implementation at NyvMarket*ng, strengthening the company ' s resilience against resource challenges.
Furthermore, NyvMarketing prioritized industry standards and best practices in information security, diligently following ISOfIEC 27002 guidelines. This commitment, driven by excellence and ISO/IEC 27001 requirements, underscored NyvMafketinq*s dedication to upholding the h*ghest Standards Of information security governance.
While working on the ISMS implementation, NyvMarketing opted to exclude one Of the requirements related to competence (as stipulated in ISO/IEC 27001, Clause 7.2). The company believed that its existing workforce possessed the necessary competence to fulfill ISMS*telated tasks_ However, it did not provide a valid justification for this omission.
Moreover. when specific controls from Annex A Of ISO/IEC 27001 were not implemented. NyvMarketing neglected to provide an acceptable justification for these exclusions.
During the ISMS implementation, NFMarketing thoroughly assessed vulnerabilities that could affect its information Security These vulnerabilities included insufficient maintenance and faulty installation Of storage media, insufficient periodic replacement schemes for equipment, Inadequate software testing. and unprotected communication lines.
Recognizing that these vulnerabilities could pose risks to its data security. NBMarketing took steps to address these specific weaknesses by implementing the necessary controls and countermeasures- Based on the scenario above, answer the following question.
In the scenario 2. NyvMarketing faced the threat of insufficient resources during the ISMS implementation. In which of the following categories does this threat fall?
According to scenario 2, what is Michael's role at NyvMarketing?
A. Risk owner

B. Incident manager
C. Crisis manager
D. ISMS auditor
Answer: A (LEAVE A REPLY)
A risk owner is defined in ISO/IEC 27001:2022 as the person or entity with the accountability and authority to manage a risk. In the scenario, Michael was appointed to manage the risks related to resource constraints- identifying gaps, strategizing mitigation, and allocating resources-demonstrating that he is assigned responsibility and authority for a specific risk area.
" Risk owner: person or entity with the accountability and authority to manage a risk. "
- ISO/IEC 27000:2018, 3.32 (referenced by ISO/IEC 27001:2022, Section 3)
" The organization shall assign risk owners to ensure that risks are managed. "
- ISO/IEC 27001:2022, Clause 6.1.2

NEW QUESTION: 57
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 (LEAVE A REPLY)
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.
References:
ISO/IEC 27002:2022 Clause 5.1 - Policies for information security==========

NEW QUESTION: 58
Which of the following practices Indicates that Company A has Implemented clock synchronization?
A. Information processing systems are coordinated according to an approved time source
B. Suspected information security events are reported in a timely manner through an appropriate channel

C. Logs that record activities and other relevant events are stored and analyzed
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Scenario 4: UX Software, a company specializing in L.JXfUI design. QA and software testing. and mobile application development. recognized the need to improve its information security measures, As such. the company implemented an ISMS based on ISO/IEC 27001- This strategic move aimed to enhance the confidentiality. availability, and integrity Of information shared internally and externally, aligning with industry standards and best practices.
The integration of ISMS into UX Software's existing processes and ensuring that these processes are adjusted in accordance with the framework of ISMS signified an important milestone. underscoring the organization'S commitment to information security. UX Software meticulously tailored these procedures to align with the ISMS framework, ensuring they ate contextually and culturally appropriate while avoiding mismatches. This proactive stance reassured their employees and instilled confidence in their clients, ensuring the protection of sensitive data throughout their operations.
UX Software'S top management took action to define the Scope Of their ISMS to adhere to ISOflEC 27003 to drive this initiative forward. Sven, a key member Of the top management team at UX Software. assumed the role of project sponsor. a critical position responsible for ensuring the execution of ISMS implementation with adequate resources. Sven's leadership was pivotal in steering the project towards compliance with
27001, thus elevating the organization's information security posture to the highest level- In parallel with their dedication to information security. UX Software incorporated the technical specifications Of security controls within the justification section Of their Statement Of Applicability This approach demonstrated their Commitment to meeting ISO/IEC 27001 requirements and ensured thorough documentation and justification Of Security controls, thereby Strengthening the overall Security framework Of the organization. Additionally. UX Software established a committee responsible for ensuring the effectiveness of correctrve actions, managing the ISMS documented information, and continually improving the ISMS while addressing nonconformities.
By implementing an ISMS based on ISO/IEC 27001, UX Software improved its information security and reinforced its position as a reliable partner. This dedication to information security serves as a testament to UX Software's commitment to delivering high-quality software solutions while safeguarding the interests of its internal stakeholders and valued clients.
Based on scenario 4, the developers of UX Software incorporated the technical specifications of security controls within the justification section of their Statement of Applicability. Is this recommended?
A. Yes, the technical specifications of security controls must be included within the justification section

B. No, the justification section should encompass the rationale for the inclusion and exclusion of each security control
C. No, the justification section should concisely overview previous software projects
Answer: (SHOW ANSWER)
The justification section of the Statement of Applicability (SoA) is specifically intended to document the rationale for the inclusion or exclusion of each Annex A control, as well as its implementation status.
Technical specifications can be referenced elsewhere but do not belong in the justification section.
"The Statement of Applicability shall contain... justification for inclusions and exclusions of controls."
- ISO/IEC 27001:2022, Clause 6.1.3 d
"The justification must clearly explain why each control is included or excluded, not technical implementation details."
- ISO/IEC 27001:2022, Clause 6.1.3, ISO/IEC 27002:2022, 6.1.3

NEW QUESTION: 60
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022 Lead Implementer Training Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2

NEW QUESTION: 61
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: (SHOW ANSWER)
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 information assets. 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.
ISO/IEC 27001:2022 Lead Implementer Course Content, Module 5: Introduction to Information Security Controls based on ISO/IEC 27001:20221; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 3.6: Confidentiality2; ISO/IEC 27002:2022 Code of practice for information security controls, Clause 9.4: Access control3

NEW QUESTION: 62
Why should the security testing processes be defined and implemented in the development life cycle?
A. To validate if information security requirements are met when applications are deployed to the production environment
B. To Identify organizational assets and define appropriate protection responsibilities
C. To protect the production environment and data from compromise by development and test activities
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following processes may involve increasing risk in order to pursue an opportunity?
A. Risk analysis
B. Risk identification
C. Risk treatment
Answer: (SHOW ANSWER)

NEW QUESTION: 64
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 controls did Socket Inc. implement by conducting pre-employment background checks? Refer to scenario 3.
A. Annex A 6.4 Disciplinary process
B. Annex A 6.7 Remote working
C. Annex A 6.1 Screening
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A 5.7 Threat Intelligence ISO/IEC 27002:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection controls, Clause 5.7 Threat Intelligence PECB ISO/IEC 27001:2022 Lead Implementer Course, Module 6: Implementation of Information Security Controls Based on ISO/IEC 27002:2022, Slide 18: A.5.7 Threat Intelligence

NEW QUESTION: 66
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: (SHOW ANSWER)
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.
ISO 27001:2022 Annex A 8.13 - Information Backup1
ISO 27001:2022 Annex A 8.1 - Access Control Policy2
ISO 27001:2022 Annex A 8.2 - User Access Management3
ISO 27001:2022 Annex A 8.3 - User Responsibilities4
ISO 27001:2022 Annex A 8.4 - System and Application Access Control
ISO 27001:2022 Annex A 8.5 - Cryptography
ISO 27001:2022 Annex A 8.6 - Network Security Management

NEW QUESTION: 67
Scenario 5: OperazeIT 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, OperazeIT implemented an information security management system (ISMS) based on ISO/IEC 27001.
In a collaborative effort involving the implementation team, OperazeIT 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 OperazeIT's commitment to information security.
OperazeIT'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. Organizational and physical boundaries
C. Physical boundaries only
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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: (SHOW ANSWER)
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."
References:
ISO/IEC 27001:2022 Clause 10.2==========

NEW QUESTION: 69
' 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: (SHOW ANSWER)
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.
ISO/IEC 27001:2013, clause 4.3: Determining the scope of the information security management system ISO/IEC 27001 Lead Implementer Course, Module 4: Planning the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC
27001
ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit ISO/IEC 27001 scope statement | How to set the scope of your ISMS - Advisera1

How to Write an ISO 27001 Scope Statement (+3 Examples) - Compleye2 How To Use an Information Flow Map to Determine Scope of Your ISMS3 ISMS SCOPE DOCUMENT - Resolver4 Define the Scope and Objectives - ISMS Info5

NEW QUESTION: 70
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 a security control that ensures the confidentiality of information
B. Org Y has implemented an integrity control that avoids the involuntary corruption of data
C. Org Y has incorrectly implemented a security control that could become a vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Scenario 1: NobleFind is an online retailer specializing in high-end, custom-design furniture. The company offers a wide range of handcrafted pieces tailored to meet the needs of residential and commercial clients.
NobleFind also provides expert design consultation services. Despite NobleFind ' s efforts to keep its online shop platform secure, the company faced persistent issues, including a recent data breach. These ongoing challenges disrupted normal operations and underscored the need for enhanced security measures. The designated IT team quickly responded to resolve the problem, demonstrating their agility in handling technical challenges. To address these issues, NobleFind decided to implement an Information Security Management System (ISMS) based on ISO/IEC 27001 to improve security, protect customer data, and ensure the stability of its services.
In addition to its commitment to information security, NobleFind focuses on maintaining the accuracy and completeness of its product data. This is ensured by carefully managing version control, checking information regularly, enforcing strict access policies, and implementing backup procedures. Product details and customer designs are accessible only to authorized individuals, with security measures such as multi-factor authentication and data access policies. NobleFind has implemented an incident investigation process within its ISMS and established record retention policies. NobleFind maintains and safeguards documented information, encompassing a wide range of data, records, and specifications-ensuring the security and integrity of customer data, historical records, and financial information.
Has NobleFind implemented any preventive controls? Refer to Scenario 1.
A. Yes, by establishing an information security policy
B. Yes, by monitoring the resources used by its systems
C. No, NobleFind has implemented only corrective and detective controls
D. Yes, by conducting audit log analysis only

Answer: (SHOW ANSWER)
Preventive controls are those that are designed to prevent security incidents before they occur. According to ISO/IEC 27001:2022, establishing an information security policy is a foundational preventive measure because it sets the direction, principles, and rules for information security throughout the organization. This policy informs staff about required behaviors and actions that must be taken to protect information assets, and it guides the implementation of additional preventive, detective, and corrective controls.
ISO/IEC 27001:2022, Annex A, control A.5.1 " Policies for information security, " explicitly requires the establishment of an information security policy as a preventive measure:
" Information security policies shall be defined, approved by management, published and communicated to employees and relevant external parties. "
- ISO/IEC 27001:2022, Annex A, A.5.1
The purpose of this policy is to prevent undesirable security events by ensuring everyone understands their responsibilities regarding information security. Monitoring the resources used by systems (option B) is considered a detective control, not a preventive one, as it helps to detect and respond to anomalies after they occur. Option C is incorrect, as the scenario explicitly mentions the information security policy (a preventive control).
References:
ISO/IEC 27001:2022, Annex A, A.5.1 " Policies for information security " ISO/IEC 27002:2022, 5.1 (explanation of policies as preventive controls)

NEW QUESTION: 72
An internal auditor at a mid-sized company is asked to conduct an internal ISMS audit of the IT Department, where the auditor held daily operational responsibilities just three months ago The company has well- documented job descriptions distinguishing between The auditor's current audit duties and their previous operational role in the IT Department. What is the most appropriate act on to uphold the objectivity and impartiality of the audit?
A. Proceed with the audit since the job descriptions are clearly defined
B. Decline the audit assignment because the one-year cooling-off period has not passed
C. Conduct the audit jointly with a colleague from another department
Answer: C (LEAVE A REPLY)
The correct answer is Option C, as it best upholds objectivity and impartiality while allowing the internal audit to proceed effectively.
ISO/IEC 27001:2022 Clause 9.2 - Internal audit requires that audits be conducted in a manner that ensures objectivity and impartiality. This requirement is further reinforced by ISO 19011, which states that auditors should not audit their own work and should avoid conflicts of interest.
In this scenario, the auditor:
* Held daily operational responsibilities in the IT Department just three months ago.
* Is now asked to audit the same department.

Although job descriptions clearly distinguish past and present roles, the risk of perceived or actual bias remains high due to the short time elapsed. A common best practice is a cooling-off period (often around one year), but ISO standards do not mandate a fixed duration.
* Option A is incorrect because clear job descriptions alone do not eliminate bias risk.
* Option B is too rigid; ISO/IEC 27001 does not mandate a one-year cooling-off period.
By conducting the audit jointly with a colleague from another department, the organization:
* Preserves audit independence,
* Introduces an objective perspective,
* Mitigates conflict-of-interest concerns,
* Remains compliant with Clause 9.2 and ISO 19011 guidance

NEW QUESTION: 73
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 (LEAVE A REPLY)
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.
References:
ISO/IEC 27001:2022 Clauses 6.1.3 (e), (f)
ISO/IEC 27005:2022 - Risk treatment methodology

NEW QUESTION: 74
Scenario 8: SecureLynx is one Of the largest cybersecurity advisory and consulting companies that helps private sector organizations prevent security threats. improve security systems. and achieve business SecureLynr is committed to complying with national and international standards to enhance the company ' S resilience and credibility_ SecureLynx has Started implementing an ISMS based on ISO/IEC 27001 as part of its relentless pursuit of security.

As part of the internal audit activities. the top management reviewed and approved the audit objectives to assess the effectiveness of SecureLynx*s ISMS During the audit, the internal auditor evaluated whether top management Supports activities associated with the ISMS and if the toles and responsibilities Of relevant parties are Clearly defined. This rigorous examination is a testament to SecureLynx ' S commitment to continuous improvernent and alignment of security measures with organizational goals.
SecureLynx employs an innovative dashboard that visually represents implemented processes and controls to ensure transparency and accountability within the Organization. This tool Offers stakeholders a real- time overview of security measures. empowering them to make informed decisions and swiftly respond to emerging threats. As part of this initiative, Paula was appointed to a new position entrusted with the responsibility Of collecting, recordlng, and Stoting data to measure the effectiveness Of the ISMS-Furthermore, SecureLynx conducts management reviews every six months to ensure its Systems are robust and continually improving. These reviews serve as a crucial mechanism for assessing the efficacy Of security measures and identifying areas for enhancement. SecureLynx ' s dedication to implementing and maintaining a robust ISMS exemplifies its commitment to innovation and Client satisfaction.
Based on the scenario above, answer the following question.
Based on the description of Paula ' s responsibilities at SecureLynx, her role is known as:
A. Information collector
B. Information analyst
C. Information communicator
Answer: (SHOW ANSWER)
Paula is responsible for collecting, recording, and storing data to measure the effectiveness of the ISMS. This describes an information analyst-someone who analyzes collected data to evaluate ISMS performance and inform improvements.
"The role of an information analyst includes collecting, recording, analyzing, and reporting data to support management decisions and measure ISMS effectiveness."
- ISO/IEC 27004:2016, Clause 6.3

NEW QUESTION: 75
Scenario 7: Yefund, an insurance Company headquartered in Monaco, is a reliable name in Commerce, industry, and Corporate services. With a rich history spanning decades, Yefund has consistently delivered tailored insurance solutions to businesses of all sizes. safeguarding their assets and mitigating risks. As a forward-thinking company, Yetund recognizes the importance of information security in protecting sensitive data and maintaining the trust Of Its clients. Thus, has embarked on a transformative journey towards implemenung an ISMS based on ISO/IEC 27001- iS implementing cutting-edge Al technologies within its ISMS to improve the identification and management Of information assets, Through Al. is automating the identification Of assets. tracking changes over time. and strategically selecting controls based on asset sensitivity and exposure. This proactive

approach ensures that Yefund remains agile and adaptive in safeguarding critical information assets against emerging threats. Although Yetund recognized the urgent need to enhance its security posture, the implementation team took a gradual approach to integrate each ISMS element- Rather than waiting for an official launch, they carefully tested and validated security controls, gradually putting each element into operational mode as it was completed and approved. This methodical process ensured that critical security measures, such as encryption protocols. access controls. and monitoring systems. were fully operational and effective in safeguarding customer information, including personal. policy, and financial details.

Recently. Kian. a member of Vefund ' s information security team. identified two security events. Upon evaluation. one reported incident did not meet the criteria to be classified as such- However, the second incident. involving critical network components experiencing downtime. raised concerns about potential risks to sensitive data security and was therefore categorized as an incident. The first event was recorded as a report without further action, whereas the second incident prompted a series Of actions, including investigation. containment, eradication, recovery. resolution, closure, incident reporting, and post-incident activities. Additionally. IRTS were established to address the events according to their Categorization.

After the incident. Yetund recognized the development of internal communication protocols as the single need to improve their ISMS framework It determined the relevance of communication aspects such as what, when, with whom. and how to Communicate effectively Yefund decided to focus On developing internal communication protocols, reasoning that internal coordination their most immediate priority. This decision was made despite having external stakeholders. such as clients and regulatory bodies. who also required secure and timely communication.

Additionally, Yefund has prioritized the professional development Of its employees through comprehensive training programs, Yefund assessed the effectiveness and impact Of its training initiatives through Kirkpatrick ' s four-level training evaluation model. From measuring trainees ' involvement and impressions of the training (Level 1) to evaluating learning outcomes (Level 2), post-training behavior (Level 3), and tangible results (Level 4), Yefund ensures that Its training programs ate holistic. impactful. and aligned With organizational objectives.

Yefund*s journey toward implementing an ISMS reflects a commitment to security, innovation, and continuous improvement, By leveraging technology, fostering a culture Of proactive vigilance, enhancing communication ptotOCOIS, and investing in employee development. Yefund seeks to fortify its position as a trusted partner in safeguarding the interests Of its Clients and stakeholders.

Did Yefund handle the identified information security events appropriately? Refer to scenario 7.

A. Yes, both information security events were effectively addressed

B. No, because information security events should not be categorized merely as event reports under any circumstances
C. No, monitoring teams must be established to address the events according to their categorization
Answer: (SHOW ANSWER)
Yefund appropriately classified and handled each security event: one was not an incident and was recorded as a report (no further action needed); the other was a genuine incident and prompted a full incident response cycle. This is in line with best practices and requirements for security event and incident management.
"Events should be assessed to determine whether they are to be classified as information security incidents.
Not all events are incidents. Incidents require response per documented procedures."
- ISO/IEC 27001:2022, Annex A, Control 5.24; ISO/IEC 27035-1:2016, Clause 6.3

NEW QUESTION: 76
Which of the following is the most suitable option for presenting raw data in a user-friendly, easy-to-read format?
A. Reports
B. Scorecards
C. Gages
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.14.

NEW QUESTION: 78
Why is an in-depth review crucial for organizations to evaluate their security architecture?
A. To conduct background checks on potential employees to ensure security compliance
B. To determine the organization's compliance with financial regulations
C. To assess whether security requirements based on industry best practices can be met
D. To meet shareholder expectations
Answer: C (LEAVE A REPLY)
An in-depth review of security architecture allows organizations to ensure that their security requirements, particularly those aligned with industry best practices and applicable standards, are effectively met. This process enables organizations to identify gaps, align security controls with business and regulatory needs, and maintain robust protection for information assets.
"Security architecture reviews help verify that security requirements, including those based on industry best practices, have been properly implemented and maintained."
- ISO/IEC 27001:2022, Annex A, Control A.8.27 Secure system architecture and engineering principles; ISO
/IEC 27002:2022, 8.27

NEW QUESTION: 79
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. Application and data
C. Servers and storage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
A rapidly expanding cloud service provider is facing new data protection regulations and evolving cyber threats. To ensure its ISMS continues to meet business and compliance needs, what qualities are most important for its design and operation?
A. Structured and resistant to frequent modification
B. Adaptable and responsive to external change
C. Adaptable and responsive to internal growth only
Answer: B (LEAVE A REPLY)
ISO/IEC 27001:2022 Clause 4.1 requires organizations to understand external and internal issues, and Clause
6.1 mandates that risks and opportunities are addressed continuously. The standard ' s PDCA (Plan-Do-Check- Act) cycle is built on the premise that an ISMS must be dynamic and responsive to its environment. For a rapidly expanding cloud provider facing new regulations and emerging threats, the ISMS must be adaptable and responsive to external change - not rigid or resistant to modification. ISO/IEC 27001:2022 explicitly requires the ISMS to reflect changes in context, including legal, regulatory, and threat landscape shifts. Internal growth alone is insufficient; external factors such as new compliance requirements (e.g., GDPR, NIS2) and evolving attack vectors require proactive external responsiveness as a core ISMS design quality.

NEW QUESTION: 81
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: (SHOW ANSWER)

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 15504 standard, 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.
1: ISO/IEC 27001:2022 Lead Implementer Course Brochure, page 5
2: ISO/IEC 27001:2022 Lead Implementer Course Presentation, slide 25

NEW QUESTION: 82
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. 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 (LEAVE A REPLY)
The initial error (sending confidential data to a competitor) is a classic breach of confidentiality (unauthorized disclosure of information).
The competitor altering and misusing the information is a violation of integrity (unauthorized modification or falsification of data).
" Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity is the property of safeguarding the accuracy and completeness of assets. "
- ISO/IEC 27000:2018, 3.6 & 3.8

NEW QUESTION: 83
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 (LEAVE A REPLY)
In the scenario described, Beauty's decision to install new anti-malware software after a security incident is a Preventive control. 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.
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Security Controls? | IBM3 What Are Security Controls? - F54

NEW QUESTION: 84
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 (LEAVE A REPLY)
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.
References:
ISO/IEC 17021-1:2015 Clause 7.2.7
ISO/IEC 27006:2015 Clause 8.5 - Certification decision criteria==========

NEW QUESTION: 85
Infralink is a medium-sized IT consultancy firm headquartered in Dublin, Ireland. It specializes in secure cloud infrastructure, software integration, and data analytics, serving a diverse client base in the healthcare, financial services, and legal sectors, including hospitals, insurance providers, and law firms. To safeguard sensitive client data and support business continuity, Infralink has implemented an information security management system (ISMS) aligned with the requirements of ISO/IEC 27001.
In developing its security architecture, the company adopted services to support centralized user identification and shared authentication mechanisms across its departments. These services also governed the creation and management of credentials within the company. Additionally, Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity across its systems.
In preparation for implementing information security controls, the company ensured the availability of necessary resources, personnel competence, and structured planning. It conducted a cost-benefit analysis, scheduled implementation phases, and prepared documentation and activity checklists for each phase. The intended outcomes were clearly defined to align security controls with business objectives.
Infralink started by implementing several controls from Annex A of ISO/IEC 27001. These included regulating physical and logical access to information and assets in accordance with business and information security requirements, managing the identity life cycle, and establishing procedures for providing, reviewing, modifying, and revoking access rights. However, controls related to the secure allocation and management of authentication information, as well as the establishment of rules or agreements for secure information transfer, have not yet been implemented. During the documentation process, the company ensured that all ISMS- related documents supported traceability by including titles, creation or update dates, author names, and unique reference numbers. Based on the scenario above, answer the following question.

Is the project team's decision to not consider certain business processes and departmental responsibilities during the review for the ISMS scope establishment acceptable? Refer to scenario 5.

A. Yes, because the exclusion of some processes and departments aligns with ISO/IEC 27001 flexibility.

B. No, as all organizational units, structures, and processes should be considered when defining the ISMS scope

C. Yes, because the exclusion of some processes and departments is allowed in a decentralized structure.

Answer: (SHOW ANSWER)

The correct answer is Option B. According to ISO/IEC 27001:2022, excluding business processes or departmental responsibilities without proper consideration is not acceptable when defining the ISMS scope.

ISO/IEC 27001:2022 Clause 4.3 - Determining the scope of the ISMS requires the organization to:

"determine the boundaries and applicability of the information security management system to establish its scope." It further requires consideration of:

* external and internal issues (Clause 4.1),
* requirements of interested parties (Clause 4.2),
* interfaces and dependencies between activities performed by the organization.

This means all organizational units, structures, and processes that affect information security must be considered when defining scope. While exclusions are permitted, they must be justified, documented, and not undermine the ISMS's ability to achieve intended outcomes.

* Option A is incorrect because ISO/IEC 27001 flexibility does not permit arbitrary exclusion.
* Option C is incorrect because decentralization does not remove the obligation to consider all relevant processes and departments.

Conclusion: Failure to consider certain business processes and departmental responsibilities during scope definition is nonconformant with Clause 4.3. Therefore, Option B is 100% correct.

NEW QUESTION: 86

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 (LEAVE A REPLY)

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.

ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, specifically:

ISO/IEC 27001:2022, clause 6.1.2 Information security risk assessment

ISO/IEC 27005:2021, clause 5.2 Asset identification and valuation

PECB ISO/IEC 27001 Lead Implementer Course, Module 6: Risk Management

NEW QUESTION: 87

Which control in Annex A of ISO/IEC 27001 requires that the information security requirements shall be identified, specified, and approved when developing or acquiring applications?

A. A.8.25 Secure development life cycle
B. A.8.26 Application security requirements
C. A.8.27 Secure system architecture and engineering principles
Answer: B (LEAVE A REPLY)
Annex A control A.8.26 Application security requirements mandates that security requirements must be identified, specified, and approved during the development or acquisition of applications.
"Information security requirements shall be identified, specified and approved when developing or acquiring applications."
- ISO/IEC 27001:2022, Annex A, Control 8.26 Application security requirementsQuestion No. 22/80 What iS the purpose of ISO, ' IEC 27002 clause 8u8?
TO ensure all security requitements are addressed during application development To ensure software is written securely to reduce information security vulnerabilities To ensure secure system design principles are followed

NEW QUESTION: 88
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 (LEAVE A REPLY)
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.
ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Section 8.2.3.2.1, page 162
ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 13 ISO/IEC 27002 : 2022, Section 13.1.3, page 66

NEW QUESTION: 89
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 (LEAVE A REPLY)

NEW QUESTION: 90
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: (SHOW ANSWER)
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.
ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements ISO 27001 Key Terms - PJR Network Segmentation: What It Is and How It Works | Imperva ISO 27001:2022 Annex A 8.2 - Privileged Access Rights - ISMS.online
[ISO 27001:2022 Annex A 8.3 - Cryptographic Controls - ISMS.online]
[ISO 27001:2022 Annex A 5.30 - Information Security Threat Management - ISMS.online]
[ISO 27001:2022 Annex A 5.31 - Information Security Integration into Project Management - ISMS.online]
[ISO 27001:2022 Annex A 8.13 - Information Backup - ISMS.online]

NEW QUESTION: 91

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. No, as temporary corrective actions are not allowed in the evaluation phase
B. Yes, Julia's decision to implement temporary corrective actions was consistent with best practices
C. No, implementing temporary actions during the corrective action process is not recommended

Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
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 (LEAVE A REPLY)
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.
1: ISO/IEC 27001:2022, clause 10.2 2: Procedure for Corrective Action [ISO 27001 templates] 3: ISO 27001 Clause 10.2 Nonconformity and corrective action

NEW QUESTION: 93
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: (SHOW ANSWER)
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.
ISO/IEC 27001:2022, clause 5.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 9.

NEW QUESTION: 94
Scenario 1: NobleFind is an online retailer specializing in high-end, custom-design furniture. The company offers a wide range of handcrafted pieces tailored to meet the needs of residential and commercial clients.
NobleFind also provides expert design consultation services. Despite NobleFind ' s efforts to keep its online shop platform secure, the company faced persistent issues, including a recent data breach. These ongoing challenges disrupted normal operations and underscored the need for enhanced security measures. The designated IT team quickly responded to resolve the problem. To address these issues, NobleFind decided to

implement an Information Security Management System (ISMS) based on ISO/IEC 27001 to improve security, protect customer data, and ensure the stability of its services.
In addition to its commitment to information security, NobleFind focuses on maintaining the accuracy and completeness of its product data. This is ensured by carefully managing version control, checking information regularly, enforcing strict access policies, and implementing backup procedures. Moreover, product details and customer designs are accessible only to authorized individuals, with security measures such as multi- factor authentication and data access policies.
NobleFind has implemented an incident investigation process within its ISMS, as part of its comprehensive approach to information security. Additionally, it has established record retention policies to ensure that online information about each product and client information remains readily accessible and usable on demand for authorized entities.
NobleFind established an information security policy offering clear guidelines for safeguarding historical data. It also insisted that personnel sign confidentiality agreements and were committed to recruiting only qualified individuals. Additionally, NobleFind implemented measures for monitoring the resources used by its systems, reviewing user access rights, and conducting a thorough analysis of audit logs to swiftly identify and address any security anomalies.
With its ISMS in place, NobleFind maintains and safeguards documented information, encompassing a wide range of data, records, and specifications. This documented information is vital to its operations, ensuring the security and integrity of customer data, historical records, and financial information.
Based on the scenario above, answer the following question.
Which information security principle was impacted during the service interruption that NobleFind experienced?
A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation
Answer: C (LEAVE A REPLY)
The principle that was impacted during the service interruption at NobleFind is Availability. According to ISO/IEC 27001:2022, information security is built upon three core principles, known as the CIA Triad:
Confidentiality: Ensuring that information is accessible only to those authorized to have access.
Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Availability: Ensuring that authorized users have access to information and associated assets when required.
A service interruption directly affects the availability of information and services. This is explicitly supported by ISO/IEC 27001:2022 in Annex A, control A.8.14 " Redundancy of

information processing facilities, " which emphasizes the need to ensure that information and assets are available when needed. Moreover, Clause 6.1.2(c)1 of ISO/IEC 27001:2022 highlights the necessity to identify risks associated with the loss of confidentiality, integrity, and availability within the scope of the ISMS. A disruption in the normal operation, such as the service interruption faced by NobleFind, constitutes a breach of the availability principle.
Reference Extracts:
"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 information security management system..."- ISO/IEC 27001:2022, Clause 6.1.2 (c)1.
" availability: property of being accessible and usable upon demand by an authorized entity " - ISO/IEC
27000:2018, 3.7 (as referenced in ISO/IEC 27001:2022, Section 3 Terms and definitions).
" A disruption is an incident... that causes an unplanned negative deviation from the expected delivery of products and services according to an organization's objectives. " - ISO/IEC 27002:2022, 3.1.9 Disruption.
A service interruption that affects customer access or company operations is thus a classic example of an availability incident.
References:
ISO/IEC 27001:2022, Clause 6.1.2(c)1
ISO/IEC 27001:2022, Section 3 Terms and Definitions
ISO/IEC 27002:2022, 3.1.9 Disruption
ISO/IEC 27000:2018 (vocabulary referenced by ISO/IEC 27001:2022)

NEW QUESTION: 95
Scenario 6: CB Consulting iS a reputable firm based in Dublin, Ireland. providing Strategic business Solutions to diverse clients, With a dedicated team Of professionals, CB Consulting prides itself on its commitment to excellence, integrity, and client satisfaction. CB Consulting started implementing an ISMS aligned with ISOflEC 27001 as part of its ongoing commitment to enhancing its information security practices. Throughout this process, ensuring effective communication and adherence to establi Shed security protocols is essential.
Sarah, an employee at CB has been appointed as the head Of a new project focused on managing sensitive client data, Additionally, she is responsible for Overseeing activities during the response phase of incident management, including regular reporting to the incident manager of the incident management team and keeping key stakeholders informed. Meanwhile, CB Consulting has reassigned Tom to serve as the company ' s legal consultant.
CB Consulting has also reassigned Clare. formerly an IT security analyst, as their information security officer to oversee the implementation Of the ISMS and ensure compliance with ISO/IEC 27001. Clare ' s primary responsibility iS to conduct regular risk

assessments. identlfy potential vulnerabilities, and implement appropriate Security measures to mitigate risks effectively. Clare has established a procedure Stating that information security risk assessments are conducted only when significant changes occur. playing a crucial role in strengthening the companys security posture and safeguarding against potential threats.

TO ensure it has a Competent workforce to meet information security Objectives, CB Consulting has implemented a process to and verify that all employees, including Sarah, Tom, and Clare, possess the necessary competence based on their education. training, or experience. Where gaps were identified, the company has taken specific actions such as providing additional training and mentoring. Additionally, CB Consulting retains documented information as evidence of the competencies requ.red and acquired.

CB Consulting has established a robust communication strategy aligned with industry standards to ensure secure and effective information exchange. It identified the requirements for communication on relevant issues. First, the company designated specific toles. Such as a public relations officer for external communication and a Security officer for internal matters, to manage sensitive issues like data breaches. Then. communication triggers, content. and recipients were carefully defined. with messages pre-approved by management where necessary. Lastly, dedicated channels were implemented to ensure the confidentiality and integrity of transmitted information.

Based on the scenario above, answer the following question.

CB Consulting prioritizes transparent and Substantive communication practices to foster trust, enhance Stakeholder engagement, and reinforce its commitment to information security excellence. Which principle of effective communication is emphasized by this approach?

Transparency

Has CB Consulting taken appropriate measures to ensure compliance with ISO/IEC 27001 requirements regarding acquiring necessary competence? Refer to scenario 6.

A. Yes. CB Consulting has taken compliant actions regarding acquiring the necessary competence

B. No, reassigning current employees for tasks directly related to ISMS implementation management is not permissible

C. No, reassigning current employees for tasks related to legal consulting is not permissible

Answer: A (LEAVE A REPLY)

ISO/IEC 27001:2022 Clause 7.2 requires organizations to ensure that employees are competent on the basis of education, training, or experience, and to take action when gaps are identified. CB Consulting verified competence, provided additional training and mentoring as needed, and kept records as evidence-all compliant with the standard.

"The organization shall... ensure that employees... are competent... on the basis of appropriate education, training, or experience; where applicable, take actions to acquire

the necessary competence and retain appropriate documented information as evidence of competence."
- ISO/IEC 27001:2022, Clause 7.2

NEW QUESTION: 96
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 exclusively available to the Information Technology Department or a similar unit within the company
C. No, operating procedures for information processing facilities should have been specifically provided to personnel who require them
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
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: (SHOW ANSWER)
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.
1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10: Nonconformity and Corrective Action, slide 9 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10: Nonconformity and Corrective Action, slide 10 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 10: Nonconformity and Corrective Action, slide 11

NEW QUESTION: 98
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements ISO 27001 Key Terms - PJR

NEW QUESTION: 99

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. Corrective controls
B. Detective controls
C. Preventive controls
Answer: (SHOW ANSWER)

NEW QUESTION: 100
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 modification
B. Risk retention
C. Risk avoidance
Answer: C (LEAVE A REPLY)

NEW 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:
According to scenario 1. to detect (1)_____, Antiques should have implemented (2)
A. (1) Intrusions on networks. (?) an intrusion detection system
B. (1) Patches. (2) an access control software
C. (1) Technical vulnerabilities. (2) network intrusions
Answer: (SHOW ANSWER)

NEW QUESTION: 102
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 (LEAVE A REPLY)
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.
1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 22 2: PECB, ISO/IEC
27001 Lead Implementer Course, Module 9: Internal Audit, slide 23 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 9: Internal Audit, slide 24

NEW QUESTION: 103
Which of the following steps is necessary to effectively implement information security controls?
A. Implement security controls before conducting a risk assessment
B. Establish a schedule for the implementation of each control
C. Hire an external contractor with cybersecurity expertise
Answer: B (LEAVE A REPLY)
ISO/IEC 27001:2022 requires that once information security controls are selected, organizations must plan their implementation. Establishing a clear schedule ensures that each control is implemented effectively and that responsibilities and timelines are managed.
"The organization shall plan the implementation of information security controls, including assigning responsibilities and defining implementation schedules."
- ISO/IEC 27001:2022, Clause 6.2, 8.1, and 8.3

NEW QUESTION: 104
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 (LEAVE A REPLY)
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.
ISO 27001 - Annex A.10 - Cryptography
ISO 27001 Annex A.10 - Cryptography | ISMS.online
ISO 27001 cryptographic controls policy | What needs to be included?

NEW QUESTION: 105
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. The recodification audit Is planned to be conducted two years after HealthGenic implemented the ISMS
B. Emma has an operational role in the HealthGenic's management system
C. Emma had access to all offices and documentation of HealthGenic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
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 (LEAVE A REPLY)

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.

ISO/IEC 27001:2022, clause 8.2.3; PECB ISO/IEC 27001 Lead Implementer Study Guide, section 8.2.3.

NEW QUESTION: 107

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 (LEAVE A REPLY)
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.
1: ISO/IEC 27001:2022, Clause 9.2.3
2: ISO/IEC 27001:2022, Clause 3.23
3: ISO/IEC 27001:2022, Clause 3.5
ISO/IEC 27001:2022, Annex A.9.2.3

NEW QUESTION: 108
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. Strategic dashboards
B. Operational dashboards
C. Tactical dashboards
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Infralink is a medium-sized IT consultancy firm headquartered in Dublin, Ireland. It specializes in secure cloud infrastructure, software integration, and data analytics, serving a diverse client base in the healthcare, financial services, and legal sectors, including hospitals, insurance providers, and law firms. To safeguard sensitive client data and support business continuity, Infralink has implemented an information security management system (ISMS) aligned with the requirements of ISO/IEC 27001.
In developing its security architecture, the company adopted services to support centralized user identification and shared authentication mechanisms across its departments. These services also governed the creation and management of credentials within the company. Additionally, Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity across its systems.
In preparation for implementing information security controls, the company ensured the availability of necessary resources, personnel competence, and structured planning. It conducted a cost-benefit analysis, scheduled implementation phases, and prepared documentation and activity checklists for each phase. The intended outcomes were clearly defined to align security controls with business objectives.
Infralink started by implementing several controls from Annex A of ISO/IEC 27001. These included regulating physical and logical access to information and assets in accordance with business and information security requirements, managing the identity life cycle, and establishing procedures for providing, reviewing, modifying, and revoking access rights. However, controls related to the secure allocation and management of authentication information, as well as the establishment of rules or agreements for secure information transfer, have not yet been implemented. During the documentation process, the company ensured that all ISMS- related documents supported traceability by including titles, creation or update dates, author names, and unique reference numbers. Based on the scenario above, answer the following question.
According to scenario A. did AegisCure identify supporting assets?
A. Yes, the company identified all supporting assets as part of the asset identification process.
B. No, the company limited its asset identification to business processes and information.
C. No, the company identified primary assets only.
Answer: (SHOW ANSWER)
Based on the scenario, Infralink did not explicitly identify supporting assets; it focused primarily on information and access-related assets, which are considered primary assets. Therefore, Option C is the correct answer.
ISO/IEC 27001:2022 requires organizations to identify information and other associated assets as part of establishing and operating the ISMS. While the standard itself does not mandate a specific asset taxonomy, ISO/IEC 27002:2022 Annex A control A.5.9 - Inventory of information and other associated assets requires that:

"Information and other associated assets shall be identified and an inventory of these assets shall be maintained." In common ISO/IEC 27001-aligned risk management practice (as supported by ISO/IEC 27005), primary assets typically include information and business processes, while supporting assets include hardware, software, networks, facilities, people, and services that support those primary assets.
In the scenario, Infralink implemented controls related to:
* Access to information and assets (A.5.15)
* Identity lifecycle management (A.5.16)
* Access rights management (A.5.18)
However, there is no explicit reference to identifying or inventorying supporting assets such as infrastructure components, platforms, physical facilities, or third-party services. The focus remains on information access and control mechanisms, indicating that asset identification was limited to primary assets.
* Option A is incorrect because there is no evidence that all supporting assets were identified.
* Option B is incorrect because the scenario does go beyond business processes and information by addressing access mechanisms-but still does not explicitly include supporting assets.

NEW QUESTION: 110
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.
Based on scenario 10. did invalid Electric provide a valid reason for requesting the replacement of the audit learn leader?
A. No, because the auditee can request the replacement of an auditor only if the auditor has worked for the auditee
B. No, because Issuing a recommendation for certification lo a main competitor is not a conflict of interest situation
C. Yes, because the auditee can request to replace an auditor that has worked for one of its major competitors
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Nimbus Route, a cloud-native logistics optimization company based in the Netherlands, offers Al-driven route planning fleet management tools, and real time shipment tracking

solutions to clients across Europe and North America. To safeguard sensitive logistics data and ensure resilience across its cloud services. Nimbus Route has implemented an information security management system (ISMS) based on ISO/IEC 27001. The company is also integrating intelligent transport systems and predictive analytics to increase operational efficiency and sustainability. As part of the ISMS implementation process, the company is determining the competence levels required to manage its ISMS. It has 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 expectations of its customers. Furthermore, the company has 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 have been formally documented: instead, the company classified and managed communication based on its needs. ensuring that documentation is maintained only to the extent necessary for the ISMS's effectiveness To support its expanding digital services and ensure operational scalability. Nimbus Route utilizes virtualized computing resources provided by an external cloud service provider. This setup allows the company to configure and manage its operating systems, deploy applications. and control storage environments as needed while relying on the provider to maintain the underlying cloud environment. To further enhance is predictive capabilities. Nimbus Route is adopting machine learning techniques across several of its core services Specifically, it uses machine learning for route optimization and delivery time estimation, leveraging algorithms such as logistic regression and support vector machines to identify patterns in historical transportation data. As Nimbus Route's ISMS matures, the company has chosen a chased approach to its transition into full operational mode Rather than waiting for a formal launch, individual elements of the ISMS, such as risk treatment procedures, access controls, and audit logging, are being activated progressively as soon as they are developed and approved Based on the scenario above answer the follow rig question.

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

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

B. No, because Nimbus Route did not consider external issues that are relevant to the ISMS

C. Yes, because Numbus Route considered external issues, internal factors, and the needs and expectations of relevant interested parties.

Answer: C (LEAVE A REPLY)

Nimbus Route appropriately determined the competence levels required to support its ISMS, making Option C the correct and verified answer.

ISO/IEC 27001:2022 requires organizations to define competence by considering both internal and external factors, as well as the needs and expectations of relevant interested parties. This requirement is explicitly addressed across several clauses.
Under Clause 7.2 - Competence, the standard requires the organization to:
"determine the necessary competence of person(s) doing work under its control that affects information security performance." Determining competence does not occur in isolation. It must be informed by:
* Clause 4.1 - Understanding the organization and its context, which requires identification of internal and external issues relevant to the ISMS.
* Clause 4.2 - Understanding the needs and expectations of interested parties, which includes customers, regulators, and partners.
The scenario clearly states that Nimbus Route considered:
* Technological advancements (external/internal context),
* Regulatory requirements (external issues),
* Mission and strategic objectives (internal issues),
* Available resources (internal capability),
* Customer needs and expectations (interested parties).
This demonstrates full alignment with Clauses 4.1, 4.2, and 7.2.
* Option A is incorrect because Nimbus Route did not consider only internal factors.
* Option B is incorrect because the scenario explicitly states that external issues were considered.
Conclusion: Nimbus Route followed the ISO/IEC 27001:2022 requirements for determining competence in a comprehensive and context-aware manner. Therefore, Option C is 100% correct and verified.

NEW QUESTION: 112
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 (LEAVE A REPLY)
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.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Annex A; PECB ISO/IEC 27001 Lead Implementer Course, Module
8: Implementation of Information Security Controls.

NEW QUESTION: 113
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 (LEAVE A REPLY)

NEW QUESTION: 114

Which of the following is categorized under the organizational controls of ISO/IEC 27001?

A. Annex 5.3 Segregation of duties

B. Annex 7.6 Working in secure areas

C. Annex 8.8 Management of technical vulnerabilities

Answer: (SHOW ANSWER)

Annex A 5.3 Segregation of duties is classified as an organizational control. Organizational controls include policies, procedures, and structures established to support information security. Segregation of duties aims to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets by dividing tasks and associated privileges.

"Annex A.5 contains organizational controls, including A.5.3 Segregation of duties, which ensures that no single person is responsible for completing a critical task alone, thereby reducing the risk of fraud or error."

- ISO/IEC 27001:2022, Annex A; ISO/IEC 27002:2022, 5.3

NEW QUESTION: 115
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 (LEAVE A REPLY)
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) ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, specifically:
ISO/IEC 27001:2022, clause 10.2 Nonconformity and corrective action
ISO/IEC 27001:2022, Annex A.16 Information security incident management ISO/IEC TS 27022:2021, clause 7.5.3.16 Information security incident management process PECB ISO/IEC 27001 Lead Implementer Course, Module 9: Incident Management

NEW QUESTION: 116
BioLooVitalis is a biopharmaceutical firm headquartered in Singapore Renowned for its pioneering work in the fie d of human therapeutics. BioLooVitalis places a strong emphasis on addressing critical healthcare concerns particularly in the domains of cardiovascular diseases, oncology bone health, and inflammation BioLooVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 77001 for the past two years. After noticing an increase m failed login attempts over several weeks. bioLooVitalis IT security learn reviewed log data, correlated it with user behavior patterns, and mapped it against known attach vectors to determine potential causes. Based on their findings, they prepared a technical report detailing the nature of the anomalies and submitted it to the compliance function. The compliance team then summarized the findings and presented them to the executive management during the quarterly ISMS performance review. To proactively track system behavior following the spike n failed login attempts. BioLooVitalis ' s IT security team configured a dashboard showing real time login activity. system response times, and

end point availability across departments. This helped the team quickly detect abnormal behavior without waiting formal reporting cycles. Following The implementation of the real time access control dashboard BioLooVitalis internal audit team assessed whether the new processes and tools effectively reduced unauthorized access attempts and met both technical and policy-based requirements. Lastly, the internal auditors collected system-generated access logs, reviewed user access reports, and conducted interviews with IT personnel. These data sources helped them verify whether the new controls were functioning as intended and aligned with internal ISMS objectives.
Based on The scenario above, answer the following question.
According to scenario 8 what did the internal auditors collect during the evaluation of the new access control measures?
A. Audit conclusions
B. Audit evidence
C. Findings as nonconformities
Answer: B (LEAVE A REPLY)
Scenario 8 explicitly states that internal auditors collected system-generated access logs, reviewed user access reports, and conducted interviews with IT personnel. These items constitute audit evidence, which is defined as records, statements of fact, or other information relevant to audit criteria and verifiable.
ISO/IEC 27001:2022 Clause 9.2 works in conjunction with ISO 19011 (Guidelines for auditing management systems), which clarifies that auditors must gather sufficient and appropriate audit evidence to support audit conclusions.
Access logs are objective, system-generated records.
User access reports provide documentary proof of control operation.
Interviews provide corroborating testimonial evidence.
Option A (Audit conclusions) is incorrect because conclusions are derived after evidence is evaluated.
Option C (Findings as nonconformities) is incorrect because findings are outcomes of evidence assessment and may include conformities, nonconformities, or opportunities for improvement-not raw inputs.
Conclusion: Since the auditors gathered logs, reports, and interview results to verify control operation, they collected audit evidence. Therefore, Option B is correct and ISO-aligned.

NEW QUESTION: 117
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:
Does SunDee ' s approach align with the best practices for evaluating and maintaining the effectiveness of an ISMS?
A. No, as an excessive number of measures may distort SunDee's focus and obscure what is genuinely important
B. Yes, because comprehensive coverage is essential to achieve ISMS objectives
C. Yes, because a diverse set of measures minimizes the likelihood of overlooking any potential security risks
Answer: (SHOW ANSWER)

NEW QUESTION: 118

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 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: B (LEAVE A REPLY)

Slower response times, downtime, and system saturation due to increased data flow and rapid expansion are categorized as technical failures. These issues directly relate to the limitations and breakdowns of IT systems (hardware, software, and communications infrastructure).

ISO/IEC 27005:2022 classifies such events as technical failures:

"Technical failures: Failures of IT systems, software, or infrastructure, including overload, saturation, or breakdowns, which affect the availability and performance of information systems."

- ISO/IEC 27005:2022, 8.2.2

NEW QUESTION: 119

Scenario:

Jane is a developer deploying an application using a language supported by her cloud provider. She doesn'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: (SHOW ANSWER)

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).

References:

ISO/IEC 17788:2014 Clause 6.2.4 - Cloud service models

ISO/IEC 27017:2015 - Security controls for cloud services==========

NEW QUESTION: 120
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: (SHOW ANSWER)
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.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clause 10.2.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 10: Incident Management.

NEW QUESTION: 121
Infralink is a medium-sized IT consultancy firm headquartered in Dublin, Ireland. It specializes in secure cloud infrastructure, software integration, and data analytics, serving a diverse client base in the healthcare, financial services, and legal sectors, including hospitals, insurance providers, and law firms. To safeguard sensitive client data and support business continuity, Infralink has implemented an information security management system (ISMS) aligned with the requirements of ISO/IEC 27001.
In developing its security architecture, the company adopted services to support centralized user identification and shared authentication mechanisms across its departments. These services also governed the creation and management of credentials within the company. Additionally, Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity across its systems.
In preparation for implementing information security controls, the company ensured the availability of necessary resources, personnel competence, and structured planning. It conducted a cost-benefit analysis, scheduled implementation phases, and prepared

documentation and activity checklists for each phase. The intended outcomes were clearly defined to align security controls with business objectives.
Infralink started by implementing several controls from Annex A of ISO/IEC 27001. These included regulating physical and logical access to information and assets in accordance with business and information security requirements, managing the identity life cycle, and establishing procedures for providing, reviewing, modifying, and revoking access rights. However, controls related to the secure allocation and management of authentication information, as well as the establishment of rules or agreements for secure information transfer, have not yet been implemented. During the documentation process, the company ensured that all ISMS- related documents supported traceability by including titles, creation or update dates, author names, and unique reference numbers. Based on the scenario above, answer the following question.
According to scenario 3. what aspects did Infralink ensure when documenting ISMS information?
A. Format and media
B. Identification and description
C. Review and approval scheduling
Answer: (SHOW ANSWER)
The correct and verified answer to Question 294 is B. Identification and description, based directly on the scenario and the requirements of ISO/IEC 27001:2022 Clause 7.5 - Documented information.
The scenario states that during documentation, Infralink ensured traceability by including:
* Document titles
* Creation or update dates
* Author names
* Unique reference numbers
These elements map exactly to the documented information requirements in Clause 7.5.2, which specifies how ISMS documentation must be identified and described.
ISO/IEC 27001:2022 Clause 7.5.2 a) states that documented information shall be appropriately identified and described, including:
"a title, date, author, or reference number."
This clause is explicitly reflected in the scenario wording, leaving no ambiguity that identification and description were the aspects ensured.
The other options can be clearly ruled out:
* Option A (Format and media) relates to Clause 7.5.2 b), which concerns whether documents are electronic, paper-based, language used, or software format. The scenario does not mention document formats or media.
* Option C (Review and approval scheduling) relates to Clause 7.5.2 c) and 7.5.3, which address approval for suitability and control of changes. The scenario does not describe review cycles, approval authorities, or version approval workflows.

By ensuring clear identification attributes, Infralink supports traceability, accountability, auditability, and version control, which are critical for ISMS effectiveness and certification readiness.

NEW QUESTION: 122
Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management
[^system implementation, TradeB ' s top management contracted two experts to direct and manage the ISMS implementation project.
First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted Based on scenario 4, the fact that TradeB defined the level of risk based on three nonnumerical categories indicates that;
A. The level of risk will be evaluated against qualitative criteria
B. The level of risk will be defined using a formula
C. The level of risk will be evaluated using quantitative analysis
Answer: A (LEAVE A REPLY)

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.
ISO/IEC 27001:2022, Annex A, control A.8.2.1
PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slides 12-13

NEW QUESTION: 123
NeuroTrustMed is a leading medical technology company based in Seoul, South Korea. The company specializes in developing AI-assisted neuroimaging solutions used in early diagnosis and treatment planning for neurological disorders. As a data-intensive company handling sensitive patient health records and medical research data, NeuroTrustMed places a strong emphasis on cybersecurity and regulatory compliance. The company has maintained an ISO/IEC 27001-certified ISMS for the past three years. It continuously reviews and improves its ISMS to address emerging threats, support innovation in medical diagnostics, and maintain stakeholder trust. As part of its commitment to continual improvement, NeuroTrustMed actively tracks potential nonconformities, performs root-cause analyses, implements corrective and preventive actions, and ensures all changes are documented and aligned with the company's strategic objectives. When a new data protection regulation came into effect affecting cross-regional data handling, the information security team conducted a gap assessment between current policies and the new regulation. Then, it updated relevant documentation and processes to meet compliance. Following these revisions, NeuroTrustMed updated the ISMS documentation and added a new entry in the improvement register. The register, maintained in the form of a structured spreadsheet, included a unique change number, a description of the update, and a high-priority classification due to legal compliance, the dates of initiation and completion, and the sign-off by the information security manager. Around the same period, during a scheduled management review, the information security team also identified a pattern of onboarding errors. While these had not resulted in any data breaches, they posed a risk of unauthorized access. In response, the onboarding procedure was revised and an automated verification step was added to ensure accuracy before access is

granted. To understand the underlying cause, the team collected data on the provisioning process. They analyzed process logs, interviewed onboarding staff, and traced access errors back to a misconfigured step in the HR-to-IT handover workflow. The team validated this finding through test cases before implementing any changes. Once confirmed, the information security team documented the nonconformity in the ISMS log. The documentation included a description of the issue, impacted systems, affected users, and a brief risk assessment of potential consequences related to access management. Based on the scenario above, answer the following question.
What type of change caused the ISMS update at NeuroTrustMed?
A. Change in ISMS internal roles
B. External change
C. Organizational change
Answer: B (LEAVE A REPLY)
The ISMS update at NeuroTrustMed was triggered by an external change, making Option B the correct answer.
The scenario clearly states that a new data protection regulation came into effect affecting cross-regional data handling. Regulatory changes originate outside the organization and represent external issues under ISO/IEC
27001:2022.
ISO/IEC 27001:2022 Clause 4.1 - Understanding the organization and its context requires organizations to determine external issues relevant to the ISMS, including legal and regulatory changes. Furthermore, Clause
6.3 - Planning of changes requires that ISMS changes be carried out in a planned manner when such issues arise.
NeuroTrustMed responded appropriately by:
Conducting a gap assessment against the new regulation,
Updating documentation and processes,
Recording the change in the improvement register with priority, dates, and approval.
Option A is incorrect because the change was not driven by internal role restructuring.
Option C is incorrect because the organization itself did not change structure or strategy; it responded to an external regulatory trigger.

NEW QUESTION: 124
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: (SHOW ANSWER)
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.
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2

ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls What is Information Security | Policy, Principles & Threats | Imperva1 What is information security? Definition, principles, and jobs2 What is Information Security? Principles, Types - KnowledgeHut3

NEW QUESTION: 125
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. Assigning the responsibility for appropriately classifying and protecting information and other associated assets to the asset owners
B. Conducting regular reviews of identified information and other associated assets
C. Establishing rules to control physical and logical access to Information and other associated assets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
Scenario 7: Yefund, an insurance Company headquartered in Monaco, is a reliable name in Commerce, industry, and Corporate services. With a rich history spanning decades, Yefund has consistently delivered tailored insurance solutions to businesses of all sizes. safeguarding their assets and mitigating risks. As a forward-thinking company, Yetund recognizes the importance of information security in protecting sensitive data and maintaining the trust Of Its clients. Thus, has embarked on a transformative journey towards implemenung an ISMS based on ISO/IEC 27001- iS implementing cutting-edge Al technologies within its ISMS to improve the identification and management Of information assets, Through Al. is automating the identification Of assets. tracking changes over time. and strategically selecting controls based on asset sensitivity and exposure. This proactive approach ensures that Yefund remains agile and adaptive in safeguarding critical information assets against emerging threats. Although Yetund recognized the urgent need to enhance its security posture, the implementation team took a gradual approach to integrate each ISMS element- Rather than waiting for an official launch, they carefully tested and validated security controls, gradually putting each element into operational mode as it was completed and approved. This methodical process ensured that critical security measures, such as encryption protocols. access controls. and monitoring systems. were fully operational and effective in safeguarding customer information, including personal. policy, and financial details.
Recently. Kian. a member of Vefund's information security team. identified two security events. Upon evaluation. one reported incident did not meet the criteria to be classified as such- However, the second incident. involving critical network components experiencing downtime. raised concerns about potential risks to sensitive data security and was

therefore categorized as an incident. The first event was recorded as a report without further action, whereas the second incident prompted a series Of actions, including investigation. containment, eradication, recovery. resolution, closure, incident reporting, and post-incident activities. Additionally. IRTS were established to address the events according to their Categorization.

After the incident. Yetund recognized the development of internal communication protocols as the single need to improve their ISMS framework It determined the relevance of communication aspects such as what, when, with whom. and how to Communicate effectively Yefund decided to focus On developing internal communication protocols, reasoning that internal coordination their most immediate priority. This decision was made despite having external stakeholders. such as clients and regulatory bodies. who also required secure and timely communication.

Additionally, Yefund has prioritized the professional development Of its employees through comprehensive training programs, Yefund assessed the effectiveness and impact Of its training initiatives through Kirkpatrick's four-level training evaluation model. From measuring trainees' involvement and impressions of the training (Level 1) to evaluating learning outcomes (Level 2), post-training behavior (Level 3), and tangible results (Level 4), Yefund ensures that Its training programs ate holistic. impactful. and aligned With organizational objectives.

Yefund*s journey toward implementing an ISMS reflects a commitment to security, innovation, and continuous improvement, By leveraging technology, fostering a culture Of proactive vigilance, enhancing communication ptotOCOIS, and investing in employee development. Yefund seeks to fortify its position as a trusted partner in safeguarding the interests Of its Clients and stakeholders.

Based on scenario 7, is Yefund's integration of ISMS elements acceptable?

A. No, it is advisable to temporarily delay operational mode until all elements are completed

B. Yes, ISMS elements can be completed, approved, and put into operational mode gradually

C. No, it should have activated the ISMS elements to judge their effectiveness and then completed and approved them based on their performance in operational mode

Answer: B (LEAVE A REPLY)

ISO/IEC 27001:2022 does not require all ISMS components to be launched at once. Gradual implementation-where each ISMS element is validated, approved, and operationalized as ready-is fully acceptable and considered best practice for ensuring effectiveness and risk mitigation.

"It is acceptable to implement and validate ISMS components incrementally, placing each into operational mode as it is completed and approved, so long as the entire system ultimately meets the requirements."

- ISO/IEC 27003:2017, Clause 8.5; ISO/IEC 27001:2022, Clause 4.4

NEW QUESTION: 127
Which of the following is the information security committee responsible for?
A. Ensure smooth running of the ISMS
B. Treat the nonconformities
C. Set annual objectives and the ISMS strategy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Question:
Which statement best describes an organization that has achieved the "Defined" maturity level?
A. The organization has standardized, documented, and communicated its procedures through training sessions
B. The organization has implemented some processes, but there is no standardized procedure
C. The organization has fully automated and integrated its workflows for continuous improvement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
Nimbus Route, a cloud-native logistics optimization company based in the Netherlands, offers Al-driven route planning fleet management tools, and real time shipment tracking solutions to clients across Europe and North America. To safeguard sensitive logistics data and ensure resilience across its cloud services. Nimbus Route has implemented an information security management system (ISMS) based on ISO/IEC 27001. The company is also integrating intelligent transport systems and predictive analytics to increase operational efficiency and sustainability. As part of the ISMS implementation process, the company is determining the competence levels required to manage its ISMS. It has 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 expectations of its customers. Furthermore, the company has 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 have been formally documented: instead, the company classified and managed communication based on its needs. ensuring that documentation is maintained only to the extent necessary for the ISMS's effectiveness To support its expanding digital services and ensure operational scalability. Nimbus Route utilizes virtualized computing resources provided by an external cloud service provider. This setup allows the company to configure and manage its operating systems, deploy applications. and control storage environments as needed while relying on the provider to maintain the underlying cloud environment. To

further enhance is predictive capabilities. Nimbus Route is adopting machine learning techniques across several of its core services Specifically, it uses machine learning for route optimization and delivery time estimation, leveraging algorithms such as logistic regression and support vector machines to identify patterns in historical transportation data. As Nimbus Route's ISMS matures, the company has chosen a chased approach to its transition into full operational mode Rather than waiting for a formal launch, individual elements of the ISMS, such as risk treatment procedures, access controls, and audit logging, are being activated progressively as soon as they are developed and approved Based on the scenario above answer the following question.
According to the last paragraph of scenario 7. which step of the change management process was not conducted accurately?
A. Submit the change request
B. Coordinate the change
C. Review the change request
Answer: (SHOW ANSWER)
The correct answer is B. According to the last paragraph of Scenario 7, Nimbus Route activated ISMS elements progressively as soon as they were developed and approved, but there is no clear evidence that these changes were coordinated across the organization. ISO/IEC 27001:2022 Clause 6.3 - Planning of changes requires that changes to the ISMS be carried out in a planned and coordinated manner, considering:
* Purpose and consequences of the change
* Integrity of the ISMS
* Resource availability
* Assignment of responsibilities
While Nimbus Route clearly submitted changes (Option A) and approved them, the scenario does not explicitly show that cross-functional coordination-such as alignment between IT, compliance, operations, and business units-was consistently performed.
* Option A is incorrect because submitting changes clearly occurred.
* Option C is incorrect because review and approval were explicitly mentioned

NEW QUESTION: 130
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 performance indicators was NOT established by SunDee?
A. ISMS weaknesses
B. Information security cases
C. Training
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
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: (SHOW ANSWER)
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.
1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 11: Certification Audit of the ISMS, slide 13 2:
PECB, ISO/IEC 27001 Lead Implementer Course, Module 11: Certification Audit of the ISMS, slide 14

NEW QUESTION: 132
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: (SHOW ANSWER)

Privileged utility programs (such as those that can bypass access controls or directly manipulate system files) present a significant security risk if misused. ISO/IEC 27001:2022 Annex A control A.8.11 mandates restriction and tight control over these utilities to prevent unauthorized activities and safeguard system integrity.
"The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled."
- ISO/IEC 27001:2022, Annex A, Control 8.11 Privileged utility programs; ISO/IEC 27002:2022, 8.11

NEW QUESTION: 133
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 (LEAVE A REPLY)

NEW QUESTION: 134
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 (LEAVE A REPLY)
Annex A 6.1 (Screening) requires background checks prior to employment, except where prohibited by law, regulation, or collective agreements. An acceptable justification for exclusion is when a collective agreement with employees prohibits such security checks.
"Screening should be carried out for all candidates for employment, subject to relevant laws, regulations, and ethics, and should be proportional to business requirements. Where prohibited by law or collective agreement, exclusion is justified."
- ISO/IEC 27001:2022, Annex A, Control 6.1; ISO/IEC 27002:2022, 6.1

NEW QUESTION: 135
What should an organization demonstrate through documentation?
A. That Its security controls are implemented based on risk scenarios
B. That the distribution of paper copies is regularly complete
C. That the complexity of processes and their interactions is documented
Answer: A (LEAVE A REPLY)

NEW QUESTION: 136

BioLooVitalis is a biopharmaceutical firm headquartered in Singapore Renowned for its pioneering work in the fie d of human therapeutics. BioLooVitalis places a strong emphasis on addressing critical healthcare concerns particularly in the domains of cardiovascular diseases, oncology bone health, and inflammation BioLooVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 77001 for the past two years. After noticing an increase m failed login attempts over several weeks. bioLooVitalis IT security learn reviewed log data, correlated it with user behavior patterns, and mapped it against known attach vectors to determine potential causes. Based on their findings, they prepared a technical report detailing the nature of the anomalies and submitted it to the compliance function. The compliance team then summarized the findings and presented them to the executive management during the quarterly ISMS performance review. To proactively track system behavior following the spike n failed login attempts. BioLooVitalis ' s IT security team configured a dashboard showing real time login activity. system response times, and end point availability across departments. This helped the team quickly detect abnormal behavior without waiting formal reporting cycles. Following The implementation of the real time access control dashboard BioLooVitalis internal audit team assessed whether the new processes and tools effectively reduced unauthorized access attempts and met both technical and policy-based requirements. Lastly, the internal auditors collected system-generated access logs, reviewed user access reports, and conducted interviews with IT personnel. These data sources helped them verify whether the new controls were functioning as intended and aligned with internal ISMS objectives.
Based on The scenario above, answer the following question.
What process is illustrated after increased failed login attempts over several weeks was noticed?
A. Analysis
B. Evaluation
C. Monitoring
Answer: A (LEAVE A REPLY)
After noticing an increase in failed login attempts, BioLooVitalis's IT security team:
Reviewed log data
Correlated it with user behavior
Mapped it against known attack vectors
Determined potential causes
These activities clearly represent analysis, not monitoring or evaluation.
ISO/IEC 27001:2022 Clause 9.1 - Monitoring, measurement, analysis and evaluation differentiates these concepts:
Monitoring = observing and detecting
Analysis = examining data to understand causes and patterns
Evaluation = assessing results against criteria

The team went beyond observation and actively interpreted and correlated data, which is analytical work.

NEW QUESTION: 137
Infralink is a medium-sized IT consultancy firm headquartered in Dublin, Ireland. It specializes in secure cloud infrastructure, software integration, and data analytics, serving a diverse client base in the healthcare, financial services, and legal sectors, including hospitals, insurance providers, and law firms. To safeguard sensitive client data and support business continuity, Infralink has implemented an information security management system (ISMS) aligned with the requirements of ISO/IEC 27001.
In developing its security architecture, the company adopted services to support centralized user identification and shared authentication mechanisms across its departments. These services also governed the creation and management of credentials within the company. Additionally, Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity across its systems.
In preparation for implementing information security controls, the company ensured the availability of necessary resources, personnel competence, and structured planning. It conducted a cost-benefit analysis, scheduled implementation phases, and prepared documentation and activity checklists for each phase. The intended outcomes were clearly defined to align security controls with business objectives.
Infralink started by implementing several controls from Annex A of ISO/IEC 27001. These included regulating physical and logical access to information and assets in accordance with business and information security requirements, managing the identity life cycle, and establishing procedures for providing, reviewing, modifying, and revoking access rights. However, controls related to the secure allocation and management of authentication information, as well as the establishment of rules or agreements for secure information transfer, have not yet been implemented. During the documentation process, the company ensured that all ISMS- related documents supported traceability by including titles, creation or update dates, author names, and unique reference numbers. Based on the scenario above, answer the following question.

Based on scenario -1. which methodology did AegisCure use to implement its ISMS?

A. IMS2

B. PMBOK

C. ISO 10006

Answer: A (LEAVE A REPLY)

The correct and verified answer is Option A - IMS2, which is the methodology specifically designed to support the implementation of ISO/IEC management system standards, including ISO/IEC 27001.

IMS2 (Integrated Management System methodology) is structured to align directly with Annex SL, the harmonized high-level structure used by ISO/IEC 27001:2022. It emphasizes:

Understanding organizational context

Planning based on risks and objectives

Resource and competence management

Phased implementation

Documented information and traceability

Continual improvement

Scenario 3 clearly reflects these elements: Infralink conducted planning, cost-benefit analysis, phased implementation, documentation with traceability, and alignment with business objectives-all hallmarks of the IMS2 methodology.

The other options are not appropriate:

PMBOK is a generic project management framework and does not specifically address ISMS or ISO Annex SL requirements.

ISO 10006 provides guidance on quality management in projects, not ISMS implementation.

ISO/IEC 27001:2022 requires a systematic, standards-aligned methodology for implementation, which IMS2 is designed to provide.

NEW QUESTION: 138

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 (LEAVE A REPLY)

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

The other three risk treatment options are:
Risk avoidance: This option involves eliminating the risk source or discontinuing the activity that causes the risk. For example, Company A could avoid the risk of email compromise by not using email at all, but this would also mean losing the benefits of email communication.
Risk retention: This option involves accepting the risk and its consequences, either because the risk is too low to justify any treatment, or because the cost of treatment is too high compared to the potential loss. For example, Company A could retain the risk of email compromise by not implementing any security measures, but this would expose the company to potential breaches and reputational damage.
Risk transfer: This option involves sharing or transferring the risk to a third party, such as an insurer, a supplier, or a partner. For example, Company A could transfer the risk of email compromise by outsourcing its email service to a cloud provider, who would be responsible for the security and availability of the email accounts.
ISO/IEC 27001:2013, clause 6.1.3: Information security risk treatment
ISO/IEC 27001 Lead Implementer Course, Module 4: Planning the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001 ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC
27001
ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide - Advisera1 Infosec Risk Treatment for ISO 27001 Requirement 8.3 - ISMS.online2 ISO 27001 Clause 6.1.3 Information security risk treatment3 ISO 27001 Risk Treatment Plan - Scrut Automation4

NEW 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 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 systems approach
B. The systematic approach
C. The iterative approach
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
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. Application and data
C. Servers and storage
Answer: (SHOW ANSWER)

NEW QUESTION: 141
According to ISO/IEC 270G1. why shall organizations document nonconformities?
A. To provide evidence of regulations set by external sources that need to be followed by the organization

B. To provide evidence of the results of the corrective actions and the nature of the nonconformities
C. To provide evidence of the requirements set by internal audit after reviewing their audit reports
Answer: B (LEAVE A REPLY)

NEW QUESTION: 142
BotaneBloom is a skincare brand specializing in plant-based formulations. In response to evolving consumer shopping habits, BotaneBloom transitioned to a digital-first business model. During its risk assessment, the company identified that a sudden system crash caused by a malfunctioning server could lead to temporary loss of access to customer orders and inventory data. This malfunction was not linked to any malicious activity.
Under which category does the identified threat related to the system malfunction fall?
A. Technical failure
B. Infrastructure failure
C. Organizational threat
Answer: A (LEAVE A REPLY)
ISO/IEC 27005:2022 classifies threats into categories such as technical failures, human actions, environmental events, and organizational issues. A malfunctioning server causing system crashes - with no malicious activity involved - is a classic example of a technical failure. Technical failures include hardware malfunctions, software crashes, system overloads, and equipment breakdowns. Infrastructure failure typically refers to broader utility disruptions (power outages, connectivity loss), while the scenario specifies a server-level malfunction, not a facility-level failure. Organizational threats relate to management or governance deficiencies. Since the threat originates from a server technical malfunction unrelated to external or human causes, it is correctly classified as a technical failure per ISO/IEC 27005 threat categorization guidelines, which distinguish between failure of equipment and broader infrastructure events.

NEW QUESTION: 143
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, 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 (LEAVE A REPLY)
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.
ISO/IEC 27001 : 2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Clause 16.1.7, Collection of evidence ISO/IEC 27001 : 2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Annex A.16.1.7, Collection of evidence ISO/IEC 27001 : 2022 Lead Implementer Study Guide, Chapter 9, Information security incident management

NEW QUESTION: 144
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.

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

A. Risk acceptance
B. Risk treatment
C. Risk evaluation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 145
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
D. It must be controlled, maintained, and available as necessary to support the operation of the ISMS
Answer: D (LEAVE A REPLY)
The primary requirement for the documented information of an ISMS (Information Security Management System) is that it must be appropriately controlled, maintained, and made available as necessary to support the operation and effectiveness of the ISMS.
Relevant Extract:
ISO/IEC 27001:2022, Clause 7.5 (Documented information) states:
"The organization's information security management system shall include documented information required by this document and determined by the organization as being necessary for the effectiveness of the ISMS.
Documented information required by the information security management system and by this document shall be controlled to ensure it is available and suitable for use, where and when it is needed." ISO/IEC 27001:2022, Clause 7.5.3 (Control of documented information) specifically requires:
"Documented information required by the information security management system and by this document shall be controlled to ensure:
- it is available and suitable for use, where and when it is needed;
- it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity)." There is no requirement for ISMS documentation to exist only in digital format (A), to be public (C), or to be arbitrarily flexible to any change trigger (B). Control and availability as needed are the requirements.
References:
ISO/IEC 27001:2022, Clause 7.5, 7.5.3

NEW QUESTION: 146
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: (SHOW ANSWER)
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) PECB ISO/IEC 27001 Lead Implementer Course Manual, page 107 PECB ISO/IEC 27001 Lead Implementer Info Kit, page 7 ISO/IEC 27001:2022 (en), Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clause 9.3.3 1

NEW QUESTION: 147
What is the primary purpose of the Zachman Framework in enterprise architecture?
A. To automate IT operations across multiple departments, enabling faster service delivery and system integration
B. To prescribe detailed implementation procedures for IT service management
C. To organize and evaluate enterprise artifacts, enabling better analysis and planning
Answer: C (LEAVE A REPLY)
The Zachman Framework is a taxonomy for enterprise architecture, not a methodology, process model, or automation tool. Its primary purpose is to organize, classify, and evaluate enterprise artifacts in a structured and logical manner so that enterprises can achieve better analysis, completeness, consistency, and planning across business and IT domains. Therefore, Option C is the correct and verified answer.
The framework is structured as a 6×6 matrix, intersecting six interrogatives (What, How, Where, Who, When, Why) with six stakeholder perspectives (Planner, Owner, Designer, Builder, Subcontractor, and Enterprise).
Each cell represents a unique architectural artifact, ensuring that no critical viewpoint or enterprise concern is overlooked. Importantly, the Zachman Framework does not prescribe implementation steps, workflows, or operational procedures. Instead, it provides a

classification schema that enables organizations to understand what architectural artifacts exist, what is missing, and how they relate to one another.
This clearly eliminates:
Option A, because the Zachman Framework does not automate IT operations or enable service delivery.
Option B, because it does not prescribe detailed IT service management procedures.
Alignment with ISO/IEC 27001:2022Although the Zachman Framework is not an ISO standard, it strongly supports the architectural and contextual requirements of ISO/IEC 27001:2022 by enabling structured analysis of organizational context, assets, processes, and responsibilities.
This aligns directly with:
Clause 4.1 - Understanding the organization and its context, which states:"The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its information security management system." Clause 4.2 - Understanding the needs and expectations of interested parties, which requires systematic identification and evaluation of stakeholder requirements.
By organizing enterprise artifacts across business, data, application, and technology dimensions, the Zachman Framework provides a foundation for informed risk assessment, scope definition, and control selection, all of which are essential to an effective ISMS.