PECB.ISO-IEC-27001-Lead-Implementer.v2026-03-02.q141

Exam Code:	ISO-IEC-27001-Lead-Implementer
Exam Name:	PECB Certified ISO/IEC 27001 Lead Implementer Exam
Certification Provider:	PECB
Free Question Number:	141
Version:	v2026-03-02
# of views:	107
# of Questions views:	1419
https://www.freecram.net/torrent/PECB.ISO-IEC-27001-Lead-Implementer.v2026-03-02.q141.html	

NEW QUESTION: 1
What category of decision-making does the implementation of an ISMS belong to within an organization's framework?
A. Tactical
B. Operational
C. Strategic
Answer: (SHOW ANSWER)
The decision to implement an Information Security Management System (ISMS) is a strategic decision, made at the highest management level. ISO/IEC 27001:2022 emphasizes that top management must demonstrate leadership and commitment, and integration of the ISMS into the organization's strategic direction.
"Top management shall ensure that the information security policy and the objectives of the ISMS are compatible with the strategic direction of the organization."
- ISO/IEC 27001:2022, Clause 5.1

NEW QUESTION: 2
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:

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

A. Supporting assets

B. Business assets

C. Financial assets

Answer: (SHOW ANSWER)

NEW QUESTION: 3

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

What does the percentage represent?

A. Measurement objective

B. Attribute

C. Performance indicator

Answer: (SHOW ANSWER)

According to the ISO/IEC 27001:2022 standard, a performance indicator is "a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization" (section
3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements1 ISO/IEC 27001 Lead Implementer Info Kit Key performance indicators for an ISO 27001 ISMS2

NEW QUESTION: 4
SkyFleet did not submit action plans within the specified deadline and was not recommended for certification.
Is this acceptable?
A. No, SkyFleet should receive an extension
B. No, SkyFleet should be recommended for certification
C. Yes, SkyFleet should not be recommended for certification
Answer: (SHOW ANSWER)
Certification can only be recommended if all major nonconformities are addressed in the timeframe specified by the certification body. Failure to submit action plans on time means the organization is not meeting ISO
/IEC 27001 requirements and cannot be recommended for certification.
"If the organization does not address nonconformities within the agreed timeframe, the certification body shall not recommend certification until corrective actions are completed." - ISO/IEC 17021-1:2015, Clause 9.5.1; ISO/IEC 27006:2015

NEW QUESTION: 5
What distinguishes the internal auditor's role in evaluating the ISMS risk management process from that of an external auditor?
A. The internal auditor only observes and reports risks without engagement.
B. The internal auditor may actively participate in identifying and assessing risks as an interested party.
C. The internal auditor must defer all risk evaluations to the external audit team.
Answer: (SHOW ANSWER)
An internal auditor differs from an external auditor primarily in organizational role and engagement level.

While both must remain objective and impartial, internal auditors are part of the organization and may actively participate as interested parties in improving risk management processes-provided independence is preserved.
ISO/IEC 27001:2022 Clause 9.2 allows internal audits to be conducted by the organization itself, and ISO
19011 recognizes that internal auditors may provide insight, advice, and feedback to improve management systems. This can include participating in risk identification and assessment discussions, especially where they are not auditing their own work.
* Option A is incorrect because internal auditors do more than observe; they evaluate and may recommend improvements.
* Option C is incorrect because internal auditors do not defer all risk evaluations to external auditors; they play an active assurance role.
External auditors, by contrast, must remain strictly independent and cannot participate in risk identification or assessment, as this would compromise certification impartiality.

NEW QUESTION: 6
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.
After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.
However, the company requested from the certification body that the documentation could not be carried off- site However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body Based on scenario 10. NetworkFuse did not conduct a self-evaluation of the ISMS before the audit. Is this compliant to ISO/IEC 27001?
A. No, the auditee must review the requirements of clauses 4 to 10 before the conduct of a certification audit
B. Yes, the standard indicates that the auditee shall rely only on internal audit and management review reports to prepare for the certification audit
C. Yes, the standard does not require to conduct a self-evaluation before the audit but it is a good practice to follow
Answer: (SHOW ANSWER)

According to the ISO/IEC 27001:2022 standard, the organization is responsible for establishing, implementing, maintaining and continually improving the information security management system (ISMS) in accordance with the requirements of the standard (section 4.1). The standard does not explicitly require the organization to conduct a self-evaluation of the ISMS before the certification audit, which is an external audit performed by an independent certification body to verify the conformity of the ISMS with the standard and to grant the certification (section 9.3.2). However, the standard does require the organization to conduct internal audits (section 9.2) and management reviews (section 9.3) of the ISMS at planned intervals to ensure its effectiveness, suitability and adequacy, and to identify opportunities for improvement and corrective actions.
Therefore, conducting a self-evaluation of the ISMS before the certification audit is a good practice to follow, as it can help the organization to prepare for the audit, to identify any gaps or nonconformities, and to demonstrate its commitment and readiness for the certification.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements1 ISO/IEC 27001 Lead Implementer Info Kit SELF EVALUATION CHECKLIST ISO/IEC 27001:20222

NEW QUESTION: 7
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:
Which ISMS boundaries did OperazeIT include in its ISMS scope?
A. Solely information system boundaries
B. Organizational and physical boundaries
C. Physical boundaries only
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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: (SHOW ANSWER)
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: 9
Which dashboard did SecureLynx use to report the results of implemented processes and controls?
A. Operational dashboards
B. Tactical dashboards
C. Strategic dashboard
Answer: (SHOW ANSWER)
Operational dashboards are used to report on the real-time status of processes and controls, providing transparency and accountability for day-to-day operations. These dashboards allow stakeholders to monitor ongoing security measures and make informed,

timely decisions, aligning with ISO/IEC 27001's requirement for performance evaluation and continual improvement.
"Operational dashboards provide real-time, process-level visibility for continuous monitoring and improvement of controls and processes."
- ISO/IEC 27001:2022, Clause 9.1; ISO/IEC 27004:2016, Section 6.3

NEW QUESTION: 10
A. HealthGenic might not be able to renew the ISMS certificate, as it has not conducted management reviews at planned intervals
B. HealthGenic might not be able to renew the ISMS certificate, as the internal audit lasted longer than planned
C. HealthGenic will be able to renew the ISMS certificate, as they did not detect any information security incident in the past two years
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Levo Corporation has implemented a demilitarized zone (DMZ) and virtual private network (VPN) to secure its network. What controls did Levo Corporation implement in this case?
A. Preventive controls
B. Detective controls
C. Corrective controls
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Scenario 5: Bytes iS a dynamic and innovative Company specializing in the design, manufacturing. and distribution Of hardware and software, with a focus On providing comprehensive network and supporting services. It is headquartered in the vibrant tech hub of Lagos, Nigeria. It has a diverse and dedicated team, boasting a workforce of over 800 employees who are passionate about delivering cutting-edge solutions to their Clients. Given the nati-jte Of its business. Bytes frequently handles sensitive data both internally and When collaborating With Clients and partners.
Recognizing the Challenges inherent in securely sharing data with clients. partners, and within its own internal operations. Bytes has implemented robust information security measures, They utilize a defined risk assessment process, which enables them to assess and address potential threats and information security risks.
This process ensures compliance with ISOflEC 27001 requirements, a critical aspect of Bytes' operations.
Initially. Bytes identified both external and internal issues that are relevant to its purpose and that impact its ability to achieve the intended information security management System Outcomes, External issues beyond the company'S control include factors Such as social and Cultural dynamics, political. legal.

normative, and regulatory environments, financial and macroeconomic conditions. technological developments, natural factors, and competitive pressures. Internal issues, which are within the organization's control, encompass aspects like the company's culture. its policies, objectives, and strategies; govetnance structures.
roles, and responsibilities: adopted standards and guidelines; contractual relationships that influence processes within the ISMS scope: processes and procedures resources and knowledge capabilities; physical infrastructure information systems. information flows. and decisiorwnaking processes; as well as the results of previous audits and risk assessments. Bytes also focused on identifying the interested parties relevant to the ISMS understanding their requirements, and determining which Of those requirements will be addressed by the ISMS In pursuing a secure digital environment, Bytes leverages the latest technology, utilizing automated vulnerability scanning tools to identify known vulnerable services in their ICT systems. This proactive approach ensures that potential weaknesses are swiftly addressed. bolstering their overall information security posture.
In their comprehensive approach to information security, Bytes has identified and assessed various risks. During this process, despite implementing the security controls, Bytes' expert team identified unacceptable residual risks, and the team Currently faces uncertainty regarding which specific options to for addressing these identified and unacceptable residual risks.
According to Scenario 5, which type of policy did Bytes formulate?
A. High-level specific policies
B. High-level general policies
C. Topic-specific policies
Answer: (SHOW ANSWER)
The scenario highlights Bytes establishing overall direction for its information security efforts, describing comprehensive, organization-wide approaches rather than policies tailored to specific topics or technical details. High-level general policies are those which set the overall direction, support, and rules for information security management, in line with ISO/IEC 27001:2022 Annex A 5.1.
"An information security policy shall be defined, approved by management, published and communicated. It provides high-level direction and support for information security."
- ISO/IEC 27001:2022, Annex A, Control 5.1
- ISO/IEC 27002:2022, 5.1

NEW QUESTION: 13
What is the primary purpose of risk analysis?
A. To comprehend the nature of risk and determine its level
B. To implement risk treatment measures
C. To assess vulnerabilities and determine their source
Answer: (SHOW ANSWER)

Risk analysis is conducted to understand the nature of risk and determine its level, which is essential for making informed risk treatment decisions. This process is outlined in ISO/IEC 27001:2022, Clause 6.1.2 and further detailed in ISO/IEC 27005:2022.
"The aim of risk analysis is to comprehend the nature of risk and determine its level."
- ISO/IEC 27001:2022, Clause 6.1.2; ISO/IEC 27005:2022, 8.3

NEW QUESTION: 14
What potential vulnerability in AI systems could be exploited for malicious purposes?
A. High computational power
B. Lack of real-time processing capabilities
C. Adversarial manipulation of data inputs
Answer: (SHOW ANSWER)
Adversarial manipulation of data inputs refers to attackers deliberately crafting input data to mislead AI/ML models, causing them to make incorrect predictions or classifications. This is a well-known AI/ML vulnerability that can be exploited for attacks.
"Adversarial examples are crafted inputs to ML models that cause the model to make a mistake. Protecting against adversarial manipulation is critical for AI system security."
- ISO/IEC 27001:2022, Annex A 8.19; ISO/IEC 27005:2022; NIST SP 800-53 Rev. 5

NEW QUESTION: 15
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 incorrectly implemented a security control that could become a vulnerability
C. Org Y has implemented an integrity control that avoids the involuntary corruption of data
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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: (SHOW ANSWER)

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: 17
Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company's departments within the ISMS scope.
The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.
Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top

management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.
Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.
Based on scenario 5. in which category of the interested parties does the MR manager of Operaze belong?
A. Positively influenced interested parties, because the ISMS will increase the effectiveness and efficiency of the HR Department
B. Negatively influenced interested parties, because the HR Department will deal with more documentation
C. Both A and B
Answer: B (LEAVE A REPLY)
According to ISO/IEC 27001, interested parties are those who can affect, be affected by, or perceive themselves to be affected by the organization's information security activities, products, or services.
Interested parties can be classified into four categories based on their influence and interest in the ISMS:
Positively influenced interested parties: those who benefit from the ISMS and support its implementation and operation Negatively influenced interested parties: those who are adversely affected by the ISMS and oppose its implementation and operation High-interest interested parties: those who have a strong interest in the ISMS and its outcomes, regardless of their influence Low-interest interested parties: those who have a weak interest in the ISMS and its outcomes, regardless of their influence In scenario 5, the HR manager of Operaze belongs to the category of negatively influenced interested parties, because he/she perceives that the ISMS will create more paperwork and documentation for the HR Department, and therefore opposes its implementation and operation. The HR manager does not benefit from the ISMS and does not support its objectives and requirements.
ISO/IEC 27001:2013, clause 4.2: Understanding the needs and expectations of interested parties ISO/IEC 27001:2013, Annex A.18.1.4: Assessment of and decision on information security events ISO/IEC 27001 Lead Implementer Course, Module 2: Introduction to Information Security Management System (ISMS) concepts as required by ISO/IEC 27001 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

NEW QUESTION: 18
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: 19
An organization has decided to conduct information security awareness and training sessions on a monthly basis for all employees. Only 45% of employees who attended these sessions were able to pass the exam.
What does the percentage represent?
A. Measurement objective

B. Performance indicator
C. Attribute
Answer: (SHOW ANSWER)
According to the ISO/IEC 27001:2022 standard, a performance indicator is "a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization" (section
3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements1 ISO/IEC 27001 Lead Implementer Info Kit Key performance indicators for an ISO 27001 ISMS2

NEW QUESTION: 20
A. Yes, as the top management gave the final approval.
B. No, because the scope statement was too simple.
C. No, because the scope statement should have been developed entirely by top management.
Answer: (SHOW ANSWER)
The correct and verified answer is Option A.
ISO/IEC 27001:2022 places clear responsibility on top management for approval of key ISMS elements, including the ISMS scope.
Under Clause 5.1 - Leadership and commitment, top management must demonstrate leadership by ensuring the ISMS is established and compatible with the organization's strategic direction. Additionally, Clause 4.3 requires the ISMS scope to be documented and maintained as documented information.
While the standard does not explicitly state "top management must author the scope," it is expected that top management approves it, as part of governance and accountability.
* Option B is incorrect because simplicity of scope wording is not a nonconformity if it is accurate and complete.
* Option C is incorrect because the scope does not need to be developed entirely by top management- only approved by them.
Conclusion: Since top management gave final approval, the ISMS scope approval process was handled correctly and in full alignment with ISO/IEC 27001:2022, making Option A the correct answer.

NEW QUESTION: 21

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: B (LEAVE A REPLY)
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: 22
A healthcare organization needs to ensure that patient records are available to the medical staff whenever needed. Which measure should it prioritize to achieve this?
A. Implementing multi-factor authentication
B. Establishing record retention policies
C. Using version control systems for data management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
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: (SHOW ANSWER)

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: 24

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 outlined the responsible party for approving its action plan for the revamp of the company's entire data management system?

A. Yes, the employees directly involved in implementing the actions should approve the action plans

B. No, the responsibility for approving action plans lies on top management

C. No, an independent third party should be responsible for approving action plans

D. Yes, any employee can approve as long as they are part of the team

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, the responsibility for ensuring that corrective actions (including major action plans for system-wide changes) are appropriate and adequately resourced rests with top management.

While input from those directly implementing the changes is essential, the standard places ultimate accountability for the ISMS, including the approval of major action plans, on top management.
Relevant Extracts:
"Top management shall demonstrate leadership and commitment with respect to the information security management system by... ensuring that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization... ensuring the integration of the information security management system requirements into the organization's processes; ensuring that the resources needed... are available."
- ISO/IEC 27001:2022, Clause 5.1 (Leadership and commitment)
"Top management shall assign the responsibility and authority for... ensuring that the information security management system conforms to the requirements of this International Standard; reporting on the performance of the information security management system to top management."
- ISO/IEC 27001:2022, Clause 5.3 (Organizational roles, responsibilities and authorities)
Approval of significant action plans (such as a full revamp of the data management system) is a management responsibility, as it can impact resourcing, strategy, and risk management at the organizational level. Input from those implementing the actions is vital for effectiveness, but the formal approval must come from top management or a designated authority within management.
References:
ISO/IEC 27001:2022, Clause 5.1 and 5.3 (Leadership, Roles, and Responsibilities)
ISO/IEC 27001:2022 Implementation Guidance, Section 10 (Corrective Action and Improvement) Summary:
While operational staff and those implementing the plan should be closely involved in its creation and execution, top management must approve major corrective action plans.
Therefore, the correct answer is:
B). No, the responsibility for approving action plans lies on top management

NEW QUESTION: 25
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: (SHOW ANSWER)

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: 26
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, what is the role of Sven in the UX Software?
A. ISMS project manager
B. ISMS project champion
C. Member of the project team
Answer: (SHOW ANSWER)
Sven is described as a "key member of the top management team at UX Software [who] assumed the role of project sponsor, a critical position responsible for ensuring the execution of ISMS implementation with adequate resources." The project sponsor or project champion is the executive who provides leadership, secures resources, and drives the ISMS initiative forward.
"Top management shall assign roles and responsibilities for the ISMS project, including a project sponsor or champion who ensures adequate resourcing and organizational support."
- ISO/IEC 27003:2017, 5.3; ISO/IEC 27001:2022, Clause 5.3

NEW QUESTION: 27
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: (SHOW ANSWER)
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: 28
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the
[^involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Based on the scenario above, answer the following question:
According to scenario 1, which of the following controls implemented by Antiques is a detective and administrative control?
A. Review of all user access rights
B. Enable the automatic update feature of the new software
C. Review of the information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security- related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on the last paragraph of scenario 6, which principles of an effective communication strategy did Colin NOT follow?

A. Transparency and credibility

B. Credibility and responsiveness

C. Appropriateness and clarity

Answer: (SHOW ANSWER)

According to ISO/IEC 27001 : 2022 Lead Implementer, an effective communication strategy should follow some principles, such as transparency, credibility, appropriateness, clarity, responsiveness, and consistency.

These principles help to ensure that the communication is relevant, accurate, understandable, timely, and coherent. Based on the last paragraph of scenario 6, it seems that Colin did not follow the principles of appropriateness and clarity. Appropriateness means that the communication should be tailored to the needs, expectations, and level of understanding of the audience. Clarity means that the communication should be simple, concise, and precise, avoiding ambiguity and jargon. However, Colin explained the information security issues in a too technical manner, which made Lisa confused and unable to comprehend the session.

Therefore, Colin should have adapted his communication style and content to suit the HR personnel, who may not have the same technical background as him.

ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 7.4 Communication ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 12, Information security communication

1, ISO 27001 Communication Plan - How to create a good one

2, ISO 27001 Clause 7.4 - Ultimate Certification Guide

NEW QUESTION: 30

A. To protect the production environment and data from compromise by development and test activities

B. To Identify organizational assets and define appropriate protection responsibilities

C. To validate if information security requirements are met when applications are deployed to the production environment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 31

Question:

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

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

B. To ensure secure system design principles are followed
C. To ensure software is written securely to reduce information security vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 32
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: (SHOW ANSWER)
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: 33
Scenario 2:
Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.
In response to the rapidly evolving landscape of consumer shopping habits, Beauty transitioned from traditional retail to an e-commerce model. To initiate this strategy, Beauty conducted a comprehensive information security risk assessment, analyzing potential

threats and vulnerabilities associated with its new e- commerce venture, aligned with its business strategy and objectives.
Concerning the identified risks, the company implemented several information security controls. All employees were required to sign confidentiality agreements to emphasize the importance of protecting sensitive customer data. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.
After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.
During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action.
Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.
To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in.
Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.
Based on scenario 2, which information security requirement was NOT assessed by Beauty?
A. Principles and objectives for the information life cycle
B. Alignment of the risk assessment with the organization's strategy
C. Compliance with legal, regulatory, and contractual obligations
Answer: (SHOW ANSWER)

NEW QUESTION: 34

Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management
[^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.
First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted What should TradeB do in order to deal with residual risks?
Refer to scenario 4.
A. TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment
B. TradeB should immediately implement new controls to treat all residual risks
C. TradeB should accept the residual risks only above the acceptance level
Answer: (SHOW ANSWER)
According to ISO/IEC 27001 : 2022 Lead Implementer, residual risk is the risk remaining after risk treatment. Residual risk should be compared with the acceptable level of risk, which is the level of risk that the organization is willing to tolerate. If the residual risk is below the acceptable level of risk, then the risk can be accepted. If the residual risk is above the acceptable level of risk, then additional risk treatment options should be considered. Therefore, TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment, which is the difference between the initial risk and the residual risk. This will help TradeB to determine whether the risk treatment was effective and whether the residual risk is acceptable or not.
ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process

NEW QUESTION: 35

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: 36

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: (SHOW ANSWER)

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: 37

Scenario 10: CircuitLinking is a company specializing in water purification solutions, designing and manufacturing efficient filtration and treatment systems for both residential and commercial applications.

Over the past two years, the company has actively implemented an integrated management system (IMS) that aligns with both ISO/IEC 27001 for information security and ISO 9001 for quality management. Recently, the company has taken a significant step forward by applying for a combined audit, aiming to achieve certification against both ISO/IEC 27001 and ISO 9001.

In preparation for the certification audit, CircuitLinking ensured a clear understanding of ISO/IEC 27001 within the company and identified key subject-matter experts to assist the auditors. It also allocated sufficient resources and performed a self-assessment to verify that processes were clearly defined, roles and responsibilities were segregated, and documented information was maintained. To avoid delays, the company gathered all necessary documentation in advance to provide evidence that procedures were in place and effective.

Following the successful completion of the Stage 1 audit, which focused on verifying the design of the management system, the Stage 2 audit was conducted to examine the

implementation and effectiveness of the information security and quality management systems.
One of the auditors, Megan, was a previous employee of the company. To uphold the integrity of the certification process, the company notified the certification body about the potential conflict of interest and requested an auditor change. Subsequently, the certification body selected a replacement, ensuring impartiality. Additionally, the company requested a background check of the audit team members; however, the certification body denied this request. The necessary adjustments to the audit plan were made, and transparent communication with stakeholders was maintained.
The audit process continued seamlessly under the new auditor's guidance. Upon audit completion, the certification body evaluated the results and conclusions of the audit and CircuitLinking's public information and awarded CircuitLinking the combined certification.
A recertification audit for CircuitLinking was conducted to verify that the company's management system continued to meet the required standards and remained effective within the defined scope of certification.
CircuitLinking had implemented significant changes to its management system, including a major overhaul of its information security processes, the adoption of new technology platforms, and adjustments to comply with recent changes in industry legislation. Due to these substantial updates, the recertification audit required a Stage 1 assessment to evaluate the impact of these changes.
According to Scenario 10, is the request made by CircuitLinking to replace Megan acceptable?
A. Yes, but no other auditor should have been assigned in her place
B. No, as long as she remains impartial, she can audit CircuitLinking
C. Yes, considering her past as an employee for CircuitLinking
D. No, only the same auditor can complete the full audit cycle
Answer: C (LEAVE A REPLY)
According to ISO/IEC 17021-1:2015 (the international standard for bodies providing audit and certification of management systems), impartiality is a foundational requirement for the credibility and trustworthiness of the audit and certification process. The standard specifies that audit teams must be free from conflicts of interest, including recent employment with the auditee, which could impair actual or perceived impartiality.
Relevant Extract:
ISO/IEC 17021-1:2015, Clause 5.2.7:
"The certification body shall require personnel, internal and external, to reveal any situation known to them that may present them or the certification body with a conflict of interest. Certification bodies shall use this information as input to identifying and resolving conflicts of interest." ISO/IEC 17021-1:2015, Clause 9.2.2.3:
"The certification body shall ensure that, where an auditor has provided management system consultancy, including being employed by the client organization, there is a minimum period of two years before that auditor can participate in an audit or other

certification activities of that client." Even if Megan can remain impartial, her previous employment at CircuitLinking can create a perception of bias or a conflict of interest, and ISO best practices are to replace such an auditor to ensure impartiality.
CircuitLinking's request for replacement is both reasonable and encouraged under ISO/IEC 17021-1.
References:
ISO/IEC 17021-1:2015, Clauses 5.2.7 and 9.2.2.3
ISO/IEC 27001:2022 Implementation Guidance, Auditor Impartiality and Conflict of Interest
Summary:
A client's request to replace an auditor with a potential conflict of interest-such as a previous employment relationship-is not only acceptable but also aligned with international best practices for impartiality and objectivity in the certification process.
C). Yes, considering her past as an employee for CircuitLinking

NEW QUESTION: 38
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: (SHOW ANSWER)
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: 39
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: 40

A. Risk acceptance

B. Risk evaluation

C. Risk treatment

Answer: (SHOW ANSWER)

NEW QUESTION: 41

Scenario 1:

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

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

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

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

Therefore, HealthGenic decided to prioritize controls related to organizational structure, including segregation of duties, job rotations, job descriptions, and approval processes.

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

Additionally, the company promptly assessed the unauthorized access and data alterations.
To ensure that all employees, including interns, are aware of the importance of data security and the proper handling of patient information, HealthGenic included controls tailored to specifically address employee training, management reviews, and internal audits. Additionally, given the sensitivity of patient data, HealthGenic implemented strict confidentiality measures, including robust authentication methods, such as multi-factor authentication.
In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.
Which information security principle was impacted by the alteration of medical records?
A. Confidentiality
B. Integrity
C. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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: 43
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security- related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.
One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an

honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on scenario 6. Lisa found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. What does this indicate?

A. Lisa did not take actions to acquire the necessary competence

B. The effectiveness of the training and awareness session was not evaluated

C. Skyver did not determine differing team needs in accordance to the activities they perform and the intended results

Answer: (SHOW ANSWER)

According to the ISO/IEC 27001:2022 Lead Implementer Training Course Guide1, one of the requirements of ISO/IEC 27001 is to ensure that all persons doing work under the organization's control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. To achieve this, the organization should determine the necessary competence of persons doing work under its control that affects its information security performance, provide training or take other actions to acquire the necessary competence, evaluate the effectiveness of the actions taken, and retain appropriate documented information as evidence of competence. The organization should also determine differing team needs in accordance to the activities they perform and the intended results, and provide appropriate training and awareness programs to meet those needs.

Therefore, the scenario indicates that Skyver did not determine differing team needs in accordance to the activities they perform and the intended results, since Lisa, who works in the HR Department, found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. This implies that the session was not tailored to the specific needs and roles of the HR personnel, and that the information security expert did not consider the level of technical knowledge and skills required for them to perform their work effectively and securely.

ISO/IEC 27001:2022 Lead Implementer Training Course Guide1

ISO/IEC 27001:2022 Lead Implementer Info Kit2

NEW QUESTION: 44

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, Julia revised the action plan to ensure alignment with best practices
B. Yes, as action plan submission can be flexible
C. No, as action plans are typically expected to meet specified deadlines
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Scenario 7: InfoSec is a multinational corporation headquartered in Boston, MA, which provides professional electronics, gaming, and entertainment services. After facing numerous information security incidents, InfoSec has decided to establish teams and implement measures to prevent potential incidents in the future Emma, Bob. and Anna were hired as the new members of InfoSec's information security team, which consists of a security architecture team, an incident response team (IRT) and a forensics team Emma's job is to create information security plans, policies, protocols, and training to prepare

InfoSec to respond to incidents effectively Emma and Bob would be full-time employees of InfoSec, whereas Anna was contracted as an external consultant.
Bob, a network expert, will deploy a screened subnet network architecture This architecture will isolate the demilitarized zone (OMZ) to which hosted public services are attached and InfoSec's publicly accessible resources from their private network Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company's network. Bob is also responsible for ensuring that a thorough evaluation of the nature of an unexpected event is conducted, including the details on how the event happened and what or whom it might affect.
Anna will create records of the data, reviews, analysis, and reports in order to keep evidence for the purpose of disciplinary and legal action, and use them to prevent future incidents. To do the work accordingly, she should be aware of the company's information security incident management policy beforehand Among others, this policy specifies the type of records to be created, the place where they should be kept, and the format and content that specific record types should have.
Based on this scenario, answer the following question:
Based on his tasks, which team is Bob part of?
A. Security architecture team
B. Forensics team
C. Incident response team
Answer: (SHOW ANSWER)
Based on his tasks, Bob is part of the incident response team (IRT) of InfoSec. According to ISO/IEC 27035-
2:2023, the IRT is a team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way1. One of the tasks of the IRT is to conduct an evaluation of the nature of an unexpected event, including the details on how the event happened and what or whom it might affect1.
This is consistent with Bob's responsibility of ensuring that a thorough evaluation of the nature of an unexpected event is conducted. Therefore, Bob belongs to the incident response team.
ISO/IEC 27035-2:2023 (en), Information technology - Information security incident management - Part 2:
Guidelines to plan and prepare for incident response1
Response to Information Security Incidents | ISMS.online2

NEW QUESTION: 46
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: 47
Which service category provided by the incident response teams supports organ national functions such as training and auditing?
A. Proactive services

B. Reactive services
C. Security quality management services
Answer: (SHOW ANSWER)
Incident response team service categories typically include reactive, proactive, and security quality management services. Proactive services are designed to support organizational functions such as training, awareness, readiness, and auditing, with the aim of preventing incidents before they occur.
These services include:
* Security awareness and training
* Simulations and exercises
* Readiness assessments
* Advisory support to audits
This aligns with ISO/IEC 27001:2022's preventive intent, particularly:
* Clause 7.2 - Competence
* Clause 7.3 - Awareness
* Annex A A.5.35 - Independent review of information security
Reactive services (Option B) focus on incident handling after an event, while security quality management services (Option C) focus on metrics and maturity oversight.

NEW QUESTION: 48
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.
According to Scenario 8, did SecureLynx follow the recommended steps when reviewing and approving the internal audit objectives?
A. No, the internal auditor should review and approve internal audit objectives
B. No, the information security manager should review and approve internal audit objectives
C. Yes, the top management should review and approve the internal audit objectives
Answer: (SHOW ANSWER)
ISO/IEC 27001:2022, Clause 9.2.2, states that top management should approve internal audit objectives to ensure they are aligned with organizational goals and priorities. This helps ensure the ISMS supports the business strategy.
"The internal audit programme shall be approved by top management to ensure objectives are aligned with the organization's strategy and the ISMS's requirements."
- ISO/IEC 27001:2022, Clause 9.2.2

NEW QUESTION: 49
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: (SHOW ANSWER)
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: 50
A. Information security committee
B. Steering committee
C. Operational committee
Answer: (SHOW ANSWER)
The scenario states: "UX Software established a committee responsible for ensuring the effectiveness of corrective actions, managing the ISMS documented information, and continually improving the ISMS while addressing nonconformities." Such roles are typically fulfilled by a steering committee, which oversees ISMS governance and continual improvement, rather than day-to-day operations or tactical incident response.
"An ISMS steering committee should be established to oversee ISMS effectiveness, review corrective actions, and guide continual improvement."
- ISO/IEC 27003:2017, 7.4; ISO/IEC 27001:2022, Clause 9.3

NEW QUESTION: 51
An organization has justified the exclusion of control 5.18 Access rights of ISO/IEC 27001 in the Statement of Applicability (SoA) as follows: "An access control reader is already installed at the main entrance of the building." Which statement is correct'
A. The justification for the exclusion of a control is not required to be included in the SoA
B. The justification is not acceptable, because it does not reflect the purpose of control 5.18
C. The justification is not acceptable because it does not indicate that it has been selected based on the risk assessment results
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, clause 6.1.3, the Statement of Applicability (SoA) is a document that identifies the controls that are applicable to the organization's ISMS and explains why they are selected or not. The SoA is based on the results of the risk assessment and risk treatment, which are the previous steps in the risk management process. Therefore, the justification for the exclusion of a control should be based on the risk assessment results and the risk treatment plan, and should reflect the purpose and objective of the control.
Control 5.18 of ISO/IEC 27001:2022 is about access rights to information and other associated assets, which should be provisioned, reviewed, modified and removed in

accordance with the organization's topic-specific policy on and rules for access control. The purpose of this control is to prevent unauthorized access to, modification of, and destruction of information assets. Therefore, the justification for the exclusion of this control should explain why the organization does not need to implement this control to protect its information assets from unauthorized access.
The justification given by the organization in the question is not acceptable, because it does not reflect the purpose of control 5.18. An access control reader at the main entrance of the building is a physical security measure, which is related to control 5.15 of ISO/IEC 27001:2022, not control 5.18. Control 5.18 is about logical access rights to information systems and services, which are not addressed by the access control reader. Therefore, the organization should either provide a valid justification for the exclusion of control 5.18, or include it in the SoA and implement it according to the risk assessment and risk treatment results.
ISO/IEC 27001:2022, clause 6.1.3, control 5.18; PECB ISO/IEC 27001 Lead Implementer Course, Module 5, slide 18, Module 6, slide 10.

NEW QUESTION: 52
Which statement is an example of risk retention?
A. An organization has decided to release the software even though some minor bugs have not been fixed yet
B. An organization has implemented a data loss protection software
C. An organization terminates work in the construction site during a severe storm
Answer: A (LEAVE A REPLY)
According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, either because the bugs are not critical or because the cost of fixing them would outweigh the benefits.
ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process
3, ISO 27001: Top risk treatment options and controls explained

NEW QUESTION: 53
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.
According to scenario 7, did Yefund correctly define Level 2 of Kirkpatrick's four-level training evaluation model?
A. Yes, at this level, Yefund should evaluate the training's learning outcomes by determining what the trainees learned from it
B. No, at this level, Yefund should measure the trainees' involvement in the training and determine their general impressions of the training
C. No, at this level, Yefund should evaluate the behavior of trainees after the training
Answer: (SHOW ANSWER)
Level 2 of Kirkpatrick's model focuses on learning outcomes-the knowledge, skills, or attitudes participants have acquired. Measuring impressions or engagement (Level 1: Reaction) and post-training behavior (Level
3: Behavior) are separate, subsequent stages.
"Level 2: Learning-measures what participants have learned as a result of the training (knowledge, skills, attitudes)."
- ISO/IEC 27001:2022, Clause 7.2; Kirkpatrick, D.L., Evaluating Training Programs: The Four Levels

NEW QUESTION: 54
How is an "information need' typically defined in the context of ISMS monitoring?
A. As a detailed technical specification
B. As a predefined list of controls to monitor
C. As a high level security question or statement
Answer: (SHOW ANSWER)
In the context of ISMS monitoring, an "information need" is typically defined as a high-level security question or statement that management wants answered to support decision-making. It frames what information is required and why, rather than specifying how it will be technically measured.
ISO/IEC 27001:2022 Clause 9.1 - Monitoring, measurement, analysis and evaluation requires organizations to determine:
* what needs to be monitored and measured,
* methods for monitoring and measurement,
* when monitoring and measurement shall be performed,
* and when results shall be analyzed and evaluated.
An information need precedes metrics and indicators. Examples include:
* "Are access controls preventing unauthorized access?"
* "Is incident response timely and effective?"

These are high-level questions, not technical specifications (Option A) and not predefined control lists (Option B). Metrics, dashboards, and KPIs are derived after the information need is defined.
This approach ensures that monitoring remains business-relevant and risk-focused, aligning measurement with objectives and management review requirements.

NEW QUESTION: 55
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.
Based on Scenario 9, SkyFleet did not take any measures in certain situations when the employees do not behave as expected by procedures and policies. Is this acceptable?
A. Yes, as it pertains to a limited number of employees and is not deemed a significant concern
B. Yes, it is acceptable when the issues are limited in scope
C. No, they should have taken action to control and correct it

D. Yes, if the ISMS review is pending

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, organizations must address nonconformities-regardless of their scale or scope-to ensure the effectiveness of the ISMS. Clause 10.1 ("Nonconformity and corrective action") states:

"When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity;

3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; e) make changes to the information security management system, if necessary."

- ISO/IEC 27001:2022, Clause 10.1

The standard does not provide exceptions for minor or limited-scope nonconformities. All nonconformities must be addressed to prevent recurrence and to maintain and improve the ISMS. Failure to do so would be a direct violation of the ISO/IEC 27001:2022 requirements and could lead to a loss of certification or an increased risk to the organization.

References:

ISO/IEC 27001:2022, Clause 10.1 ("Nonconformity and corrective action") ISO/IEC 27001:2022 Implementation Guide, Section 10 (Continual improvement and corrective action) Summary:

Regardless of the scale or the number of employees involved, SkyFleet must take corrective action when procedures and policies are not followed. The correct answer is: C). No, they should have taken action to control and correct it

NEW QUESTION: 56

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: 57
Question:
Which statement best describes an organization that has achieved the "Defined" maturity level?
A. The organization has implemented some processes, but there is no standardized procedure
B. The organization has fully automated and integrated its workflows for continuous improvement
C. The organization has standardized, documented, and communicated its procedures through training sessions
Answer: (SHOW ANSWER)
According to the ISO/IEC 27003:2017 and various ISMS implementation maturity models (e.g., COBIT, CMMI), a "Defined" maturity level implies:
"Processes are well-characterized and understood, and are described in standards, procedures, tools, and methods. These are communicated through training and organizational policy." This level ensures repeatability and consistency. It is higher than "initial" or "basic" maturity where ad hoc approaches dominate but does not yet include automation (which would fall under "Managed" or
"Optimized").
References:
ISO/IEC 27003:2017 Clause 5 - ISMS implementation guidance
ISMS Toolkit Implementation Guide - Maturity Models (Defined Level)==========

NEW QUESTION: 58
Scenario 3: Auto Tsaab, a Swedish Car manufacturer founded in and headquartered in Sweden, iS well- known for its innovation in the automotive industry, Despite this Strong reputation, the company has faced considerable challenges managing its documented information.
Although manual methods of handling this information may have been sufficient in the past, they now pose substantial challenges. particularly in efficiency, accuracy, and scalability. Moreover, entrusting the responsibility Of managing documented information to

a single individual creates a critical vulnerability, introducing a potential single point Of failure within the organization's information management system, To address these challenges and reinforce its commitment to protecting information assets, Auto Tsaab implemented an information security management system ISMS aligned with ISO/IEC 27001. This move was critical 10 ensuring the security, confidentiality, and integrity of the companys information, particularly as it transitioned from manual to automated information management methods.

initially, Auto Tsaab established automated checking Systems that detect and Correct corruption. By implementing these automated checks, Auto Tsaab not only improved its ability to maintain data accuracy and consistency but also significantly reduced the risk of undetected errors.

Central to Auto ISMS ate documented processes. By documenting essential aspects and processes Such as the ISMS scope, information security policy, operational planning and control, information security risk assessment, internal audit. and management review. Auto Tsaab ensured that these documents were readily available and adequately protected.

Moreover. Auto Tsaab utilizes a comprehensive framework incorporating 36 distinct categories spanning products, services. hardware, and software. This framework. organized in a two-dimensional matrix with six rows and six columns, facilitates the specification of technical details for components and assemblies in its small automobiles. underscoring the company's commitment to innovation and quality, TO maintain the industry standards. Auto Tsaab follows rigorous protocols in personnel selection. guaranteeing that every team member is not only eligible but also well-suited for their respective roles within the organization. Additionally, the company established formal procedures for handling policy violations and appointed an internal consultant to continuously enhance its documentation and security practices.

Based on scenario 3, which control of Annex A does Auto Tsaab apply in the personnel selection process?

A. Annex A 6.4 Disciplinary process

B. Annex A 6.1 Screening

C. Annex A 6.3 Information Security awareness, education, and training

Answer: B (LEAVE A REPLY)

Auto Tsaab "follows rigorous protocols in personnel selection, guaranteeing that every team member is not only eligible but also well-suited for their respective roles within the organization." This directly aligns with Annex A 6.1 Screening, which requires verification of candidates' suitability prior to employment.

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

- ISO/IEC 27001:2022, Annex A, Control 6.1 Screening

NEW QUESTION: 59
Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company's departments within the ISMS scope.
The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.
Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.
Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.
Based on scenario 5. after migrating to cloud. Operaze's IT team changed the ISMS scope and implemented all the required modifications Is this acceptable?
A. Yes, because the ISMS scope should be changed when there are changes to the external environment
B. No, because the company has already defined the ISMS scope
C. No, because any change in ISMS scope should be accepted by the management
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, clause 4.3, the organization shall determine the scope of the ISMS by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organizations. The scope shall be available as documented information and shall state what is included and what is excluded

from the ISMS. The scope shall be reviewed and updated as necessary, and any changes shall be approved by the top management. Therefore, it is not acceptable for the IT team to change the ISMS scope and implement the required modifications without the approval of the management.
ISO/IEC 27001:2022, clause 4.3; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 10.

NEW QUESTION: 60
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: 61
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: (SHOW ANSWER)
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: 62
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 aspect of the internal audit was addressed by BioLooVital s? Refer to scenario 8

A. Evaluation of effectiveness and efficiency of ISMS life cycle

B. Evaluation of effectiveness and efficiency of processes and controls

C. Evaluation of ISMS measurement review

Answer: (SHOW ANSWER)

In Scenario 8, BioLooVitalis's internal audit team assessed whether new processes and tools effectively reduced unauthorized access attempts and met both technical and policy-based requirements. This activity squarely addresses the evaluation of the effectiveness and efficiency of processes and controls, making Option B the correct answer.

ISO/IEC 27001:2022 Clause 9.2 - Internal audit requires that the organization conduct internal audits to provide information on whether the ISMS:

* conforms to the organization's own requirements and ISO/IEC 27001 requirements; and
* is effectively implemented and maintained.

The scenario describes auditors examining specific controls (access controls, monitoring dashboards) and processes (log review, reporting, response) to verify that they function as intended and reduce risk. This aligns with evaluating controls and processes, not the entire ISMS lifecycle (Option A), nor a narrow review of measurement processes alone (Option C).

Additionally, auditors collected logs, reviewed reports, and conducted interviews, which are classic audit techniques used to test control effectiveness and process efficiency. The

focus was not on redesigning the ISMS or assessing maturity across all lifecycle phases, but on verifying whether the implemented controls achieved their objectives.

NEW QUESTION: 63
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: (SHOW ANSWER)
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: 64
Question:
According to ISO/IEC 27001 controls, why should the use of privileged utility programs be restricted and tightly controlled?
A. To ensure that utility programs are compatible with existing system software
B. To prevent misuse of utility programs that could override system and application controls
C. To enable the correlation and analysis of security-related events

Answer: (SHOW ANSWER)
ISO/IEC 27002:2022 Clause 8.11 addresses "Use of privileged utility programs":
"The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled to prevent misuse." Such tools can provide powerful access or modification capabilities, which if misused can compromise the integrity and confidentiality of systems.
References:
ISO/IEC 27002:2022 Clause 8.11
ISO/IEC 27001:2022 Annex A Control A.8.11

NEW QUESTION: 65
Which layer of the SABSA-model focuses on aligning security architecture with business requirements and drivers?
A. Contextual architecture
B. Component architecture
C. Logical architecture
Answer: (SHOW ANSWER)
The SABSA (Sherwood Applied Business Security Architecture) model is a widely accepted framework for developing risk-driven enterprise information security architectures. The model includes six layers:
Contextual, Conceptual, Logical, Physical, Component, and Operational. Among these, Contextual architecture is the topmost layer and is designed specifically to align the security architecture with the business's goals, drivers, and requirements.
In detail, the Contextual architecture layer answers questions such as:
* What is the business trying to achieve?
* Who are the stakeholders?
* What are the critical business assets?
* What are the risk appetite and tolerance levels?This layer sets the foundation for all subsequent layers and ensures that the security strategy directly supports business objectives and strategic direction.
This makes Option A: Contextual architecture the correct answer, as it focuses on aligning the security architecture with business requirements and drivers.
Relevance to ISO/IEC 27001:2022While the SABSA model is not explicitly part of ISO/IEC 27001:2022, it complements the ISO standard, particularly in how it supports the design and implementation of an effective Information Security Management System (ISMS) aligned with business strategy.
Under ISO/IEC 27001:2022, the following clauses support the alignment of security architecture with business requirements:
* Clause 4.1 - "Understanding the organization and its context": "The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended results of its ISMS."

* Clause 4.2 - "Understanding the needs and expectations of interested parties": "The organization shall determine the interested parties that are relevant to the ISMS and the requirements of these interested parties." These clauses emphasize the importance of understanding the broader business environment, stakeholder expectations, and strategic business drivers-exactly what the SABSA Contextual layer is designed to address.
In summary, the Contextual architecture layer in SABSA aligns directly with the intent and structure of ISO
/IEC 27001:2022 Clause 4, making it the correct and verified choice for this question.

NEW QUESTION: 66
A manufacturing company faced a risk of production delays due to potential supply chain disruptions. After assessing the potential impact of the risk, the company decided to accept the risk, considering the disruption unlikely to significantly affect its operations. Which risk treatment option did the company select in this case?
A. Risk avoidance
B. Risk retention
C. Risk deflection
Answer: (SHOW ANSWER)
Risk retention means accepting the risk, either knowingly or by default, often because it is deemed acceptable or cost-effective compared to the mitigation effort. In this scenario, the company assessed the risk and decided to accept it, which is classic risk retention.
"Risk retention involves knowingly accepting a risk. Risk retention can be a conscious decision based on risk assessment."
- ISO/IEC 27001:2022, Clause 6.1.3, ISO/IEC 27005:2022, Section 8.3.2

NEW QUESTION: 67
The IRT has been notified of a potential compromise in the organization's network. Which type of services would be most appropriate for the IRT to provide in this situation?
A. Proactive services
B. Reactive services
C. Security quality management services
Answer: (SHOW ANSWER)
Reactive services are incident response services provided after an incident or compromise is detected, including incident analysis, containment, eradication, recovery, and post-incident activities.
"Reactive services are provided by an Incident Response Team (IRT) in response to actual or suspected security incidents."
- ISO/IEC 27035-1:2016, Section 6.4; ISO/IEC 27001:2022, Annex A 5.24

NEW QUESTION: 68

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: (SHOW ANSWER)
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: 69
Who is responsible for ensuring that the information security management system (ISMS) achieves its intended outcome(s)?
A. The organization's IT department
B. The top management of the organization
C. The ISMS project manager
Answer: (SHOW ANSWER)

NEW QUESTION: 70
A. Backdoor in the training set
B. Data poisoning
C. Membership inference attack
Answer: (SHOW ANSWER)
ISO/IEC 23894:2023 (Artificial Intelligence Risk Management) and NIST SP 800-207A define Membership Inference Attacks (MIA) as:
"An adversary attempts to determine whether specific data was used in the training phase of a machine learning model." This is a privacy threat and can lead to data breaches, especially with personally identifiable information (PII).
It differs from data poisoning, which manipulates the training process, and backdoors, which alter behavior intentionally.
References:
ISO/IEC 23894:2023 Clause 8.2 - Machine Learning Threats
ISO/IEC 27001:2022 - Controls A.8.10 and A.8.12 (Data protection, leakage prevention)==========

NEW QUESTION: 71

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, has SecureLynx appropriately conducted management reviews?

A. No, management reviews should only occur when there are significant changes to the company's ISMS

B. No, ISO/IEC 27001 requires management reviews to be conducted annually

C. Yes, management reviews are intended to be conducted periodically

Answer: (SHOW ANSWER)

ISO/IEC 27001:2022 requires that management reviews be conducted at planned intervals, not only annually or when there are changes. Reviews every six months, as in SecureLynx, are not only compliant but a best practice.

"Top management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy, effectiveness, and alignment with strategic direction."

- ISO/IEC 27001:2022, Clause 9.3

NEW QUESTION: 72

Scenario 9: CoreBit Systems

CoreBit Systems, with its headquarters m San Francisco, specializes in information and communication technology (ICT) solutions, its clientele primarily includes data

communication enterprises and network operators. The company's core objective is to enable its clients a smooth transition into multi-service providers, aligning their operations with the complex demands of the digital landscape.
Recently. John, the internal auditor of CoreBit Systems, conducted an internal audit which uncovered nonconformities related to their monitoring procedures and system vulnerabilities, in response to the identified nonconformities. CoreBit Systems decided to employ a comprehensive problem-solving approach to solve these issues systematically. The method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of issues. This approach involves several steps. First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.
Following the analysis of the root cause of the nonconformities, CoreBit Systems's ISMS project manager.
Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity.
While assessing potential corrective action for addressing a nonconformity, Julia identified the issue as significant and assessed a high likelihood of its reoccurrence Consequently, she chose to implement temporary corrective actions. Afterward. Julia combined all the nonconformities Into a single action plan and sought approval from the top management. The submitted action plan was written as follows:
A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department.
However. Julia's submitted action plan was not approved by top management The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process, and notably, the revised action plans lacked a defined schedule for execution.
Question:
Which method did CoreBit Systems use to address and prevent reoccurring problems after identifying the nonconformities?
A. The Eight Disciplines Problem Solving (8Ds) method
B. DMAIC (Define, Measure, Analyze, Improve, Control) method
C. Lean Six Sigma method
Answer: (SHOW ANSWER)

The described process matches the 8D (Eight Disciplines) method, commonly used for quality and compliance management. The method includes:
Forming a team
Describing the problem
Implementing containment
Identifying root causes
Choosing corrective actions
Implementing actions
Preventing recurrence
Recognizing contributions
This aligns exactly with CoreBit's approach.
References:
ISO/IEC 27001:2022 Clause 10.1 and 10.2 - Nonconformity and corrective action ISMS Toolkit - Incident & Nonconformity Handling (8D Reference)==========

NEW QUESTION: 73
Scenario 3: Auto Tsaab, a Swedish Car manufacturer founded in and headquartered in Sweden, iS well- known for its innovation in the automotive industry, Despite this Strong reputation, the company has faced considerable challenges managing its documented information.
Although manual methods of handling this information may have been sufficient in the past, they now pose substantial challenges. particularly in efficiency, accuracy, and scalability. Moreover, entrusting the responsibility Of managing documented information to a single individual creates a critical vulnerability, introducing a potential single point Of failure within the organization's information management system, To address these challenges and reinforce its commitment to protecting information assets, Auto Tsaab implemented an information security management system ISMS aligned with ISO/IEC 27001. This move was critical 10 ensuring the security, confidentiality, and integrity of the companys information, particularly as it transitioned from manual to automated information management methods.
initially, Auto Tsaab established automated checking Systems that detect and Correct corruption. By implementing these automated checks, Auto Tsaab not only improved its ability to maintain data accuracy and consistency but also significantly reduced the risk of undetected errors.
Central to Auto ISMS ate documented processes. By documenting essential aspects and processes Such as the ISMS scope, information security policy, operational planning and control, information security risk assessment, internal audit. and management review. Auto Tsaab ensured that these documents were readily available and adequately protected.
Moreover. Auto Tsaab utilizes a comprehensive framework incorporating 36 distinct categories spanning products, services. hardware, and software. This framework. organized in a two-dimensional matrix with six rows and six columns, facilitates the

specification of technical details for components and assemblies in its small automobiles. underscoring the company's commitment to innovation and quality, TO maintain the industry standards. Auto Tsaab follows rigorous protocols in personnel selection. guaranteeing that every team member is not only eligible but also well-suited for their respective roles within the organization. Additionally, the company established formal procedures for handling policy violations and appointed an internal consultant to continuously enhance its documentation and security practices.
According to scenario 3, which security architecture framework does Auto Tsaab utilize?
A. The Open Group Architecture
B. Open Security
C. Zachman
Answer: C (LEAVE A REPLY)
The scenario describes "a comprehensive framework incorporating 36 distinct categories ... organized in a two-dimensional matrix with six rows and six columns." This is a direct reference to the Zachman Framework, which is a well-known enterprise architecture framework structured as a 6x6 matrix.
"The Zachman Framework is a two-dimensional model using six communication interrogatives (What, How, Where, Who, When, Why) intersecting with six player perspectives (Planner, Owner, Designer, Builder, Subcontractor, and Working System)."
- Zachman International; also referenced in ISO/IEC 42010 (architecture frameworks)

NEW QUESTION: 74
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.
After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.
However, the company requested from the certification body that the documentation could not be carried off- site However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body According to scenario 10, NetworkFuse requested from the certification body to review all the documentation only on-site. Is this acceptable?
A. Yes, the auditee may request that the review of the documentation takes place on-site

B. Yes, only if a confidentiality agreement is formerly signed by the audit team
C. No, the certification body decides whether the documentation review takes place on-site or off-site
Answer: (SHOW ANSWER)
According to the ISO/IEC 27001:2022 standard, the certification body is responsible for planning and conducting the audit, including the review of the documented information. The certification body may decide to review the documentation on-site or off-site, depending on the audit objectives, scope, criteria, and risks.
The auditee may not impose any restrictions on the access to the documentation, unless there are valid reasons for confidentiality or security. However, such restrictions should be agreed upon before the audit and should not compromise the effectiveness and impartiality of the audit.
ISO/IEC 27001:2022, clause 9.2.2
ISO/IEC 27006:2021, clause 7.1.4

NEW QUESTION: 75
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. Followingthis, the implementation team conducted a comprehensive review of the company's functional units, opting to include most of the company departments within the ISMS scope. Additionally, the team decided to include internal and external physical locations, both external and internal issues referred to in clause 4.1, the requirements in clause 4.2, and the interfaces and dependencies between activities performed by the company. The IT manager had a pivotal role in approving the final scope, reflecting 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:
Did OperazeIT include all the necessary factors when determining its scope?
A. No, it should have included the interfaces and dependencies between activities performed by other organizations as well
B. No, it should have only considered external issues referred to in 4.1 and the requirements referred to in
4.2
C. Yes, the company adhered to the requirements of ISO/IEC 27001
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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: (SHOW ANSWER)
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: 77
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.
In scenario 3. which security controls did Infrelink implement?
A. 5.14 Information transfer and A.5.17 Authentication information
B. 5.15 Access control. A.5.16 Identity management, and A.5.18 Access rights
C. 5.35 Independent review of information security
Answer: (SHOW ANSWER)
The correct answer is Option B, as it precisely reflects the Annex A controls explicitly implemented by Infralink in Scenario 3.
The scenario states that Infralink implemented controls that:
* Regulate physical and logical access to information and assets
* Manage the identity life cycle
* Establish procedures for providing, reviewing, modifying, and revoking access rights
These map directly to the following ISO/IEC 27001:2022 Annex A organizational controls:
* A.5.15 - Access controlRequires access to information and assets to be restricted in accordance with business and security requirements.
* A.5.16 - Identity managementCovers the establishment, maintenance, and removal of identities throughout their lifecycle.
* A.5.18 - Access rightsRequires formal processes for granting, reviewing, and revoking access rights.
The scenario explicitly notes that A.5.17 (Authentication information) and A.5.14 (Information transfer) have not yet been implemented, which rules out Option A.
Option C is incorrect because A.5.35 - Independent review of information security relates to audit and governance activities, not access or identity controls, and is not referenced in the scenario.

NEW QUESTION: 78
Scenario 10: CircuitLinking is a company specializing in water purification solutions, designing and manufacturing efficient filtration and treatment systems for both residential and commercial applications.
Over the past two years, the company has actively implemented an integrated management system (IMS) that aligns with both ISO/IEC 27001 for information security and ISO 9001 for quality management. Recently, the company has taken a significant step forward by applying for a combined audit, aiming to achieve certification against both ISO/IEC 27001 and ISO 9001.

In preparation for the certification audit, CircuitLinking ensured a clear understanding of ISO/IEC 27001 within the company, identified key subject-matter experts to assist the auditors, allocated sufficient resources, performed a self-assessment, and gathered all necessary documentation in advance. Following the successful completion of the Stage 1 audit (which focused on verifying the design of the management system), the Stage 2 audit was conducted to examine the implementation and effectiveness of the information security and quality management systems.

One of the auditors, Megan, was a previous employee of the company. To uphold the integrity of the certification process, the company notified the certification body about the potential conflict of interest and requested an auditor change. Subsequently, the certification body selected a replacement, ensuring impartiality. Additionally, the company requested a background check of the audit team members; however, the certification body denied this request. The necessary adjustments to the audit plan were made, and transparent communication with stakeholders was maintained.

The audit process continued seamlessly under the new auditor's guidance. Upon audit completion, the certification body evaluated the results and conclusions of the audit and CircuitLinking's public information, and awarded CircuitLinking the combined certification.

A recertification audit for CircuitLinking was conducted to verify that the company's management system continued to meet the required standards and remained effective within the defined scope of certification.

CircuitLinking had implemented significant changes, including a major overhaul of its information security processes, new technology platforms, and adjustments to comply with recent legislative changes. Due to these updates, the recertification audit required a Stage 1 assessment to evaluate the impact.

Which of the following does NOT follow auditing best practices? Refer to Scenario 10.

A. CircuitLinking's request for background information on audit team members being denied

B. CircuitLinking applying for a combined audit

C. The certification body evaluating the audit findings

D. The company notifying the certification body about a conflict of interest

Answer: (SHOW ANSWER)

According to ISO/IEC 17021-1:2015 (which provides the requirements for bodies providing audit and certification of management systems and is referenced by ISO/IEC 27001 audits), clients do not have the right to request or conduct background checks on auditors provided by an accredited certification body, except for potential conflicts of interest or impartiality concerns, which must be disclosed. The certification body is responsible for ensuring the competence, integrity, and impartiality of its auditors.

It is best practice for the certification body to evaluate audit findings and make certification decisions (C).

It is perfectly acceptable and encouraged for organizations to apply for a combined audit for integrated management systems, such as ISO 9001 and ISO/IEC 27001 (B).

Notifying the certification body of a conflict of interest is a best practice and required for audit impartiality (D).
Requesting background checks beyond verifying competence, impartiality, and conflict of interest is NOT aligned with auditing best practices (A), and it is proper for the certification body to deny such a request.
Relevant Extracts:
ISO/IEC 17021-1:2015, Clause 9.2.2.2: "The certification body shall select audit team members and technical experts that, collectively, have the necessary competence for the audit. The certification body shall not provide information that compromises confidentiality or privacy." ISO/IEC 27001:2022 Implementation Guidance, auditing section: "Certification bodies ensure the independence and competence of auditors and maintain impartiality. Organizations may raise concerns about impartiality or conflicts of interest, but certification bodies manage personnel records and background information in accordance with confidentiality requirements." References:
ISO/IEC 17021-1:2015, Clauses 5.2, 9.2.2.2
ISO/IEC 27001:2022 Implementation Guidance, Section on Certification Audits Summary: Requesting a background check on audit team members is not a recognized right or best practice for certified organizations; only impartiality and competence are relevant, and the certification body is responsible for these aspects. Thus, the denial of this request is proper.
A). CircuitLinking's request for background information on audit team members being denied

NEW QUESTION: 79
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: (SHOW ANSWER)

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: 80

A. An extrinsic vulnerability, since it is fin external factor that impacts the asset

B. A type of threat, since it may result in an unwanted incident

C. An intrinsic vulnerability, since it is a characteristic of the asset
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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.
Question:
Has CyTekShield appropriately addressed the handling of evidence related to information security events?
A. No - as it does not include proper training for staff involved in evidence handling
B. Yes - it has appropriately addressed the handling of evidence
C. No - because the process of evidence acquisition was not fully detailed
Answer: B (LEAVE A REPLY)
ISO/IEC 27037:2012 and ISO/IEC 27002:2022 Clause 8.16 - Monitoring activities and Clause 6.8 - Information security event reporting emphasize that:
"Evidence must be appropriately identified, collected, preserved, and protected to ensure it remains reliable and admissible in investigations." CyTekShield's approach covers all major evidence handling practices, including safeguarding devices in powered/unpowered states and defining content format/location, meeting accepted standards.
References:
ISO/IEC 27002:2022 Clause 6.8 & 8.16
ISO/IEC 27037:2012 - Guidelines for evidence handling==========

NEW QUESTION: 82
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: 83
Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.
Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.
Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.
To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.
Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001' Refer to scenario 3.

A. No, the control should be implemented only for defining rules for cryptographic key management

B. Yes, the control for the effective use of the cryptography can include cryptographic key management

C. No, because the standard provides a separate control for cryptographic key management

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, Annex A.8.24, the control for the effective use of cryptography is intended to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This control can include cryptographic key management, which is the process of generating, distributing, storing, using, and destroying cryptographic keys in a secure manner. Cryptographic key management is essential for ensuring the security and functionality of cryptographic solutions, such as encryption, digital signatures, or authentication.

The standard provides the following guidance for implementing this control:

A policy on the use of cryptographic controls should be developed and implemented.

The policy should define the circumstances and conditions in which the different types of cryptographic controls should be used, based on the information classification scheme, the relevant agreements, legislation, and regulations, and the assessed risks.

The policy should also define the standards and techniques to be used for each type of cryptographic control, such as the algorithms, key lengths, key formats, and key lifecycles.

The policy should be reviewed and updated regularly to reflect the changes in the technology, the business environment, and the legal requirements.

The cryptographic keys should be managed through their whole lifecycle, from generation to destruction, in a secure and controlled manner, following the principles of need-to-know and segregation of duties.

The cryptographic keys should be protected from unauthorized access, disclosure, modification, loss, or theft, using appropriate physical and logical security measures, such as encryption, access control, backup, and audit.

The cryptographic keys should be changed or replaced periodically, or when there is a suspicion of compromise, following a defined process that ensures the continuity of the cryptographic services and the availability of the information.

The cryptographic keys should be securely destroyed when they are no longer required, or when they reach their end of life, using methods that prevent their recovery or reconstruction.

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 Understanding Cryptographic Controls in Information Security5

NEW QUESTION: 84

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 scenario 6, is Nimbus Route's method of implementing ISMS components consistent with recommended ISMS deployment practices?

A. Yes, incremental implementation allows for early risk reduction and gradual integration with business processes.

B. No, all ISMS elements must be deployed simultaneously to ensure compliance.

C. No, the ISMS should be fully implemented only after all controls have been finalized and approved.

Answer: (SHOW ANSWER)

Nimbus Route's phased (incremental) activation of ISMS components is fully consistent with recommended ISMS deployment practices, making Option A correct.

ISO/IEC 27001:2022 does not require a "big bang" implementation. Instead, it supports progressive implementation, continual improvement, and risk-based prioritization.

The scenario explains that Nimbus Route:

* Activated ISMS elements as soon as they were developed and approved
* Implemented controls such as risk treatment, access control, and audit logging progressively
* Avoided waiting for a formal, single launch date

This approach aligns with:

* Clause 6.1 - Actions to address risks and opportunities, which encourages early risk mitigation
* Clause 8.1 - Operational planning and control, allowing staged operationalization
* Clause 10.1 - Continual improvement, which supports incremental maturity Options B and C are incorrect because ISO/IEC 27001 does not mandate simultaneous deployment nor does it require waiting until all controls are finalized before operation begins.

NEW QUESTION: 85

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: (SHOW ANSWER)

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: 86

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. which reporting method was used by BioLooVitalis?

A. Operational dashboard

B. Strategic scorecard

C. Gages

Answer: (SHOW ANSWER)

The scenario describes a real-time dashboard displaying:

* Login activity
* System response times
* Endpoint availability

This is the definition of an operational dashboard, which supports day-to-day monitoring and rapid detection of abnormal behavior.

ISO/IEC 27001:2022 Clause 9.1 supports the use of real-time monitoring tools to ensure effective operational control.

* Strategic scorecards (Option B) are used for long-term, high-level performance indicators.
* Gauges (Option C) typically represent single metrics, not integrated views.

NEW QUESTION: 87
A tech company rapidly expanded its operations over the past few years. Its information system, consisting of servers, databases, and communication tools, is a critical part of its daily operations. However, due to the rapid growth and increased data flow, the company is now facing a saturation of its information system. This saturation has led to slower response times, increased downtime, and difficulty in managing the overwhelming volume of dat a. In which category does this threat fall into?
A. Infrastructure failures
B. Technical failures
C. Compromise of functions
Answer: (SHOW ANSWER)

NEW QUESTION: 88
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 avoidance
C. Risk retention
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the
[^involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Intrinsic vulnerabilities, such as the_____ are related to the characteristics of the asset. Refer to scenario 1.
A. Software malfunction
B. Service interruptions
C. Complicated user interface

Answer: (SHOW ANSWER)
Intrinsic vulnerabilities are related to the characteristics of the asset that make it susceptible to threats, regardless of the presence or absence of controls. In scenario 1, the complicated user interface of the web- based medical software is an intrinsic vulnerability, as it is a feature of the software that makes it difficult to use and increases the likelihood of human errors. The software malfunction and the service interruptions are not intrinsic vulnerabilities, but rather incidents that occurred due to external factors, such as the increased number of users or the software company's actions.
ISO/IEC 27001:2022 Lead Implementer Course Content, Module 6: Risk Assessment and Treatment1; ISO
/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 6.1.2: Information security risk assessment2

NEW QUESTION: 90
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: (SHOW ANSWER)

NEW QUESTION: 91
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: (SHOW ANSWER)
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: 92
Scenario 5: Evergreen

Evergreen is undergoing ISMS implementation. In their structure, there exists an Information Security Committee (ISC), which leads and governs security operations.
Question:
Can the information security committee at Evergreen take on the role of the emergency committee in the event of a major incident?
A. No - no one should assume the role of the emergency committee to prevent the mismanagement of major incidents
B. Yes - can assume the role of the emergency committee in the event of a major incident
C. No - only the steering committee can assume the role of the emergency committee
Answer: (SHOW ANSWER)
ISO/IEC 27002:2022 Clause 5.17 - Information Security in Project Management, and Clause 5.2 - Roles and Responsibilities, support role flexibility provided responsibilities are clear and documented.
The same group can assume multiple roles, provided:
The roles are defined
Competency is proven
There is no conflict of interest
It's acceptable and sometimes encouraged for an established, competent committee like the ISC to assume emergency roles during incidents, enhancing response efficiency.
References:
ISO/IEC 27002:2022 Clause 5.2, 5.17
ISO/IEC 27001:2022 Clause 5.3 - Organizational roles, responsibilities, and authorities==========

NEW QUESTION: 93
Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.
Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and

recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management How does SunDee's negligence affect the ISMS certificate? Refer to scenario 8.

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

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

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

Answer: B (LEAVE A REPLY)

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: 94

Scenario 6: GreenWave

GreenWave, a manufacturer of sustainable and energy efficient home appliances, specializes in solar-powered devices, EV chargers, and smart thermostats. To ensure the protection of customer data and internal operations against digital threats, the company

has implemented an ISO/IEC 27001-based information security management system (ISMS). GreenWave is also exploring innovative loT solutions to further improve energy efficiency in buildings GreenWave is committed to maintaining a high standard of information security within its operations As part of its continuous improvement approach, the company is in the process of determining the competence levels required to manage its ISMS. GreenWave considered various factors when defining these competence requirements, including technological advancements, regulatory requirements, the company's mission, strategic objectives, available resources, as well as the needs and expecations of its customers Furthermore, the company remained committed to complying with ISO/IEC 27001's communication requirements. It established clear guidelines for internal and external communication related to the ISMS, defining what information to share, when to share it. with whom, and through which channels. However, not all communications were formally documented; instead, the company classified and managed communication based on its needs, ensuring that documentation was maintained only to the extent necessary for the ISMS effectiveness .

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

Additionally, GreenWave looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for GreenWave's electronic product development According to GreenWave, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. GreenWave assigned Colin the responsibility of determining the materiality of this change within the company.

Question:

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

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

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

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

Answer: (SHOW ANSWER)

ISO/IEC 27001:2022 Clause 7.2 - Competence states:

"The organization shall determine the necessary competence of persons... considering internal and external issues, and the needs and expectations of interested parties relevant

to the ISMS." GreenWave followed this clause by factoring in both internal and external influences, including regulatory and customer requirements. This comprehensive view ensures that assigned personnel are adequately equipped to manage ISMS functions.
References:
ISO/IEC 27001:2022 Clause 7.2 - Competence
ISO/IEC 27001 Implementation Guide - Competence Mapping==========

NEW QUESTION: 95
What does the organization still need to manage when using Platform as a Service (PaaS)?
A. Operating system and virtualization
B. Servers and storage
C. Application and data
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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.
As indicated in scenario 6. what does Nimbus Route s approach to managing its computing environment suggest about the type of cloud service model it uses?
A. Infrastructure as a service
B. Software as a service
C. Platform as a service
Answer: A (LEAVE A REPLY)
Nimbus Route's cloud usage clearly indicates Infrastructure as a Service (IaaS), making Option A the correct and verified answer.
The scenario states that Nimbus Route:
* Uses virtualized computing resources from an external cloud provider
* Configures and manages its own operating systems
* Deploys applications
* Controls storage environments
* Relies on the provider only to maintain the underlying cloud infrastructure These characteristics align precisely with the IaaS service model, where the cloud provider supplies compute, storage, networking, and virtualization, while the customer retains responsibility for operating systems, middleware, applications, and data.
In contrast:
* Software as a Service (SaaS) would not allow Nimbus Route to manage operating systems or storage directly.
* Platform as a Service (PaaS) would abstract away OS management and infrastructure control, which the scenario explicitly says Nimbus Route performs.
From an ISO/IEC 27001:2022 perspective, this distinction is critical for defining shared responsibility under Annex A controls, especially:
* A.5.19 - Information security in supplier relationships
* A.5.23 - Information security for use of cloud services
These controls require organizations to understand which security responsibilities remain with the organization versus the cloud service provider.

NEW QUESTION: 97
Which of the following statements is accurate regarding the methodology for managing the implementation of an ISMS?
A. Organizations can adapt the methodology to their specific context, and steps can be modified as needed
B. Organizations must strictly follow a specific methodology to meet the minimum requirements

C. The sequence of steps must remain fixed throughout the ISMS implementation
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Question:
An organization has compared its actual performance against predetermined performance targets. What is the primary purpose of this action?
A. To verify that all security incidents are resolved
B. To assess whether the organization's security objectives are being met
C. To eliminate the need for manual tracking and reporting
Answer: (SHOW ANSWER)
ISO/IEC 27001:2022 Clause 9.1 - Monitoring, measurement, analysis, and evaluation: "The organization shall evaluate the performance and effectiveness of the information security management system. The evaluation shall include... comparison against performance indicators and security objectives." The purpose is to ensure that security objectives (Clause 6.2) are being met. Measuring performance allows organizations to determine whether controls and processes are effective and aligned with strategic goals. Option A is too narrow, and Option C is incorrect because manual tracking may still be required in some cases.
References:
ISO/IEC 27001:2022 Clause 6.2 and 9.1
ISO/IEC 27004:2016 - Clause 7.2 (Use of metrics for objective evaluation)==========

NEW QUESTION: 99
Is Yefund's development of communication protocols acceptable?
A. Yes, because internal communications are the primary factor influencing information security
B. Yes, because external communications are not relevant to the ISMS
C. No, Yefund should have determined internal and external communications
Answer: (SHOW ANSWER)
ISO/IEC 27001:2022 Clause 7.4 requires that organizations determine both internal and external communications relevant to the ISMS. This includes what to communicate, when, with whom, and how, to ensure stakeholders-including clients and regulators-are properly informed. Focusing only on internal communications is noncompliant.
"The organization shall determine the need for internal and external communications relevant to the information security management system, including on what to communicate, when, with whom, and how."
- ISO/IEC 27001:2022, Clause 7.4

NEW QUESTION: 100
A. Gathering documented information

B. Identifying subject matter experts
C. Preparing the personnel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Which tool is used to identify, analyze, and manage interested parties?
A. The probability/impact matrix
B. The power/interest matrix
C. The likelihood/severity matrix
Answer: (SHOW ANSWER)
The power/interest matrix is a tool that can be used to identify, analyze, and manage interested parties according to ISO/IEC 27001:2022. The power/interest matrix is a two-dimensional diagram that plots the level of power and interest of each interested party in relation to the organization's information security objectives. The power/interest matrix can help the organization to prioritize the interested parties, understand their expectations and needs, and develop appropriate communication and engagement strategies. The power /interest matrix can also help the organization to identify potential risks and opportunities related to the interested parties.
ISO/IEC 27001:2022, clause 4.2; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 12.

NEW QUESTION: 102
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: (SHOW ANSWER)

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: 103

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

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.

Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

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

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

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

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

A. Detective and administrative

B. Corrective and managerial
C. Legal and technical
Answer: A (LEAVE A REPLY)
Preventive controls: These are controls that aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Examples of preventive controls are encryption, firewalls, locks, policies, etc.
Detective controls: These are controls that aim to detect or discover the occurrence of a security incident or its symptoms. Examples of detective controls are logs, alarms, audits, etc.
Corrective controls: These are controls that aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact. Examples of corrective controls are backups, recovery plans, incident response teams, etc.
Administrative controls: These are controls that involve the management and governance of information security, such as policies, procedures, roles, responsibilities, awareness, training, etc.
Technical controls: These are controls that involve the use of technology or software to implement information security, such as encryption, firewalls, anti-malware, authentication, etc.
Physical controls: These are controls that involve the protection of physical assets or locations from unauthorized access, damage, or theft, such as locks, fences, cameras, guards, etc.
Legal controls: These are controls that involve the compliance with laws, regulations, contracts, or agreements related to information security, such as privacy laws, data protection laws, confidentiality agreements, etc.
In scenario 2, the action of Beauty reviewing all user access rights is best described as a "Preventive and Administrative" control.
Preventive Control: The review of user access rights is a preventive measure. It is designed to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to specific files. By controlling access rights, the organization aims to prevent potential security breaches and protect sensitive data.
Administrative Control: This action also falls under administrative controls, sometimes referred to as managerial controls. These controls involve policies, procedures, and practices related to the management of the organization and its employees. In this case, the review of access rights is a part of the company's administrative procedures to manage the security of information systems.
ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements

NEW QUESTION: 104
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: B (LEAVE A REPLY)
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: 105
Scenario 10: CircuitLinking is a company specializing in water purification solutions, designing and manufacturing efficient filtration and treatment systems for both residential and commercial applications.

Over the past two years, the company has actively implemented an integrated management system (IMS) that aligns with both ISO/IEC 27001 for information security and ISO 9001 for quality management. Recently, the company has taken a significant step forward by applying for a combined audit, aiming to achieve certification against both ISO/IEC 27001 and ISO 9001.

In preparation for the certification audit, CircuitLinking ensured a clear understanding of ISO/IEC 27001 within the company and identified key subject-matter experts to assist the auditors. It also allocated sufficient resources and performed a self-assessment to verify that processes were clearly defined, roles and responsibilities were segregated, and documented information was maintained. To avoid delays, the company gathered all necessary documentation in advance to provide evidence that procedures were in place and effective.

Following the successful completion of the Stage 1 audit, which focused on verifying the design of the management system, the Stage 2 audit was conducted to examine the implementation and effectiveness of the information security and quality management systems.

One of the auditors, Megan, was a previous employee of the company. To uphold the integrity of the certification process, the company notified the certification body about the potential conflict of interest and requested an auditor change. Subsequently, the certification body selected a replacement, ensuring impartiality. Additionally, the company requested a background check of the audit team members; however, the certification body denied this request. The necessary adjustments to the audit plan were made, and transparent communication with stakeholders was maintained.

The audit process continued seamlessly under the new auditor's guidance. Upon audit completion, the certification body evaluated the results and conclusions of the audit and CircuitLinking's public information and awarded CircuitLinking the combined certification.

A recertification audit for CircuitLinking was conducted to verify that the company's management system continued to meet the required standards and remained effective within the defined scope of certification.

CircuitLinking had implemented significant changes to its management system, including a major overhaul of its information security processes, the adoption of new technology platforms, and adjustments to comply with recent changes in industry legislation. Due to these substantial updates, the recertification audit required a Stage 1 assessment to evaluate the impact of these changes.

According to Scenario 10, the recertification audit activities at CircuitLinking included a Stage 1 audit. Is this acceptable?

A. No, the stage 1 audit is only required for initial certification

B. Yes, when there are significant changes to the management system, recertification audit activities may need to have a stage 1 audit

C. No, the stage 1 audit is only required when unresolved nonconformities from the previous audit cycle remain and have not been adequately addressed

D. No, stage 1 audits are only for new sites, not recertification

Answer: (SHOW ANSWER)

A Stage 1 audit is typically associated with initial certification, but according to ISO/IEC 17021-1:2015 (which governs certification audits and is referenced in ISO/IEC 27001 audit practice) and ISO/IEC 27006:
2015 (guidance for ISMS certification), a Stage 1 audit may also be required in the context of recertification when there have been significant changes to the management system.
Relevant Extract:
ISO/IEC 17021-1:2015, Clause 9.6.3.2:
"Where there have been significant changes to the management system, the client, or the context in which the management system is operating (e.g., changes in legislation), a Stage 1 audit may be required as part of the recertification audit process." ISO/IEC 27006:2015, Clause 9.4.3.1:
"A stage 1 audit is performed as necessary, for example when there have been significant changes to the client or management system, or new sites are added." Thus, it is entirely in line with ISO/IEC 27001 and international certification practices to require a Stage 1 audit as part of a recertification audit if significant system, process, or context changes have occurred since the previous certification.
References:
ISO/IEC 17021-1:2015, Clause 9.6.3.2
ISO/IEC 27006:2015, Clause 9.4.3.1
ISO/IEC 27001:2022 Implementation Guidance, Recertification Activities
Summary:
A Stage 1 audit may be required for recertification when there are significant changes to the management system, context, or scope. Therefore, the correct answer is:
B). Yes, when there are significant changes to the management system, recertification audit activities may need to have a stage 1 audit

NEW QUESTION: 106

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

A. Organizational

B. Physical

C. Technological

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, the control that enables the organization to manage storage media through their life cycle of use, acquisition, transportation and disposal belongs to the category of physical and environmental security. This category covers the controls that prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. The specific control

objective for this control is A.11.2.7 Secure disposal or reuse of equipment1, which states that "equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse."2 ISO/IEC 27001:2022, Annex A ISO/IEC 27002:2022, clause 11.2.7

NEW QUESTION: 107
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: (SHOW ANSWER)
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: 108
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: (SHOW ANSWER)

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: 109
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: (SHOW ANSWER)
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: 110

A. No, because Bytes selected a method developed in-house
B. Yes, since the risk assessment methodology complied with the ISO/IEC 27001 requirements
C. No, Bytes did not consult with external stakeholders or subject matter experts when selecting the risk assessment methodology
Answer: (SHOW ANSWER)
ISO/IEC 27001:2022 allows organizations to use any risk assessment methodology (including in-house developed), as long as it meets the standard's requirements, is repeatable, and produces consistent and valid results. The scenario confirms that Bytes' method ensures compliance with ISO/IEC 27001, which means it meets the selection criteria.
"The organization shall define and apply an information security risk assessment process that:
a) establishes and maintains information security risk criteria;
b) ensures that repeated assessments produce consistent, valid and comparable results."
- ISO/IEC 27001:2022, Clause 6.1.2

NEW QUESTION: 111
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. No, OpenTech did not have a clear plan to implement a permanent corrective action
B. No, OpenTech decided not to pursue this course of action
C. Yes, OpenTech had a comprehensive plan in place to implement permanent corrective actions
Answer: (SHOW ANSWER)

NEW QUESTION: 112
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: 113
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: (SHOW ANSWER)
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: 114
Nimbus Route, a cloud-native logistics optimization company based in the Netherlands, offers AI-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.
Which type of machine learning is Nimbus Route using to enhance its delivery and scheduling accuracy?
Refer to scenario 6.
A. Reinforcement learning
B. Supervised learning
C. Unsupervised learning
Answer: (SHOW ANSWER)
The correct answer is B. Supervised learning, based on the explicit machine learning techniques described in the scenario.
Nimbus Route uses logistic regression and support vector machines (SVMs) to analyze historical transportation data and improve route optimization and delivery time estimation. These algorithms are classic supervised learning techniques, which rely on labeled datasets to learn relationships between input variables and known outcomes.
In supervised learning:
* Input data is paired with correct outputs (labels),
* Models are trained to predict outcomes based on historical examples,
* Accuracy improves through evaluation against known results.
This exactly matches the scenario's description of learning from historical transportation data to predict delivery times and optimize routes.
* Reinforcement learning (Option A) involves learning through trial-and-error interactions with an environment and reward signals, which is not described.
* Unsupervised learning (Option C) focuses on discovering hidden patterns in unlabeled data, such as clustering, which is also not indicated.
While ISO/IEC 27001:2022 does not prescribe machine learning types, its risk-based approach (Clause 6.1) and emphasis on technology awareness (Clause 7.2) require organizations to understand and competently manage the technologies they deploy-including AI and ML systems.
By clearly identifying and competently applying supervised learning techniques, Nimbus Route demonstrates appropriate technological understanding and governance within its ISMS.

NEW QUESTION: 115
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: (SHOW ANSWER)
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: 116
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: (SHOW ANSWER)
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: 117
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.
Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out- of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
Based on the scenario above, answer the following question:
Which situation described in scenario 2 Indicates service unavailability?
A. Lucas was no! able to access the website with his credentials
B. Attackers still had access to the data when Solena delivered a press release
C. Lucas was asked to change his password weekly
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the
[^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while

using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Based on the scenario above, answer the following question:
According to scenario 1. to detect (1)_____, Antiques should have implemented (2)
A. (1) Patches. (2) an access control software
B. (1) Technical vulnerabilities. (2) network intrusions
C. (1) Intrusions on networks. (?) an intrusion detection system
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts and implement measures to prevent potential incidents in the future.
Emma, Bob, and Anna were hired as the new members of InfoSec's information security team, which consists of a security architecture team, an incident response team (IRT), and a forensics team. Emma's job is to create information security plans, policies, protocols, and training to prepare InfoSec to respond to incidents effectively. Emma and Bob would be full-time employees of InfoSec, whereas Anna was contracted as an external consultant.
Bob, a network expert, will implement a screened subnet network architecture. This architecture will isolate the demilitarized zone (DMZ), to which hosted public services are attached, and InfoSec's publicly accessible resources from their private network. Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company's network. Bob is also responsible for ensuring a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.
On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for disciplinary and legal action and use them to prevent future incidents. To do the work accordingly, she should be aware of the company's information security incident management policy beforehand. Among others, this policy specifies the type of records to be created, the place where they should be kept, and the format and content that specific record types should have.
As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed

and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.
Furthermore, while implementing the communication plan for information security, InfoSec's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.
InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.
Based on this scenario, answer the following question:
Which of the following cloud service models did InfoSec use?
A. Infrastructure as a Service
B. Platform as a Service
C. Software as a Service
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A. Yes, the company relied only on manual methods for managing documented information
B. Yes, the company ensured that documented information was available and protected as needed
C. Yes, the company delegated the responsibility of managing documented information to a single individual
Answer: (SHOW ANSWER)
The scenario states that "Auto Tsaab ensured that these documents were readily available and adequately protected." This aligns directly with ISO/IEC 27001:2022, Clause 7.5, which requires that documented information is available, suitable for use, and adequately protected.
"Documented information required by the ISMS and by this International Standard shall be controlled to ensure it is available and suitable for use, where and when it is needed, and it is adequately protected."
- ISO/IEC 27001:2022, Clause 7.5

NEW QUESTION: 121
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security,

the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security- related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.
One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on scenario 6. when should Colin deliver the next training and awareness session?
A. After he ensures that the group of employees targeted have satisfied the organization's needs
B. After he conducts a competence needs analysis and records the competence related issues
C. After he determines the employees' availability and motivation
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, clause 7.2.3, the organization shall conduct a competence needs analysis to determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization shall also evaluate the effectiveness of the actions taken to acquire the necessary competence and retain appropriate documented information as evidence of competence.
Therefore, Colin should deliver the next training and awareness session after he conducts a competence needs analysis and records the competence related issues, such as the level of understanding, the gaps in knowledge, and the feedback from the participants.
ISO/IEC 27001:2022, clause 7.2.3; PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 8.

NEW QUESTION: 122
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 the controls implemented by Infralink. which category of information security controls do They fall under? Refer to scenario 3.
A. Technological
B. People
C. Organizational
Answer: (SHOW ANSWER)
The correct and verified answer is A. Technological, based on the nature of the controls implemented by Infralink in Scenario 3.
The controls implemented-A.5.15 Access control, A.5.16 Identity management, and A.5.18 Access rights- are enforced primarily through technical mechanisms, such as:
* Centralized identity systems

* Authentication platforms
* Access control lists
* Role-based access control
* System-enforced provisioning and revocation

Although these controls are classified under "Organizational controls" in Annex A's grouping, their implementation and enforcement mechanisms are technological in nature. ISO/IEC 27001:2022 emphasizes that effective security requires technical enforcement, not reliance on human behavior alone.

These controls are supported by technological services such as identity and access management (IAM), directory services, and authentication systems, which automatically enforce restrictions.

* People controls relate to awareness, training, and disciplinary processes.
* Organizational controls define policy and governance.
* Technological controls enforce access restrictions, identity validation, and authorization at system level.

Given that the scenario focuses on centralized identification, shared authentication mechanisms, and system- enforced access control, the implemented controls fall under the Technological category in practice.

NEW QUESTION: 123

Scenario 10: CircuitLinking is a company specializing in water purification solutions, designing and manufacturing efficient filtration and treatment systems for both residential and commercial applications.

Over the past two years, the company has actively implemented an integrated management system (IMS) that aligns with both ISO/IEC 27001 for information security and ISO 9001 for quality management. Recently, the company has taken a significant step forward by applying for a combined audit, aiming to achieve certification against both ISO/IEC 27001 and ISO 9001.

In preparation for the certification audit, CircuitLinking ensured a clear understanding of ISO/IEC 27001 within the company and identified key subject-matter experts to assist the auditors. It also allocated sufficient resources and performed a self-assessment to verify that processes were clearly defined, roles and responsibilities were segregated, and documented information was maintained. To avoid delays, the company gathered all necessary documentation in advance to provide evidence that procedures were in place and effective.

Following the successful completion of the Stage 1 audit, which focused on verifying the design of the management system, the Stage 2 audit was conducted to examine the implementation and effectiveness of the information security and quality management systems.

One of the auditors, Megan, was a previous employee of the company. To uphold the integrity of the certification process, the company notified the certification body about the

potential conflict of interest and requested an auditor change. Subsequently, the certification body selected a replacement, ensuring impartiality. Additionally, the company requested a background check of the audit team members; however, the certification body denied this request. The necessary adjustments to the audit plan were made, and transparent communication with stakeholders was maintained.
The audit process continued seamlessly under the new auditor's guidance. Upon audit completion, the certification body evaluated the results and conclusions of the audit and CircuitLinking's public information and awarded CircuitLinking the combined certification.
A recertification audit for CircuitLinking was conducted to verify that the company's management system continued to meet the required standards and remained effective within the defined scope of certification.
CircuitLinking had implemented significant changes to its management system, including a major overhaul of its information security processes, the adoption of new technology platforms, and adjustments to comply with recent changes in industry legislation. Due to these substantial updates, the recertification audit required a Stage 1 assessment to evaluate the impact of these changes.
According to Scenario 10, the certification body evaluated the results and conclusions of the audit and CircuitLinking's public information when making the certification decision. Is this acceptable?
A. No, the certification body should also consider the auditor's opinions when making the certification decision
B. No, the certification decision must be based solely on the audit findings, and no external information can be considered
C. Yes, the certification body must make the certification decision based on other relevant information, such as public information
D. No, only top management's input should be considered
Answer: (SHOW ANSWER)
ISO/IEC 17021-1:2015 (which sets out the requirements for bodies providing audit and certification of management systems, referenced in ISO/IEC 27001 certification practices) clearly states that the certification body must consider all relevant information when making a certification decision. This includes audit findings and other information, such as public information that may affect the decision, as long as it is relevant and objective.
Relevant Extract:
ISO/IEC 17021-1:2015, Clause 9.5.1 states:
"The certification body shall make decisions regarding granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification based on an evaluation of audit findings and conclusions and any other relevant information (e.g., public information, complaints, etc.)." ISO/IEC 27001:2022 Implementation Guidance supports this:
"Certification bodies may use other relevant information, such as publicly available data, to ensure the integrity and accuracy of the certification process." The certification decision should not be based solely on audit findings (B is incorrect) nor exclusively on auditor

opinion (A is incorrect), but must include any relevant information-this may include public records, regulatory notices, and complaints that can impact certification status.
References:
ISO/IEC 17021-1:2015, Clause 9.5.1
ISO/IEC 27001:2022 Implementation Guidance, Certification Decisions
Summary:
It is not only acceptable but required by ISO/IEC 17021-1 for the certification body to use any relevant information (including public information) to ensure a fair and thorough certification decision.
C). Yes, the certification body must make the certification decision based on other relevant information, such as public information

NEW QUESTION: 124
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: 125
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.
After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.
However, the company requested from the certification body that the documentation could not be carried off- site However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a

recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body NetworkFuse should_____to ensure that employees are prepared for the audit. Refer to scenario 10.

A. Conduct practice interviews

B. Observe the technologies used

C. Select a certification body that provides combined audits

Answer: (SHOW ANSWER)

One of the ways to prepare employees for an ISO/IEC 27001 audit is to conduct practice interviews with them. This can help them to familiarize themselves with the audit process, the types of questions they might be asked, and the evidence they need to provide to demonstrate compliance with the standard. Practice interviews can also help employees to identify any gaps or weaknesses in their knowledge or performance, and to address them before the actual audit. Practice interviews can be conducted by internal auditors, managers, or consultants, and should cover the relevant scope, objectives, and criteria of the audit. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113) PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113 PECB ISO/IEC 27001 Lead Implementer Info Kit, page 10

5 Step Plan: How to Prepare for an ISO 27001 Certification Audit

NEW QUESTION: 126

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

A. The top management

B. The appropriate management

C. The board of directors

Answer: (SHOW ANSWER)

NEW QUESTION: 127

Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation.

SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

In preparation for the recertification audit, SunDee conducted an internal audit. The company's topmanagement appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With

this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.
During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.
SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.
In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.
Based on the scenario above, answer the following question:
Is Alex suitable for the position of internal auditor within the company?
A. No, the internal audit can be conducted only by individuals who have not had operational roles
B. Yes, Alex's recent experience in the day-to-day operations of the Compliance Department would benefit the internal auditor role
C. No, Alex should wait for a reasonable period of time to pass before transitioning to the internal auditor position
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
Which approach should organizations use to implement an ISMS based on ISO/IEC 27001?
A. An approach that is suitable for organization's scope
B. Any approach that enables the ISMS implementation within the 12month period

C. Only the approach provided by the standard

Answer: (SHOW ANSWER)

ISO/IEC 27001:2022 does not prescribe a specific approach for implementing an ISMS, but rather provides a set of requirements and guidelines that can be adapted to the organization's context, scope, and objectives.

Therefore, organizations can use any approach that is suitable for their scope, as long as it meets the requirements of the standard and enables the achievement of the intended outcomes of the ISMS. The approach should also consider the needs and expectations of the interested parties, the risks and opportunities related to information security, and the legal and regulatory obligations of the organization.

ISO/IEC 27001:2022, clause 4.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 9.

NEW QUESTION: 129

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

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

B. The information security manager

C. The internal auditor

Answer: (SHOW ANSWER)

NEW QUESTION: 130

A. Stage 1

B. Stage 2

C. Audit follow-up

Answer: (SHOW ANSWER)

ISO/IEC 17021-1:2015 (used by certification bodies) defines:

Stage 1: Review of documentation, readiness, scope

Stage 2: On-site audit to assess effectiveness and implementation

Follow-up: Only done post-audit if there are nonconformities requiring verification In Scenario 10 (ProEBank), once the auditor conflict was resolved, the audit team visited the site to evaluate implementation-this is a clear Stage 2 audit activity.

References:

ISO/IEC 17021-1:2015 Clauses 9.3.1.2 (Stage 1) and 9.3.1.3 (Stage 2)

ISO/IEC 27006:2015 (Certification of ISMS)

NEW QUESTION: 131

Refer to Scenario 4 (FinSecure)

Finsecure is a financial institution based in Finland, providing services to a diverse clientele, encompassing retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in

the region. Recognizing the critical importance of information security in the modern banking landscape, FinSecure has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.

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

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

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

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

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

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

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

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

Answer: (SHOW ANSWER)

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

"Compare the controls determined in 6.1.3 b) with those in Annex A and verify that no necessary controls have been omitted." Clause 6.1.3 (d) continues:

"Produce a Statement of Applicability that contains the necessary controls, justification for inclusion, whether implemented, and justification for exclusion." The SoA does not require selection of all controls, but rather only those that are applicable based on the context, risk assessment, and needs of the organization. FinSecure's experts complied by selecting relevant controls and documenting justifications-thus aligning with the standard.
References:
ISO/IEC 27001:2022 Clause 6.1.3 (c)-(d)
ISO/IEC 27002:2022 Introduction 0.4 - Determining Controls==========

NEW QUESTION: 132
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: (SHOW ANSWER)
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: 133
Question:
What action should an organization take to ensure the security of information when it is transferred or treated by an external party?
A. Rely on external parties to implement their own security measures
B. Include security clauses in a contractual agreement with the external party
C. Exclude external parties from the ISMS scope to limit risk exposure
Answer: B (LEAVE A REPLY)
ISO/IEC 27002:2022 Clause 5.20 - Addressing information security within supplier agreements states:
"Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and products provided by suppliers." Further emphasized in Clause 5.19 - Information security in supplier relationships, which mandates managing supplier-related risks.
This means contracts must include clauses addressing information security expectations, responsibilities, access rights, compliance, audits, and breach response mechanisms.
References:
ISO/IEC 27002:2022 Clauses 5.19 and 5.20
ISO/IEC 27001:2022 Annex A Control A.5.19 & A.5.20==========

NEW QUESTION: 134
Scenario 2:
Beauty is a well-established cosmetics company in the beauty industry. The company was founded several decades ago with a passion for creating high-quality skincare, makeup, and personal care products that enhance natural beauty. Over the years, Beauty has built a strong reputation for its innovative product offerings, commitment to customer satisfaction, and dedication to ethical and sustainable business practices.

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

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

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

During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action.

Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal, statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.

To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in.

Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.

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

A. Administrative

B. Technical

C. Legal

Answer: (SHOW ANSWER)

NEW QUESTION: 135
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
Based on scenario 6, Clare has established a procedure stating that information security risk assessments are conducted only when significant changes occur. Is the frequency of risk assessments determined correctly?
A. No, she should perform risk assessments quarterly per ISO/IEC 27001 requirements
B. No, she should perform risk assessments annually, as mandated by regulatory authorities
C. No, the company must conduct risk assessments at planned intervals
Answer: C (LEAVE A REPLY)
ISO/IEC 27001:2022 requires that risk assessments be conducted at planned intervals and when significant changes occur. Only conducting risk assessments in response to significant changes is insufficient; a schedule is also required.
"Information security risk assessments shall be performed at planned intervals and when significant changes are proposed or occur."
- ISO/IEC 27001:2022, Clause 6.1.2 (c)

NEW QUESTION: 136
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.

According to scenario 9. did NeuroTrustMed document the change in accordance with continual improvement practices?

A. No, the register should have been implemented in the form of a database rather than a spreadsheet.

B. No, changes should only be recorded if they result from nonconformities.

C. Yes, the change was documented in a structured spreadsheet with appropriate metadata and formal approval.

Answer: (SHOW ANSWER)

NeuroTrustMed documented the ISMS change in full accordance with continual improvement practices, making Option C the correct answer.

ISO/IEC 27001:2022 Clause 10.1 - Continual improvement and Clause 10.2 - Nonconformity and corrective action require organizations to:

* Record changes,
* Track actions taken,
* Retain documented information as evidence.

The scenario states that NeuroTrustMed maintained an improvement register containing:

* A unique change number,
* Description of the update,
* Priority classification,
* Initiation and completion dates,
* Formal sign-off by the information security manager.

This fully satisfies Clause 7.5 - Documented information and demonstrates controlled, auditable improvement.

* Option A is incorrect because ISO/IEC 27001 does not mandate a database over a spreadsheet.
* Option B is incorrect because improvements may result from regulatory changes, risks, or opportunities-not only nonconformities.

NEW QUESTION: 137
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: 138
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. No, as it should perform them twice a year, regardless of significant changes
B. Yes, it adhered to ISO/IEC 27001 requirements
C. No, as it should perform them at planned intervals as well
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Who should be involved, among others, in the draft, review, and validation of information security procedures?
A. An external expert
B. The information security committee
C. The employees in charge of ISMS operation
Answer: B (LEAVE A REPLY)
According to ISO/IEC 27001:2022, clause 7.5.1, the organization shall ensure that the documented information required by the ISMS and by this document is controlled to ensure

that it is available and suitable for use, where and when it is needed, and that it is adequately protected. This includes ensuring that the documented information is reviewed and approved for suitability and adequacy. The information security procedures are part of the documented information that supports the operation of the ISMS processes and the implementation of the information security controls. Therefore, they should be drafted, reviewed, and validated by the information security committee, which is the group of people responsible for overseeing the ISMS and ensuring its alignment with the organization's objectives and strategy. The information security committee should include representatives from different functions and levels of the organization, as well as external experts if needed. The information security committee should also ensure that the information security procedures are communicated to the relevant employees and other interested parties, and that they are periodically reviewed and updated as necessary.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clauses 5.3, 7.5.1, and 9.3
ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

NEW QUESTION: 140

A. Organizational threats
B. Physical threats
C. Compromise of functions or services
D. Natural threats
Answer: (SHOW ANSWER)
Insufficient resources-such as lack of personnel, expertise, funding, or time-are classic examples of organizational threats. According to ISO/IEC 27001:2022 and ISO/IEC 27005:2022 (Information security risk management), organizational threats refer to weaknesses or risks arising from internal factors such as management failures, resource limitations, lack of awareness, or process gaps.
ISO/IEC 27001:2022 Clause 6.1.2 ("Information security risk assessment") requires organizations to identify risks arising from organizational weaknesses, which include inadequate allocation of resources for the ISMS:
"The organization shall determine risks that need to be addressed to give assurance that the information security management system can achieve its intended outcomes and prevent, or reduce, undesired effects." Reference:
ISO/IEC 27001:2022, Clause 6.1.2
ISO/IEC 27005:2022, Section 8.2.2 (Examples of threats - Organizational threats)

NEW QUESTION: 141

Scenario 5: OperazelT is a software development company that develops applications for various companies worldwide. Recently, the company conducted a risk assessment in response to the evolving digital landscape and emerging information security challenges. Through rigorous testing techniques like penetration testing and code review, the company

identified issues in its IT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, 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:

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

A. Policy construction

B. Risk assessment
C. Policy implementation
Answer: (SHOW ANSWER)