PECB.ISO-IEC-27001-Lead-Implementer.v2026-02-11.q133

Exam Code:	ISO-IEC-27001-Lead-Implementer
Exam Name:	PECB Certified ISO/IEC 27001 Lead Implementer Exam
Certification Provider:	PECB
Free Question Number:	133
Version:	v2026-02-11
# of views:	109
# of Questions views:	1647
https://www.freecram.net/torrent/PECB.ISO-IEC-27001-Lead-Implementer.v2026-02-11.q133.html	

NEW QUESTION: 1
Scenario 7: InfoSec, based in Boston, MA, is a multinational corporation offering professional electronics, gaming, and entertainment products. Following several information security incidents, InfoSec has decided to establish teams of experts and implement measures to prevent potential incidents in the future.
Emma, Bob, and Anna were hired as the new members of InfoSec's information security team, which consists of a security architecture team, an incident response team (IRT), and a forensics team. Emma's job is to create information security plans, policies, protocols, and training to prepare InfoSec to respond to incidents effectively. Emma and Bob would be full-time employees of InfoSec, whereas Anna was contracted as an external consultant.
Bob, a network expert, will implement a screened subnet network architecture. This architecture will isolate the demilitarized zone (DMZ), to which hosted public services are attached, and InfoSec's publicly accessible resources from their private network. Thus, InfoSec will be able to block potential attackers from causing unwanted events inside the company's network. Bob is also responsible for ensuring a thorough evaluation of the nature of an unexpected event, including how the event happened and what or whom it might affect.
On the other hand, Anna will create records of the data, reviews, analyses, and reports to keep evidence for disciplinary and legal action and use them to prevent future incidents. To do the work accordingly, she should be aware of the company's information security incident management policy beforehand. Among others, this policy specifies the type of records to be created, the place where they should be kept, and the format and content that specific record types should have.

As part of InfoSec's initiative to strengthen information security measures, Anna will conduct information security risk assessments only when significant changes are proposed and will document the results of these risk assessments. Upon completion of the risk assessment process, Anna is responsible for developing and implementing a plan for treating information security risks and documenting the risk treatment results.
Furthermore, while implementing the communication plan for information security, InfoSec's top management was responsible for creating a roadmap for new product development. This approach helps the company to align its security measures with the product development efforts, demonstrating a commitment to integrating security into every aspect of its business operations.
InfoSec uses a cloud service model that includes cloud-based apps accessed through the web or an application programming interface (API). All cloud services are provided by the cloud service provider, while data is managed by InfoSec. This introduces unique security considerations and becomes a primary focus for the information security team to ensure data and systems are protected in this environment.
Based on this scenario, answer the following question:
Is the responsibility of InfoSec's top management appropriately established in implementing the communication plan for information security?
A. Yes, the top management is responsible for creating a new product development roadmap as an activity during the communication plan implementation
B. No, the top management is responsible for communicating only technical specifications for products
C. No, the top management is responsible for allocating resources for communication activities
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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 dat a. 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, any employee can approve as long as they are part of the team

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 3

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, Nigeri a. 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.
Based on scenario 5, certain residual risks were defined as unacceptable. Which risk treatment options should Bytes consider?
A. Bytes should suspend all operations until risks are fully eliminated
B. Bytes should terminate the affected projects immediately
C. Bytes should identify alternative risk treatment options
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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. Performance indicator
B. Measurement objective
C. Attribute
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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. Evaluate the need for action to eliminate the causes of the nonconformity so that it does not recur or occur elsewhere
B. React to the nonconformity, take action to control and correct it. and deal with its consequences

C. Communicate the details of the nonconformity to every employee of the organization and suspend the employee that caused the nonconformity
Answer: (SHOW ANSWER)

NEW QUESTION: 6
What should an organization demonstrate through documentation?
A. That the distribution of paper copies is regularly complete
B. That the complexity of processes and their interactions is documented
C. That Its security controls are implemented based on risk scenarios
Answer: (SHOW ANSWER)

NEW QUESTION: 7
How should the level of detail in risk identification evolve over time?
A. It should focus on highly detailed assessments conducted on an ad-hoc basis rather than broad risk assessments
B. It should be performed in full detail only when significant changes occur in the organization
C. It should be refined gradually through iterative assessments, increasing the level of detail over time
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Scenario 6: Skyver manufactures electronic products, such as gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware. and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well informed by security principles and practices.
One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained the existing Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues In a supportive manner, Colin suggested Lisa to consider attending the session again.

Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver's commitment to improving the customer experience through data-driven insights.
Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.
According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.
Based on the scenario above, answer the following question:
How should Colin have handled the situation with Lisa?
A. Assign an individual the responsibility to provide Lisa with personalized explanations for her technical issues
B. Deliver training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company
C. Organize separate technical training sessions exclusively for Lisa
Answer: (SHOW ANSWER)

NEW QUESTION: 9
How can SkyFleet demonstrate its ongoing commitment to continual improvement in information security?
A. By publishing an annual report on information security performance
B. By letting employees take independent action ensures swift problem resolution
C. By outsourcing its information security responsibilities to a third-party vendor
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A. After he ensures that the group of employees targeted have satisfied the organization's needs
B. After he determines the employees' availability and motivation
C. After he conducts a competence needs analysis and records the competence related issues
Answer: (SHOW ANSWER)

NEW QUESTION: 11
What is the primary requirement for the documented information of an ISMS?

A. It must be sufficiently flexible to adapt to any identified change triggers
B. It must be accessible to the public at all times to maintain transparency
C. It must be controlled, maintained, and available as necessary to support the operation of the ISMS
D. It must exist solely in a digital format to ensure modern compatibility
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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 27011
C. ISO/IEC 27009
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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. No, at this level, Yefund should measure the trainees' involvement in the training and determine their general impressions of the training
B. No, at this level, Yefund should evaluate the behavior of trainees after the training
C. Yes, at this level, Yefund should evaluate the training's learning outcomes by determining what the trainees learned from it
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only

authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
Based on scenario 2, Beauty should have implemented
(1)_____ to detect (2)_____.
A. (1) Network intrusions, (2) technical vulnerabilities
B. (1) An access control software, (2) patches
C. (1) An intrusion detection system, (2) intrusions on networks
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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. Clarity
B. Transparency
C. Timeliness
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j^ombined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS. However, the company requested from the certification body that the documentation could not be carried off-site However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body Based on the scenario above, answer the following question:
Does NetworkFuse fulfill the prerequisites for a certification audit?
A. Yes, because the certification body has been selected
B. Yes, because internal audits and management reviews have been performed
C. Yes, because the ISMS must be operational for at least one year prior to the certification audit
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a

thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.
Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.
The company also implemented a control to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.
Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.
Based on the scenario above, answer the following question:
Which of the following controls did Socket Inc. implement by conducting pre-employment background checks? Refer to scenario 3.
A. Annex A 6.7 Remote working
B. Annex A 6.1 Screening
C. Annex A 6.4 Disciplinary process
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Scenario:
Evergreen tailored the format and naming convention of their information security policy to align with their internal structure and needs.

Is this acceptable?
A. No - the policy must adhere to the predefined template set by ISO/IEC 27001
B. Yes - the organization can determine the formats and names of these policy documents that meet the organization's needs
C. No - the policy format and naming conventions must be approved by an external auditor before being implemented
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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 dat a. The company thoroughly reviewed user access rights, ensuring only authorized personnel could access sensitive information. In addition, since the company stores valuable products and unique formulas in the warehouse, it installed alarm systems and surveillance cameras with real-time alerts to prevent any potential act of vandalism.
After a while, the information security team analyzed the audit logs to monitor and track activities across the newly implemented security controls. Upon investigating and analyzing the audit logs, it was discovered that an attacker had accessed the system due to out-of-date anti-malware software, exposing customers' sensitive information, including names and home addresses. Following this, the IT team replaced the anti-malware software with a new one capable of automatically removing malicious code in case of similar incidents. The new software was installed on all workstations and regularly updated with the latest malware definitions, with an automatic update feature enabled. An authentication process requiring user identification and a password was also implemented to access sensitive information.
During the investigation, Maya, the information security manager of Beauty, found that information security responsibilities in job descriptions were not clearly defined, for which the company took immediate action. Recognizing that their e-commerce operations would have a global reach, Beauty diligently researched and complied with the industry's legal,

statutory, regulatory, and contractual requirements. It considered international and local regulations, including data privacy laws, consumer protection acts, and global trade agreements.
To meet these requirements, Beauty invested in legal counsel and compliance experts who continuously monitored and ensured the company's compliance with legal standards in every market they operated in. Additionally, Beauty conducted multiple information security awareness sessions for the IT team and other employees with access to confidential information, emphasizing the importance of system and network security.
What type of controls did Beauty implement to ensure the safety of products and unique formulas stored in the warehouse?
A. Administrative
B. Legal
C. Technical
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
A. Yes - the company identified all supporting assets as part of the asset identification process
B. No - the company identified only business assets
C. No - the company identified only the valuable information and some organizational processes
Answer: (SHOW 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, what is Michael's role at NyvMarketing?
A. ISMS auditor
B. Incident manager
C. Risk owner
D. Crisis manager
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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 at planned intervals as well
B. No, as it should perform them twice a year, regardless of significant changes
C. Yes, it adhered to ISO/IEC 27001 requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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:

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 24
An organization has established a policy that provides the personnel with the information required to effectively deploy encryption solutions in order to protect organizational confidential dat a. What type of policy is this?
A. Topic-specific policy
B. High-level topic-specific policy
C. High-level general policy
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which tool is used to identify, analyze, and manage interested parties?
A. The power/interest matrix
B. The likelihood/severity matrix
C. The probability/impact matrix
Answer: (SHOW ANSWER)

NEW QUESTION: 26
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 deflection
B. Risk retention
C. Risk avoidance
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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, which of the following committees did UX Software establish?
A. Information security committee
B. Operational committee
C. Steering committee
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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: (SHOW ANSWER)

NEW QUESTION: 29
Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.

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

NEW QUESTION: 30
A. Management reviews must be carried out monthly

B. Management reviews are carried out at various levels in the organization
C. Top management can delegate the ultimate responsibility of the management review process to individuals working for the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following would be an acceptable justification for excluding the Annex A 6.1 Screening control?
A. A collective agreement with employees prohibits security checks
B. The organization considers background verification checks unnecessary for its operations
C. The organization voluntarily performs comprehensive criminal background checks on all employees
Answer: (SHOW ANSWER)

NEW QUESTION: 32
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. No, the justification section should encompass the rationale for the inclusion and exclusion of each security control
B. Yes, the technical specifications of security controls must be included within the justification section
C. No, the justification section should concisely overview previous software projects
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
Scenario 4: UX Software, a company specializing in L.JXfUI design. QA and software testing. and mobile application development. recognized the need to improve its information security measures, As such. the company implemented an ISMS based on ISO/IEC 27001- This strategic move aimed to enhance the confidentiality. availability, and integrity Of information shared internally and externally, aligning with industry standards and best practices.
The integration of ISMS into UX Software's existing processes and ensuring that these processes are adjusted in accordance with the framework of ISMS signified an important milestone. underscoring the organization'S commitment to information security. UX Software meticulously tailored these procedures to align with the ISMS framework, ensuring they ate contextually and culturally appropriate while avoiding mismatches. This

proactive stance reassured their employees and instilled confidence in their clients, ensuring the protection of sensitive data throughout their operations.
UX Software'S top management took action to define the Scope Of their ISMS to adhere to ISOflEC 27003 to drive this initiative forward. Sven, a key member Of the top management team at UX Software. assumed the role of project sponsor. a critical position responsible for ensuring the execution of ISMS implementation with adequate resources. Sven's leadership was pivotal in steering the project towards compliance with
27001, thus elevating the organization's information security posture to the highest level- In parallel with their dedication to information security. UX Software incorporated the technical specifications Of security controls within the justification section Of their Statement Of Applicability This approach demonstrated their Commitment to meeting ISO/IEC 27001 requirements and ensured thorough documentation and justification Of Security controls, thereby Strengthening the overall Security framework Of the organization. Additionally. UX Software established a committee responsible for ensuring the effectiveness of correctrve actions, managing the ISMS documented information, and continually improving the ISMS while addressing nonconformities.
By implementing an ISMS based on ISO/IEC 27001, UX Software improved its information security and reinforced its position as a reliable partner. This dedication to information security serves as a testament to UX Software's commitment to delivering high-quality software solutions while safeguarding the interests of its internal stakeholders and valued clients.
According to Scenario 4, UX Software decided to use the guidelines of ISO/IEC 27003 to define the scope of the ISMS. Is the scope defined in accordance with these guidelines?
A. Yes, they defined the scope according to ISO/IEC 27003
B. No, they should have determined the final scope first
C. No, they should have followed a multi-step approach involving management representatives and refinement
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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 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: 35
Jane is a developer looking to deploy an application she created using a programming language supported by her cloud service provider. She does not need to manage the underlying infrastructure like servers or storage, but needs control over the application and its environment. Which cloud service model does Jane need?
A. Platform as a Service
B. Infrastructure as a Service
C. Software as a Service
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Scenario 3: Socket Inc. is a dynamic telecommunications company specializing in wireless products and services, committed to delivering high-quality and secure communication solutions. Socket Inc. leverages innovative technology, including the MongoDB database, renowned for its high availability, scalability, and flexibility, to provide reliable, accessible, efficient, and well-organized services to its customers. Recently, the company faced a security breach where external hackers exploited the default settings of its MongoDB database due to an oversight in the configuration settings, which had not been properly addressed. Fortunately, diligent data backups and centralized logging through a server ensured no loss of information. In response to this incident, Socket Inc. undertook a thorough evaluation of its security measures. The company recognized the urgent need to improve its information security and decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
To improve its data security and protect its resources, Socket Inc. implemented entry controls and secure access points. These measures were designed to prevent unauthorized access to critical areas housing sensitive data and essential assets. In compliance with relevant laws, regulations, and ethical standards, Socket Inc. implemented pre-employment background checks tailored to business needs, information classification, and associated risks. A formalized disciplinary procedure was also established to address policy violations. Additionally, security measures were implemented for personnel working remotely to safeguard information accessed, processed, or stored outside the organization's premises.
Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.

The company also implemented a control to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.
Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.
Based on the scenario above, answer the following question:
Based on scenario 3, did Socket Inc. adhere to the requirements of ISO/IEC 27001 regarding ISMS documented information?
A. Yes, the standard requires that all security controls be included in a single document
B. No, Socket Inc. consolidated all controls of a group into a single document while the standard requires the controls to be documented in four groups
C. Yes, there is no mandatory requirement on how to document processes or security controls in the standard
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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)

NEW QUESTION: 38
Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.
Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee

must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management Based on scenario 8. does SunDee comply with ISO/IEC 27001 requirements regarding the monitoring and measurement process?

A. No, because even though the standard does not imply when such a process should be performed, the company must have a monitoring and measurement process in place

B. Yes, because the standard requires that the monitoring and measurement phase be conducted every two years

C. Yes. because the standard does not Indicate when the monitoring and measurement phase should be performed

Answer: (SHOW ANSWER)

NEW QUESTION: 39

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

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

Socket Inc. safeguarded its information processing facilities against power failures and other disruptions. Unauthorized access to critical records from external sources led to the implementation of data flow control services to prevent unauthorized access between departments and external networks. In addition, Socket Inc. used data masking based on

the organization's topic-level general policy on access control and other related topic-level general policies and business requirements, considering applicable legislation. It also updated and documented all operating procedures for information processing facilities and ensured that they were accessible to top management exclusively.
The company also implemented a control to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, regulations, and the information classification scheme. Network segregation using VPNs was proposed to improve security and reduce administrative efforts.
Regarding the design and description of its security controls, Socket Inc. has categorized them into groups, consolidating all controls within a single document. Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information about information security threats and integrate information security into project management.
Based on the scenario above, answer the following question:
Based on scenario 3, did Socket Inc. comply with ISO/IEC 27001 organizational controls regarding its operating procedures?
A. No, operating procedures for information processing facilities should have been exclusively available to the Information Technology Department or a similar unit within the company
B. Yes, it did comply with ISO/IEC 27001 requirements
C. No, operating procedures for information processing facilities should have been specifically provided to personnel who require them
Answer: (SHOW ANSWER)

NEW QUESTION: 40
A. The inconsistency of reports written by different employees
B. The negligence of performance evaluation and monitoring and measurement procedures
C. The voluminous written reports
Answer: (SHOW ANSWER)

NEW QUESTION: 41
According to ISO/IEC 270G1. why shall organizations document nonconformities?
A. To provide evidence of the results of the corrective actions and the nature of the nonconformities
B. To provide evidence of the requirements set by internal audit after reviewing their audit reports
C. To provide evidence of regulations set by external sources that need to be followed by the organization
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Scenario 8: BioVitalis
BioVitalis is a biopharmaceutical firm headquartered in California, the US Renowned for its pioneering work in the field of human therapeutics, BioVitalis places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation BioVitalis has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.
In preparation for the recertification audit. BioVitalis conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment. Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.
During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader BioVitalis's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow up action plans, which were then approved by top management.
In response to the review outcomes. BioVitalis promptly implemented corrective actions, strengthening its Information security measures Additionally, dashboard tools were Introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities.
Furthermore. BioVitalis embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities BioVitalis is a biopharma company with an ISMS certified under ISO/IEC 27001. For recertification, it reviewed ISMS performance, created dashboards to monitor KPIs such as incident cost, vulnerability tests, and resolution times.
What type of dashboards did BioVitalis utilize?
A. Tactical

B. Operational
C. Strategic
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which option below should be addressed in an information security policy?
A. The complexity of information security processes and their interactions
B. Legal and regulatory obligations imposed upon the organization
C. Actions to be performed after an information security incident
Answer: (SHOW ANSWER)

NEW QUESTION: 44
What service did Auto Tsaab implement to manage and protect information effectively?
A. Access control services
B. Backup services
C. Cryptographic services
D. Integrity services
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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: B (LEAVE A REPLY)

NEW QUESTION: 46
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. No, only the same auditor can complete the full audit cycle
B. No, as long as she remains impartial, she can audit CircuitLinking
C. Yes, considering her past as an employee for CircuitLinking
D. Yes, but no other auditor should have been assigned in her place
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Scenario 9:
OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.
Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.
Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan was written as follows:
"A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department." However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.
Did OpenTech have a plan in place to implement permanent corrective action to address the identified nonconformities?

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

NEW QUESTION: 48
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Which situation described in scenario 1 represents a threat to HealthGenic?
A. The software company modified information related to HealthGenic's patients
B. HealthGenic used a web-based medical software for storing patients' confidential information
C. HealthGenic did not train its personnel to use the software
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which audit phase was conducted after the issue with the audit team was resolved?
A. Audit follow-up
B. Stage 2
C. Stage 1
Answer: (SHOW ANSWER)

NEW QUESTION: 50
A. Set annual objectives and the ISMS strategy
B. Treat the nonconformities
C. Ensure smooth running of the ISMS
Answer: (SHOW ANSWER)

NEW QUESTION: 51
During a security audit, analysts discover that an attacker repeatedly queried a black-box ML model to infer if specific data points were in the training set. The attacker could determine if an individual's data was used during training. What threat does this attack represent?
A. Data poisoning
B. Membership inference attack
C. Backdoor in the training set
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Scenario 1: NobleFind is an online retailer specializing in high-end, custom-design furniture. The company offers a wide range of handcrafted pieces tailored to meet the needs of residential and commercial clients. NobleFind also provides expert design consultation services. Despite NobleFind's efforts to keep its online shop platform secure, the company faced persistent issues, including a recent data breach. These ongoing challenges disrupted normal operations and underscored the need for enhanced security measures. The designated IT team quickly responded to resolve the problem. To address these issues, NobleFind decided to implement an Information Security Management System (ISMS) based on ISO/IEC 27001 to improve security, protect customer data, and ensure the stability of its services.
In addition to its commitment to information security, NobleFind focuses on maintaining the accuracy and completeness of its product dat a. This is ensured by carefully managing version control, checking information regularly, enforcing strict access policies, and implementing backup procedures. Moreover, product details and customer designs are accessible only to authorized individuals, with security measures such as multi-factor authentication and data access policies.
NobleFind has implemented an incident investigation process within its ISMS, as part of its comprehensive approach to information security. Additionally, it has established record retention policies to ensure that online information about each product and client information remains readily accessible and usable on demand for authorized entities.
NobleFind established an information security policy offering clear guidelines for safeguarding historical data. It also insisted that personnel sign confidentiality agreements and were committed to recruiting only qualified individuals. Additionally, NobleFind implemented measures for monitoring the resources used by its systems, reviewing user access rights, and conducting a thorough analysis of audit logs to swiftly identify and address any security anomalies.
With its ISMS in place, NobleFind maintains and safeguards documented information, encompassing a wide range of data, records, and specifications. This documented information is vital to its operations, ensuring the security and integrity of customer data, historical records, and financial information.

According to scenario 1, which detective control did NobleFind implement?
A. Enforcing strict access policies
B. Implementing backup procedures
C. Conducting a thorough analysis of audit logs
D. Implementing an incident investigation process
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which of the following statements regarding information security risk is NOT correct?
A. Information security risk can be expressed as the effect of uncertainty on information security objectives
B. Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats
C. Information security risk cannot be accepted without being treated or during the process of risk treatment
Answer: (SHOW ANSWER)

NEW QUESTION: 54
An organization wants to enable the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. Which control should it implement?
A. Use of privileged utility programs
B. Installation of software on operational systems
C. Clock synchronization
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Scenario 10: ProEBank
ProEBank is an Austrian financial institution known for its comprehensive range of banking services. Headquartered in Vienna, it leaverages the city's advanced technological and financial ecosystem To enhance its security posture, ProEBank has implementied an information security management system (ISMS) based on the ISO/IEC 27001. After a year of having the ISMS in place, the company decided to apply for a certification audit to obtain certification against ISO/IEC 27001.
To prepare for the audit, the company first informed its employees for the audit and organized training sessions to prepare them. It also prepared documented information in advance, so that the documents would be ready when external auditors asked to review them Additionally, it determined which of its employees have the knowledge to help the external auditors understand and evaluate the processes.
During the planning phase for the audit, ProEBank reviewed the list of assigned auditors provided by the certification body. Upon reviewing the list, ProEBank identified a potential

conflict of interest with one of the auditors, who had previously worked for ProEBank's mein competitor in the banking industry To ensure the integrity of the audit process. ProEBank refused to undergo the audit until a completely new audit team was assigned. In response, the certification body acknowledged the conflict of interest and made the necessary adjustments to ensure the impartiality of the audit team After the resolution of this issue, the audit team assessed whether the ISMS met both the standard's requirements and the company's objectives. During this process, the audit team focused on reviewing documented information.
Three weeks later, the team conducted an on-site visit to the auditee's location where they aimed to evaluate whether the ISMS conformed to the requirements of ISO/IEC 27001. was effectively implemented, and enabled the auditee to reach its information security objectives. After the on-site visit the team prepared the audit conclusions and notified the auditee that some minor nonconformities had been detected The audit team leader then issued a recommendation for certification.
After receiving the recommendation from the audit team leader, the certification body established a committee to make the decision for certification. The committee included one member from the audit team and two other experts working for the certification body.
After the Stage 2 audit, minor nonconformities were found. Despite this, the audit team leader issued a positive recommendation for certification.
Is this acceptable?
A. No - the auditor should have issued a recommendation for certification conditional upon the filing of corrective action plans for the minor nonconformities
B. No - the auditor should have issued an unfavorable recommendation for certification because minor nonconformities were identified
C. Yes - a recommendation for certification should be issued when only minor nonconformities are identified
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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 IoT 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 AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with 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.
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)

NEW QUESTION: 57
Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.
In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With

this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.
During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.
SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.
In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.
Based on the scenario above, answer the following question:
Based on scenario 8, which of the following performance indicators was NOT established by SunDee?
A. Information security cases
B. ISMS weaknesses
C. Training
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Scenario 7: Yefund, an insurance Company headquartered in Monaco, is a reliable name in Commerce, industry, and Corporate services. With a rich history spanning decades, Yefund has consistently delivered tailored insurance solutions to businesses of all sizes. safeguarding their assets and mitigating risks. As a forward-thinking company, Yetund recognizes the importance of information security in protecting sensitive data and maintaining the trust Of Its clients. Thus, has embarked on a transformative journey

towards implemenung an ISMS based on ISO/IEC 27001- iS implementing cutting-edge Al technologies within its ISMS to improve the identification and management Of information assets, Through Al. is automating the identification Of assets. tracking changes over time. and strategically selecting controls based on asset sensitivity and exposure. This proactive approach ensures that Yefund remains agile and adaptive in safeguarding critical information assets against emerging threats. Although Yetund recognized the urgent need to enhance its security posture, the implementation team took a gradual approach to integrate each ISMS element- Rather than waiting for an official launch, they carefully tested and validated security controls, gradually putting each element into operational mode as it was completed and approved. This methodical process ensured that critical security measures, such as encryption protocols. access controls. and monitoring systems. were fully operational and effective in safeguarding customer information, including personal. policy, and financial details.

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

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

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

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

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

A. Yes, both information security events were effectively addressed

B. No, monitoring teams must be established to address the events according to their categorization

C. No, because information security events should not be categorized merely as event reports under any circumstances

Answer: (SHOW ANSWER)

NEW QUESTION: 59

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 phase of information security policy development at OperazeIT did NOT encompass all the necessary components?
A. Risk assessment
B. Policy implementation
C. Policy construction
Answer: (SHOW ANSWER)

NEW QUESTION: 60
A. No - the committee should have included only members from the audit team and not other experts that were not part of the audit
B. Yes - the committee must include one member from the audit team and other individuals working for the certification body
C. No - the certification body must ensure that persons that make the decision for certification are different from those who carried out the audit
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Scenario 4: TradeB is a newly established commercial bank located in Europe, with a diverse clientele. It provides services that encompass retail banking, corporate banking, wealth management, and digital banking, all tailored to meet the evolving financial needs of individuals and businesses in the region. Recognizing the critical importance of information security in the modern banking landscape, TradeB has initiated the implementation of an information security management system (ISMS) based on ISO/IEC 27001. To ensure the successful implementation of the ISMS, the top management decided to contract two experts to lead and oversee the ISMS implementation project.
As a primary strategy for implementing the ISMS, the experts chose an approach that emphasizes a swift implementation of the ISMS by initially meeting the minimum requirements of ISO/IEC 27001, followed by continual improvement over time. Additionally, under the guidance of the experts, TradeB opted for a methodological framework, which

serves as a structured framework and a guideline that outlines the high-level stages of the ISMS implementation, the associated activities, and the deliverables without incorporating any specific tools.

The experts analyzed the ISO/IEC 27001 controls and listed only the security controls deemed applicable to the company and its objectives. Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on a methodical approach that involved defining and characterizing the terms and criteria used in the assessment process, categorizing them into non-numerical levels (e.g., very low, low, moderate, high, very high). Explanatory notes were thoughtfully crafted to justify assessed values, with the primary goal of enhancing repeatability and reproducibility.

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

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

Based on the scenario above, answer the following question:

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 62
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. Corrective and managerial
B. Detective and administrative
C. Legal and technical
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Scenario 9:
OpenTech, headquartered in San Francisco, specializes in information and communication technology (ICT) solutions. Its clientele primarily includes data communication enterprises and network operators. The company's core objective is to enable its clients to transition smoothly into multi-service providers, aligning their operations with the complex demands of the digital landscape.

Recently, Tim, the internal auditor of OpenTech, conducted an internal audit that uncovered nonconformities related to their monitoring procedures and system vulnerabilities. In response to these nonconformities, OpenTech decided to employ a comprehensive problem-solving approach to address the issues systematically. This method encompasses a team-oriented approach, aiming to identify, correct, and eliminate the root causes of the issues. The approach involves several steps: First, establish a group of experts with deep knowledge of processes and controls. Next, break down the nonconformity into measurable components and implement interim containment measures. Then, identify potential root causes and select and verify permanent corrective actions. Finally, put those actions into practice, validate them, take steps to prevent recurrence, and recognize and acknowledge the team's efforts.
Following the analysis of the root causes of the nonconformities, OpenTech's ISMS project manager, Julia, developed a list of potential actions to address the identified nonconformities. Julia carefully evaluated the list to ensure that each action would effectively eliminate the root cause of the respective nonconformity. While assessing potential corrective actions, Julia identified one issue as significant and assessed a high likelihood of its recurrence. Consequently, she chose to implement temporary corrective actions. Julia then combined all the nonconformities into a single action plan and sought approval from top management. The submitted action plan was written as follows:
"A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department." However, Julia's submitted action plan was not approved by top management. The reason cited was that a general action plan meant to address all nonconformities was deemed unacceptable. Consequently, Julia revised the action plan and submitted separate ones for approval. Unfortunately, Julia did not adhere to the organization's specified deadline for submission, resulting in a delay in the corrective action process. Additionally, the revised action plans lacked a defined schedule for execution.
Based on scenario 9, was it acceptable that the top management rejected the action plan submitted by Julia?
A. Yes, an action plan must be submitted to address each nonconformity separately
B. No, top management should have approved the action plan submitted by Julia
C. No, a general action plan can be submitted to address all nonconformities at once
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user

permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company's departments within the ISMS scope. The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.
Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.
Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.
What is the next step that Operaze's ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.
A. Implement the information security policy
B. Obtain top management's approval for the information security policy
C. Communicate the information security policy to all employees
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A small organization that is implementing an ISMS based on ISO/IEC 27001 has decided to outsource the internal audit function to a third party. Is this acceptable?
A. Yes, outsourcing the internal audit function to a third party is often a better option for small organizations to demonstrate independence and impartiality
B. No, the organizations cannot outsource the internal audit function to a third party because during internal audit, the organization audits its own system
C. No, the outsourcing of the internal audit function may compromise the independence and impartiality of the internal audit team
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Scenario 8: SecureLynx is one Of the largest cybersecurity advisory and consulting companies that helps private sector organizations prevent security threats. improve security systems. and achieve business SecureLynr is committed to complying with national and international standards to enhance the company'S resilience and credibility_ SecureLynx has Started implementing an ISMS based on ISO/IEC 27001 as part of its relentless pursuit of security.
As part of the internal audit activities. the top management reviewed and approved the audit objectives to assess the effectiveness of SecureLynx*s ISMS During the audit, the internal auditor evaluated whether top management Supports activities associated with the ISMS and if the toles and responsibilities Of relevant parties are Clearly defined. This rigorous examination is a testament to SecureLynx'S commitment to continuous improvernent and alignment of security measures with organizational goals.
SecureLynx employs an innovative dashboard that visually represents implemented processes and controls to ensure transparency and accountability within the Organization. This tool Offers stakeholders a real- time overview of security measures. empowering them to make informed decisions and swiftly respond to emerging threats. As part of this initiative, Paula was appointed to a new position entrusted with the responsibility Of collecting, recordlng, and Stoting data to measure the effectiveness Of the ISMS-Furthermore, SecureLynx conducts management reviews every six months to ensure its Systems are robust and continually improving. These reviews serve as a crucial mechanism for assessing the efficacy Of security measures and identifying areas for enhancement. SecureLynx's dedication to implementing and maintaining a robust ISMS exemplifies its commitment to innovation and Client satisfaction.
Based on the scenario above, answer the following question.
Based on the description of Paula's responsibilities at SecureLynx, her role is known as:
A. Information collector
B. Information analyst
C. Information communicator
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which security controls must be implemented to comply with ISO/IEC 27001?
A. Those listed in Annex A of ISO/IEC 27001, without any exception
B. Those designed by the organization only
C. Those included in the risk treatment plan
Answer: (SHOW ANSWER)

NEW QUESTION: 68

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on SO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.
Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management According to scenario 8, Tessa created a plan for ISMS monitoring and measurement and presented it to the top management Is this acceptable?
A. No, Tessa must implement all the improvements needed for issues found during the audit
B. Yes, Tessa can advise the top management on improving the company's functions
C. No, Tessa should only communicate the issues found to the top management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.
Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:
A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the

Information and Communication Technology (ICT) Department The approved action plan was implemented and all actions described in the plan were documented.
Based on scenario 9. did the ISMS project manager complete the corrective action process appropriately?
A. Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions
B. No, the corrective action did not address the root cause of the nonconformity
C. No, the corrective action process should also include the review of the implementation of the selected actions
Answer: (SHOW ANSWER)

NEW QUESTION: 70
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: 71
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. Invasion of patients' privacy
B. Service interruptions due to the increased number of users
C. Modification of patients' medical reports
Answer: (SHOW ANSWER)

NEW QUESTION: 72
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)

NEW QUESTION: 73
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
Based on the scenario above, answer the following question:
According to scenario 2, Solena decided to issue a press release in which its representatives denied the attack. What does this situation present?
A. Lack of transparency toward their users
B. Lack of availability toward their users
C. Lack of communication strategies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
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, only top management's input should be considered
C. Yes, the certification body must make the certification decision based on other relevant information, such as public information
D. No, the certification decision must be based solely on the audit findings, and no external information can be considered
Answer: (SHOW ANSWER)

NEW QUESTION: 75
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 dat a. 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. SkyFleet should conduct at least an annual review of the ISMS

C. No. Reviews are only necessary when significant changes in business operations occur
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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. Compromise of functions
C. Technical failures
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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 frequency of analysis and evaluation
B. The methods for monitoring, measurement, analysis, and evaluation
C. The number of attributes to be measured
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Scenario 7: Yefund, an insurance Company headquartered in Monaco, is a reliable name in Commerce, industry, and Corporate services. With a rich history spanning decades, Yefund has consistently delivered tailored insurance solutions to businesses of all sizes. safeguarding their assets and mitigating risks. As a forward-thinking company, Yetund recognizes the importance of information security in protecting sensitive data and maintaining the trust Of Its clients. Thus, has embarked on a transformative journey towards implemenung an ISMS based on ISO/IEC 27001- iS implementing cutting-edge Al technologies within its ISMS to improve the identification and management Of information assets, Through Al. is automating the identification Of assets. tracking changes over time. and strategically selecting controls based on asset sensitivity and exposure. This proactive approach ensures that Yefund remains agile and adaptive in safeguarding critical information assets against emerging threats. Although Yetund recognized the urgent need to enhance its security posture, the implementation team took a gradual approach to integrate each ISMS element- Rather than waiting for an official launch, they carefully tested and validated security controls, gradually putting each element into operational mode as it was completed and approved. This methodical process ensured that critical security measures, such as encryption protocols. access controls. and monitoring systems. were fully operational and effective in safeguarding customer information, including personal. policy, and financial details.
Recently. Kian. a member of Vefund's information security team. identified two security events. Upon evaluation. one reported incident did not meet the criteria to be classified as

such- However, the second incident. involving critical network components experiencing downtime. raised concerns about potential risks to sensitive data security and was therefore categorized as an incident. The first event was recorded as a report without further action, whereas the second incident prompted a series Of actions, including investigation. containment, eradication, recovery. resolution, closure, incident reporting, and post-incident activities. Additionally. IRTS were established to address the events according to their Categorization.
After the incident. Yetund recognized the development of internal communication protocols as the single need to improve their ISMS framework It determined the relevance of communication aspects such as what, when, with whom. and how to Communicate effectively Yefund decided to focus On developing internal communication protocols, reasoning that internal coordination their most immediate priority. This decision was made despite having external stakeholders. such as clients and regulatory bodies. who also required secure and timely communication.
Additionally, Yefund has prioritized the professional development Of its employees through comprehensive training programs, Yefund assessed the effectiveness and impact Of its training initiatives through Kirkpatrick's four-level training evaluation model. From measuring trainees' involvement and impressions of the training (Level 1) to evaluating learning outcomes (Level 2), post-training behavior (Level 3), and tangible results (Level 4), Yefund ensures that Its training programs ate holistic. impactful. and aligned With organizational objectives.
Yefund*s journey toward implementing an ISMS reflects a commitment to security, innovation, and continuous improvement, By leveraging technology, fostering a culture Of proactive vigilance, enhancing communication ptotOCOIS, and investing in employee development. Yefund seeks to fortify its position as a trusted partner in safeguarding the interests Of its Clients and stakeholders.
Did Yefund handle the identified information security events appropriately? Refer to scenario 7.
A. Yes, both information security events were effectively addressed
B. No, monitoring teams must be established to address the events according to their categorization
C. No, because information security events should not be categorized merely as event reports under any circumstances
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Upon the risk assessment outcomes. Socket Inc. decided to:
* Require the use of passwords with at least 12 characters containing uppercase and lowercase letters, symbols, and numbers
* Require the change of passwords at least once every 60 days
* Keep backup copies of files on IT-provided network drives

* Assign users to a separate network when they have access to cloud storage files storing customers' personal data.
Based on the scenario above, answer the following question:
Which of the following options indicate that Socket Inc. used risk modification to treat risks?
A. Conducting a risk assessment before deciding to use third-party services
B. Storing customers' personal data in a cloud-based storage
C. Requiring the change of passwords at least once every 60 days
Answer: (SHOW ANSWER)

NEW QUESTION: 80
A. ISMS project manager
B. IT Department
C. Top management
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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 incorrectly implemented a security control that could become a vulnerability
B. Org Y has implemented a security control that ensures the confidentiality of information
C. Org Y has implemented an integrity control that avoids the involuntary corruption of data
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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: 83
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: (SHOW ANSWER)

NEW QUESTION: 84
According to ISO/IEC 27001 controls, why should the use of privileged utility programs be restricted and tightly controlled?
A. To enable the correlation and analysis of security-related events
B. To ensure that utility programs are compatible with existing system software
C. To prevent misuse of utility programs that could override system and application controls
Answer: (SHOW ANSWER)

NEW QUESTION: 85
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, because the standard provides a separate control for cryptographic key management
B. Yes, the control for the effective use of the cryptography can include cryptographic key management
C. No, the control should be implemented only for defining rules for cryptographic key management
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.
One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on the scenario above, answer the following question:
How should Colin have handled the situation with Lisa?
A. Deliver training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company
B. Extend the duration of the training and awareness session in order to be able to achieve better results
C. Promise Lisa that future training and awareness sessions will be easily understandable
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which control in Annex A of ISO/IEC 27001 requires that the information security requirements shall be identified, specified, and approved when developing or acquiring applications?
A. A.8.25 Secure development life cycle
B. A.8.27 Secure system architecture and engineering principles
C. A.8.26 Application security requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.
Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the

root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:
A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department The approved action plan was implemented and all actions described in the plan were documented.
Based on scenario 9, OpenTech has taken all the actions needed, except_____.
A. Corrective actions
B. Preventive actions
C. Permanent corrections
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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. No, because the company has already defined the ISMS scope
B. No, because any change in ISMS scope should be accepted by the management
C. Yes, because the ISMS scope should be changed when there are changes to the external environment
Answer: (SHOW ANSWER)

NEW QUESTION: 90
A. No - CoreBit Systems decided not to pursue this course of action
B. Yes - CoreBit Systems had a comprehensive plan in place to implement permanent corrective actions
C. No - CoreBit Systems did not have a clear plan to implement a permanent corrective action
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following standards provides the requirements and guidelines for establishing a privacy information management system (PIMS)?
A. ISO/IEC 27011
B. ISO/IEC 27009
C. ISO/IEC 27701
Answer: (SHOW ANSWER)

NEW QUESTION: 92

Is NyvMarketing required to follow the guidelines of ISO/IEC 27002 to attain ISO/IEC 27001 certification?
A. No, adherence to ISO/IEC 27002 guidelines is not mandatory for ISO/IEC 27001 certification
B. Yes, since ISO/IEC 27002 is an auditable standard
C. Yes, since it is a requirement according to ISO/IEC 27001
D. Yes, since the controls provided in Annex A of ISO/IEC 27001 are aligned with ISO/IEC 27002 controls
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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: 94
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:
Was there any issue with how OperazeIT determined its current ISMS state?
A. Yes, as it is the top management's responsibility to determine the ISMS state
B. No, as the ISMS state can be determined by outsourced external consultants
C. Yes, as the ISMS state must be determined by the implementation team
Answer: (SHOW ANSWER)

NEW QUESTION: 95
The Incident Response Team (IRT) has been notified of a potential compromise in the organization's network. Which type of services would be most appropriate for the IRT to provide in this situation?
A. Reactive services
B. Security quality management services
C. Proactive services
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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:
Based on scenario 4, from which source did TradeB's ISMS implementation draw its methodological framework?
A. ISO/IEC 27003
B. ISO 10006
C. COBIT 5
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
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 Did the experts draft the Statement of Applicability (SoA) in accordance with ISO/IEC 27001?
A. No - because they did not review all of the controls from Annex A of ISO/IEC 27001
B. No - because the SoA should have been drafted just before the risk assessment was finalized
C. Yes - because they reviewed a selected number of the controls from Annex A of ISO/IEC 27001
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Scenario 7: Incident Response at Texas H&H Inc.
Once they made sure that the attackers do not have access in their system, the security administrators decided to proceed with the forensic analysis. They concluded that their

access security system was not designed tor threat detection, including the detection of malicious files which could be the cause of possible future attacks.
Based on these findings. Texas H$H inc, decided to modify its access security system to avoid future incidents and integrate an incident management policy in their Information security policy that could serve as guidance for employees on how to respond to similar incidents.
Based on the scenario above, answer the following question:
Texas H&H Inc. decided to assign an internal expert for their forensic analysis. Is this acceptable? Refer lo scenario 7.
A. No. the company's forensic analysis should be based on the conclusion of Its cloud storage provide investigation
B. Yes. forensic analysis can be done by cither an internal or external expert
C. Yes. hiring an external expert for forensic analysis Is a requirement of the standard
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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.

Has CyTekShield appropriately addressed the handling of evidence related to information security events?

A. Yes - it has appropriately addressed the handling of evidence

B. No - because the process of evidence acquisition was not fully detailed

C. No - as it does not include proper training for staff involved in evidence handling

Answer: (SHOW ANSWER)

NEW QUESTION: 100

A. Employees involved in information security activities and tasks only

B. Experts who are directly responsible for information security only

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 101

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. No, because the action plan does not address the root cause of the identified nonconformity
B. Yes, because a separate action plan has been created for the identified nonconformity
C. No, because the action plan does not include a timeframe for implementation
Answer: (SHOW ANSWER)

NEW QUESTION: 102
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. Skyver did not determine differing team needs in accordance to the activities they perform and the intended results
B. The effectiveness of the training and awareness session was not evaluated
C. Lisa did not take actions to acquire the necessary competence
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Levo Corporation has implemented a demilitarized zone (DMZ) and virtual private network (VPN) to secure its network. What controls did Levo Corporation implement in this case?
A. Corrective controls
B. Preventive controls
C. Detective controls

Answer: (SHOW ANSWER)

NEW QUESTION: 104

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.

When UX Software integrated ISMS into their existing processes, did they adapt those processes to align with the ISMS framework?

A. Yes, they adjusted their existing processes to fit with the ISMS framework

B. No, they should have revised all existing processes to match the ISMS framework

C. No, they should have placed all existing processes on hold until the ISMS framework is fully implemented

Answer: (SHOW ANSWER)

NEW QUESTION: 105

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

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

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

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

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

Based on the scenario above, answer the following question:
Which of the following physical controls was NOT included in Socket Inc.'s strategy?
A. Annex A 7.9 Security of assets off-premises
B. Annex A 7.2 Physical entry
C. Annex A 7.11 Supporting utilities
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Has Bytes determined all the relevant factors that impact its ability to achieve the intended outcomes of its ISMS, in accordance with clause 4.1 "Understanding the organization and its context" of ISO/IEC 27001?
A. No, the company did not determine which requirements of interested parties will be addressed through the ISMS
B. No, the company did not determine whether climate change is a relevant issue
C. Yes, the company determined all the relevant issues to its purpose that affect its ability to achieve the intended outcomes
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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. No, the certification body decides whether the documentation review takes place on-site or off-site

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 108

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.
After committing to ISO/IEC 27001 adherence, was the documented information in Auto Tsaab's information security management system managed in compliance with the standard?
A. Yes, the company delegated the responsibility of managing documented information to a single individual
B. Yes, the company ensured that documented information was available and protected as needed
C. Yes, the company relied only on manual methods for managing documented information
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Scenario 6: Skyver manufactures electronic products, such as gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware, and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well-informed by security principles and practices.
One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues. In a supportive manner, Colin suggested Lisa consider attending the session again.
Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide

suggestions to customers. This strategic initiative aligned with Skyver's commitment to improving the customer experience through data-driven insights.
Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable various deployment options and enhance information security, crucial for Skyver's electronic product development.
According to Skyver, implementing additional controls in the ISMS implementation plan has been successfully executed, and the company was ready to transition into operational mode. Skyver assigned Colin the responsibility of determining the materiality of this change within the company.
Based on the scenario above, answer the following question:
As part of its strategic initiative to improve customer experiences, Skyver is exploring the implementation of advanced AI solutions. Which type of AI is the company likely considering for this purpose?
A. Strong AI
B. Machine learning
C. Weak AI
Answer: (SHOW ANSWER)

NEW QUESTION: 110
A. Management committee
B. Information security committee
C. Operational committee
Answer: (SHOW ANSWER)

NEW QUESTION: 111
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, Nigeri a. 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, what should Bytes consider when assessing the security of its ICT systems?
A. The cost of the tools they used when assessing the security of their ICT systems
B. The tools they used may produce false positives due to a lack of environmental context
C. The skills and expertise of the IT team responsible for assessing the ICT systems
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Scenario 1:
HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canad a. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless communication among various stakeholders, including patients, physicians, and medical laboratory staff.
As the organization expanded its services and demand grew, frequent and prolonged service interruptions became more common, causing significant disruptions to patient care and administrative processes. As such, HealthGenic initiated a comprehensive risk analysis to assess the severity of risks it faced.
When comparing the risk analysis results with its risk criteria to determine whether the risk and its significance were acceptable or tolerable, HealthGenic noticed a critical gap in its

capacity planning and infrastructure resilience. Recognizing the urgency of this issue, HealthGenic reached out to the software development company responsible for its platform. Utilizing its expertise in healthcare technology, data management, and compliance regulations, the software development company successfully resolved the service interruptions.

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

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

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

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

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

A. Availability

B. Integrity

C. Confidentiality

Answer: (SHOW ANSWER)

NEW QUESTION: 113

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. No, NyvMarketing's actions did not comply with ISO/IEC 27001 since it should have included all the Annex A controls
B. Yes, NyvMarketing's actions taken during the implementation of Annex A controls comply with ISO/IEC 27001
C. No, NyvMarketing's actions did not comply with ISO/IEC 27001 since it excluded one of the Annex A controls without providing justifications
D. Yes, because ISO/IEC 27002 allows for exclusions
Answer: (SHOW ANSWER)

NEW QUESTION: 114
In the SABSA framework, which layer is concerned with viewing the services at a high level?
A. Component security architecture
B. Logical security architecture
C. Physical security architecture
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.
Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.
However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.
The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.
In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.
Which statement below suggests that Beauty has implemented a managerial control that helps avoid the occurrence of incidents? Refer to scenario 2.
A. Beauty's employees signed a confidentiality agreement
B. Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information
C. Beauty updated the segregation of duties chart
Answer: (SHOW ANSWER)

NEW QUESTION: 116

Scenario 1:

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

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

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

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

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

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

confidentiality measures, including robust authentication methods, such as multi-factor authentication.
In response to the challenges faced by HealthGenic, the organization recognized the vital importance of ensuring a secure cloud computing environment. It initiated a comprehensive self-assessment specifically tailored to evaluate and enhance the security of its cloud infrastructure and practices.
Based on scenario 1, has HealthGenic implemented physical access controls?
A. No, its primary focus has been on legal access controls
B. Yes, it included physical access controls in its strategy
C. No, its primary focus has been on digital access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Following a repotted event, an Information security event ticket has been completed and its priority has been assigned. Then, the event has been evaluated to determine If it is an information security incident, which phase of the incident management has been completed?
A. Detection and reporting
B. Evaluation and confirmation
C. initial assessment and decision
Answer: (SHOW ANSWER)

NEW QUESTION: 118
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?
Which of the following categories of vulnerabilities did NyvMarketing address during its ISMS implementation? Refer to scenario 2.
A. Hardware, software, and network vulnerabilities
B. Network, personnel, and site vulnerabilities
C. Organizational and site vulnerabilities
D. Physical and administrative vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff.
Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.
The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.
Based on the scenario above, answer the following question:
According to scenario 1. to detect (1)_____, Antiques should have implemented (2)

A. (1) Patches. (2) an access control software
B. (1) Intrusions on networks. (?) an intrusion detection system
C. (1) Technical vulnerabilities. (2) network intrusions
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A. Gages
B. Scorecards
C. Reports
Answer: (SHOW ANSWER)

NEW QUESTION: 121
The purpose of control 5.9 inventory of Information and other associated assets of ISO/IEC 27001 is to identify organization's information and other associated assets in order to preserve their information security and assign ownership. Which of the following actions docs NOT fulfill this purpose?
A. Assigning the responsibility for appropriately classifying and protecting information and other associated assets to the asset owners
B. Conducting regular reviews of identified information and other associated assets
C. Establishing rules to control physical and logical access to Information and other associated assets
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Scenario 1:
HealthGenic is a leading multi-specialty healthcare organization providing patients with comprehensive medical services in Toronto, Canad a. The organization relies heavily on a web-based medical software platform to monitor patient health, schedule appointments, generate customized medical reports, securely store patient data, and facilitate seamless

communication among various stakeholders, including patients, physicians, and medical laboratory staff.

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

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

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

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

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

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

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

A. Theft
B. Lawsuit
C. Fraud
Answer: (SHOW ANSWER)

NEW QUESTION: 123
What is the main purpose of Annex A 7.1 Physical security perimeters of ISO/IEC 27001?
A. To maintain the confidentiality of information that is accessible by personnel or external parties
B. To ensure access to information and other associated assets is defined and authorized
C. To prevent unauthorized physical access, damage, and interference to the organization's information and other associated assets
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management [^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.
First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted Based on the scenario above, answer the following question:
The decision to treat only risks that were classified as high indicates that Trade B has:
A. Accepted other risk categories based on risk acceptance criteria
B. Modified other risk categories based on risk evaluation criteria
C. Evaluated other risk categories based on risk treatment criteria
Answer: (SHOW ANSWER)

NEW QUESTION: 125
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, Nigeri a. 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)

NEW QUESTION: 126
Scenario 8: SunDee is a biopharmaceutical firm headquartered in California, US. Renowned for its pioneering work in the field of human therapeutics, SunDee places a strong emphasis on addressing critical healthcare concerns, particularly in the domains of cardiovascular diseases, oncology, bone health, and inflammation. SunDee has demonstrated its commitment to data security and integrity by maintaining an effective information security management system (ISMS) based on ISO/IEC 27001 for the past two years.
In preparation for the recertification audit, SunDee conducted an internal audit. The company's top management appointed Alex, who has actively managed the Compliance Department's day-to-day operations for the last six months, as the internal auditor. With this dual role assignment, Alex is tasked with conducting an audit that ensures compliance and provides valuable recommendations to improve operational efficiency.
During the internal audit, a few nonconformities were identified. To address them comprehensively, the company created action plans for each nonconformity, working closely with the audit team leader.
SunDee's senior management conducted a comprehensive review of the ISMS to evaluate its appropriateness, sufficiency, and efficiency. This was integrated into their regular management meetings. Essential documents, including audit reports, action plans, and review outcomes, were distributed to all members before the meeting. The agenda covered the status of previous review actions, changes affecting the ISMS, feedback, stakeholder inputs, and opportunities for improvement. Decisions and actions targeting ISMS improvements were made, with a significant role played by the ISMS coordinator and the internal audit team in preparing follow-up action plans, which were then approved by top management.
In response to the review outcomes, SunDee promptly implemented corrective actions, strengthening its information security measures. Additionally, dashboard tools were introduced to provide a high-level overview of key performance indicators essential for monitoring the organization's information security management. These indicators included metrics on security incidents, their costs, system vulnerability tests, nonconformity detection, and resolution times, facilitating effective recording, reporting, and tracking of monitoring activities. Furthermore, SunDee embarked on a comprehensive measurement process to assess the progress and outcomes of ongoing projects, implementing extensive measures across all processes. The top management determined that the individual responsible for the information, aside from owning the data that contributes to the measures, would also be designated accountable for executing these measurement activities.
Based on the scenario above, answer the following question:
Based on scenario 8, which of the following dashboards did SunDee utilize?
A. Tactical dashboards

B. Strategic dashboards
C. Operational dashboards
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management [^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.
First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted Based on scenario 4, the fact that TradeB defined the level of risk based on three nonnumerical categories indicates that;
A. The level of risk will be defined using a formula
B. The level of risk will be evaluated against qualitative criteria
C. The level of risk will be evaluated using quantitative analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.
Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.
Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no

persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.
To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.
Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.
Based on scenario 3, what would help Socket Inc. address similar information security incidents in the future?
A. Using the MongoDB database with the default settings
B. Using cryptographic keys to protect the database from unauthorized access
C. Using the access control system to ensure that only authorized personnel is granted access
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Why is an in-depth review crucial for organizations to evaluate their security architecture?
A. To determine the organization's compliance with financial regulations
B. To meet shareholder expectations
C. To conduct background checks on potential employees to ensure security compliance
D. To assess whether security requirements based on industry best practices can be met
Answer: (SHOW ANSWER)

NEW QUESTION: 130
A. No - as ISO/IEC 27001 provides a predefined structure for all ISMS communication
B. No - as ISO/IEC 27001 requires all ISMS-related communication to be formally documented
C. Yes - as the organization can determine the extent and format of documented communication based on what is necessary for the effectiveness of its ISMS
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Which of the following processes may involve increasing risk in order to pursue an opportunity?
A. Risk identification
B. Risk analysis

C. Risk treatment
Answer: (SHOW ANSWER)

NEW QUESTION: 132
An employee from Reyae Ltd. unintentionally sent an email containing critical business strategies to a competitor. Which information security principle was compromised in this case?
A. Integrity
B. Availability
C. Confidentiality
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Scenario 6: Skyver manufactures electronic products, such as gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Colin, the company's information security manager, decided to conduct a training and awareness session for the company's staff about the information security risks and the controls implemented to mitigate them. The session covered various topics, including Skyver's information security approaches, techniques for mitigating phishing and malware, and a dedicated segment on securing cloud infrastructure and services. This particular segment explored the shared responsibility model and concepts such as identity and access management in the cloud. Colin organized the training and awareness sessions through engaging presentations, interactive discussions, and practical demonstrations to ensure that the personnel were well-informed by security principles and practices.
One of the participants in the session was Lisa, who works in the HR Department. Although Colin explained Skyver's information security policies and procedures in an honest and fair manner, she found some of the issues being discussed too technical and did not fully understand the session. Therefore, in many cases, she would request additional help from the trainer and her colleagues. In a supportive manner, Colin suggested Lisa consider attending the session again.
Skyver has been exploring the implementation of AI solutions to help understand customer preferences and provide personalized recommendations for electronic products. The aim was to utilize AI technologies to enhance problem-solving capabilities and provide suggestions to customers. This strategic initiative aligned with Skyver's commitment to improving the customer experience through data-driven insights.
Additionally, Skyver looked for a flexible cloud infrastructure that allows the company to host certain services on internal and secure infrastructure and other services on external and scalable platforms that can be accessed from anywhere. This setup would enable

various deployment options and enhance information security, crucial for Skyver's electronic product development.

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

Based on the scenario above, answer the following question:

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

A. Private cloud

B. Hybrid cloud

C. Public cloud

Answer: (SHOW ANSWER)