PECB.ISO-IEC-27001-Lead-Auditor.v2026-06-27.q169

Exam Code:	ISO-IEC-27001-Lead-Auditor
Exam Name:	PECB Certified ISO/IEC 27001 Lead Auditor exam
Certification Provider:	PECB
Free Question Number:	169
Version:	v2026-06-27
# of views:	102
# of Questions views:	1704
https://www.freecram.net/torrent/PECB.ISO-IEC-27001-Lead-Auditor.v2026-06-27.q169.html	

NEW QUESTION: 1
Scenario 6
Sinvestment is an insurance provider that offers a wide range of coverage options, including home, commercial, and life insurance. Originally established in North California, the company has expanded its operations to other locations, including Europe and Africa. In addition to its growth, Sinvestment is committed to complying with laws and regulations applicable to its industry and preventing any information security incident. They have implemented an information security management system (ISMS) based on ISO
/IEC 27001 and have applied for certification.
A team of auditors was assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment, they started the audit activities. For the activities of the stage 1 audit, it was decided that they would be performed on site, except the review of documented information, which took place remotely, as requested by Sinvestment.
The audit team started the stage 1 audit by reviewing the documentation required, including the declaration of the ISMS scope, information security policies, and internal audit reports. The evaluation of the documented information was based on the content and procedure for managing the documented information.
In addition, the auditors found out that the documentation related to information security training and awareness programs was incomplete and lacked essential details. When asked, Sinvestment's top management stated that the company has provided information security training sessions to all employees.
The stage 2 audit was conducted three weeks after the stage 1 audit. The audit team observed that the marketing department (not included in the audit scope) had no procedures to control employees' access rights.
Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the company's information security policy, the issue was included in the audit report.
Question
Was Sinvestment's request for reviewing documented information remotely acceptable?
A. Yes, documented information can be reviewed remotely.
B. No, as it can lead to a breach of confidentiality.
C. No, as the combination of different locations can negatively impact the audit efficiency.
Answer: (SHOW ANSWER)
Sinvestment's request to review documented information remotely during the stage 1 audit is acceptable and aligns with established auditing practices, making option A the correct answer. ISO/IEC 17021-1 and ISO
19011:2018 both permit flexibility in how audit activities are conducted, including the use of remote techniques, provided confidentiality, integrity, and effectiveness of the audit are maintained.
Stage 1 audits are primarily focused on reviewing documented information, understanding the organization's context, confirming the ISMS scope, and assessing readiness for stage 2. Reviewing documents remotely is a widely accepted practice, especially when supported by appropriate confidentiality agreements, as was the case in this scenario. The auditors had already signed confidentiality agreements, mitigating the risk of information disclosure.
Option B is incorrect because remote document review does not inherently lead to a breach of confidentiality.
Risks must be managed, not assumed. Secure document-sharing platforms and confidentiality agreements are sufficient safeguards when properly implemented. Option C is incorrect because the use of different locations or remote methods does not automatically reduce audit efficiency; in many cases, it enhances efficiency by reducing travel time and allowing better preparation.

Therefore, allowing remote review of documented information during stage 1 is fully consistent with ISO auditing standards and recognized certification body practices.

NEW QUESTION: 2
Scenario 6: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti- malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.
Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles This phase was crucial for aligning the team with the audit's objectives and scope However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber Acrypt's policies This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.
The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO /IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.
The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.
The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert s objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.
Based on the scenario above, answer the following question:
Question:
Which criteria for evaluating documented information was NOT validated by the audit team? (Refer to Scenario 6)
A. Content of the documented information
B. Format of the documented information
C. Procedure for managing the documented information
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* Scenario 6 states that the audit team reviewed the content and format of the documents but does not mention an evaluation of the document management procedure.
* ISO/IEC 27001 requires that procedures for managing documented information be reviewed.
* A. Incorrect:
* The content of documents was reviewed for compliance with ISO/IEC 27001 clauses.
* B. Incorrect:
* The audit team confirmed that all documents were in a standardized format.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 7.5 (Documented Information Requirements)

NEW QUESTION: 3
During an opening meeting of a Stage 2 audit, the Managing Director of the client organisation invites the audit team to view a new company video lasting 45 minutes. Which two of the following responses should the audit team leader make?
A. Advise the Managing Director that the audit team has to keep to the planned schedule

B. State that the audit team leader will stay behind after the opening meeting to view the video on behalf of the team
C. Invite the Managing Director to the auditors' hotel for a viewing that evening.
D. Suggest that the video could be viewed during a refreshment break
E. State that the audit team will make a decision on the viewing at a later time
F. Advise the Managing Director that the audit team agrees to his request
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, an opening meeting is a formal communication between the audit team and the auditee at the start of an audit1. The purpose of the opening meeting is to confirm the audit objectives, scope and criteria, introduce the audit team and their roles, confirm the audit plan and logistics, explain the audit methods and procedures, and establish the communication channels1. Therefore, if the Managing Director of the client organization invites the audit team to view a new company video lasting 45 minutes during the opening meeting of a Stage 2 audit, the audit team leader should respond in a way that does not compromise the effectiveness and efficiency of the audit or create any misunderstanding or conflict with the auditee. Two possible ways to respond are to advise the Managing Director that the audit team has to keep to the planned schedule, as there may be limited time and resources available for the audit; or to suggest that the video could be viewed during a refreshment break, if it is relevant and useful for the audit and does not interfere with other audit activities1. The other options are not appropriate responses for the audit team leader to make in this situation. For example, stating that the audit team leader will stay behind after the opening meeting to view the video on behalf of the team may imply that the video is not important or relevant for the rest of the audit team; inviting the Managing Director to the auditors' hotel for a viewing that evening may create an impression of bias or favouritism; stating that the audit team will make a decision on the viewing at a later time may be vague or indecisive; and advising the Managing Director that the audit team agrees to his request may result in wasting valuable audit time or losing focus on the audit objectives1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 4
Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.
Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments.
Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.
During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC
27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.
Based on the scenario above, answer the following question:
Question:
Auditors recommended Techmanic for certification after following up on corrective actions remotely. Is this acceptable?
A. Yes, auditors may follow up on action plans remotely since minor nonconformities were detected
B. No, an audit follow-up must be performed since the audit report contained nonconformities
C. No, an audit follow-up must be performed on-site since an extension was requested
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Remote follow-ups are acceptable for minor nonconformities, as long as auditors can verify corrective actions.
* ISO/IEC 17021-1:2015 allows remote follow-ups when the effectiveness of corrective actions can be demonstrated.

* B. Incorrect:
* Follow-ups are required, but remote verification is acceptable for minor issues.
* C. Incorrect:
* An on-site follow-up is not mandatory unless major nonconformities are present.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.6.8 (Remote Audit Follow-Ups)

NEW QUESTION: 5
You are an experienced ISMS audit team leader, assisting an auditor in training to write their first audit report.
You want to check the auditor in training's understanding of terminology relating to the contents of an audit report and chose to do this by presenting the following examples.
For each example, you ask the auditor in training what the correct term is that describes the activity Match the activity to the description.

An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met	
An auditor's note that the auditee is not adhering to its' clear desk policy	
An auditor making a decision regarding the auditee's conformity or otherwise to criteria	
An auditor examining verifiable records relevant to the audit process	

To complete the table, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

This example relates to the identification of an audit finding

This example relates to the use of audit criteria to determine conformity or nonconformity

This description relates to the determination of an audit conclusion

This example relates to relates to the collection of audit evidence

Answer:

An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met	This example relates to the use of audit criteria to determine conformity or nonconformity
An auditor's note that the auditee is not adhering to its' clear desk policy	This example relates to the identification of an audit finding
An auditor making a decision regarding the auditee's conformity or otherwise to criteria	This description relates to the determination of an audit conclusion
An auditor examining verifiable records relevant to the audit process	This example relates to relates to the collection of audit evidence

To complete the table, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

This example relates to the identification of an audit finding

This example relates to the use of audit criteria to determine conformity or nonconformity

This description relates to the determination of an audit conclusion

This example relates to relates to the collection of audit evidence

Explanation:

1. An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met:

Termed: Reviewing audit criteria.

Justification: The auditor is comparing the auditee's information security management system (ISMS) against the established criteria outlined in the ISO/IEC 27001:2022 standard. This activity falls under the use of audit criteria to determine conformity or nonconformity.

2. An auditor's note that the auditee is not adhering to its clear desk policy:

Termed: Identifying an audit finding.

Justification: The auditor has observed a deviation from the auditee's established policy on clear desks. This observation is documented as a potential nonconformity, which requires further investigation and evaluation.

3. An auditor making a decision regarding the auditee's conformity or otherwise to criteria:

Termed: Determining an audit conclusion.

Justification: Based on the collected audit evidence and evaluation against the established criteria, the auditor forms an opinion about the overall compliance of the auditee's ISMS. This opinion is the audit conclusion and is a key element of the audit report.

4. An auditor examining verifiable records relevant to the audit process:

Termed: Collecting audit evidence.

Justification: The auditor is gathering objective and verifiable information to support their findings and conclusions. This information comes from various sources, including documents, records, interviews, and observations.

An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met	This example relates to the use of audit criteria to determine conformity or nonconformity
An auditor's note that the auditee is not adhering to its' clear desk policy	This example relates to the identification of an audit finding
An auditor making a decision regarding the auditee's conformity or otherwise to criteria	This description relates to the determination of an audit conclusion
An auditor examining verifiable records relevant to the audit process	This example relates to relates to the collection of audit evidence

NEW QUESTION: 6
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the PHYSICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. Access to and from the loading bay
B. How power and data cables enter the building
C. Information security awareness, education, and training
D. The conducting of verification checks on personnel
E. The development and maintenance of an information asset inventory
F. The operation of the site CCTV and door control systems
G. The organisation's arrangements for maintaining equipment
H. The organisation's business continuity arrangements
Answer: (SHOW ANSWER)
The four controls from the list that are related to PHYSICAL aspects of the ISMS are:
*Access to and from the loading bay
*How power and data cables enter the building
*The operation of the site CCTV and door control systems
*The organisation's arrangements for maintaining equipment
These controls are derived from the ISO 27001 Annex A, which provides a comprehensive list of information security controls that can be applied to an ISMS1. The other controls in the list are more related to ORGANIZATIONAL, LEGAL, or HUMAN aspects of the ISMS, which are also important, but not the focus of this question.
According to the ISMS Auditing Guideline2, the auditor in training should review the PHYSICAL controls by:
*Checking the SoA to identify the applicable controls and their implementation status
*Interviewing the relevant staff and management to verify their understanding and involvement in the controls
*Observing the physical and environmental conditions to confirm the existence and effectiveness of the controls
*Examining the relevant documents and records to validate the compliance and performance of the controls I hope this helps you prepare for the exam. # References: 1: What Are ISO 27001 Controls? A Guide to Annex A | Secureframe; 2: ISMS Auditing Guideline - ISO27000

NEW QUESTION: 7

Question:
What is the main difference between qualitative and quantitative evidence?
A. Qualitative evidence originates from the analysis of a sample related to determining the audit criteria, while quantitative evidence originates from the analysis of unquantifiable information
B. Qualitative evidence focuses on evaluating if a process or control complies with the audit criteria, while quantitative evidence aims to determine if a process in operation is functional and effective
C. Qualitative evidence is used to make estimations about the whole population, while quantitative evidence focuses on evaluating if a process complies with standard requirements
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Qualitative evidence assesses whether processes comply with audit criteria based on descriptive, observational, and interview-based data.
* Quantitative evidence uses numerical data (e.g., metrics, statistics, or performance indicators) to assess if a process is functional and effective.
* A. Incorrect:
* Qualitative evidence is not limited to sampling and quantitative evidence is based on measurable data.
* C. Incorrect:
* Qualitative evidence does not estimate populations; it is subjective and descriptive.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.7 (Types of Audit Evidence: Qualitative vs. Quantitative)

NEW QUESTION: 8
You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymisation tests failed. Also, whether the Service Manager is authorised to approve the test.
The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymisation functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You are preparing the audit findings. Select the correct option.
* There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.
(Relevant to clause 8.1, control A.8.29)
A. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
B. There is a nonconformity (NC). The organisation and developer perform security tests that fail.
(Relevant to clause 8.1, control A.8.29)
C. There is NO nonconformity (NC). The Service Manager makes a good decision to continue the service.
(Relevant to clause 8.1, control A.8.30)
Answer: (SHOW ANSWER)
According to ISO 27001:2022 Annex A Control 8.30, the organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This includes developing and entering into licensing agreements that cover code ownership and intellectual property rights, and implementing appropriate contractual requirements related to secure design and coding in accordance with Annex A 8.25 and 8.2912 In this case, the organisation and the developer have performed security tests that failed, which indicates that the secure design and coding requirements of Annex A 8.29 were not met. The IT Manager explains that the encryption and pseudonymisation functions failed because they slowed down the system and service performance, and that an extra 150% of resources are needed to cover this. However, this does not justify the acceptance of the test results by the Service Manager, who is not authorised to approve the test according to the software security management procedure. The Service Manager should have consulted with the IT Manager, who is the owner of the process, and followed the procedure for handling nonconformities and corrective actions. The Service Manager's decision to continue the service based on access control alone exposes the organisation to the risk of compromising the confidentiality, integrity, and availability of personal data processed by the mobile app.
Therefore, there is a nonconformity (NC) with clause 8.1, control A.8.30.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 9

Question
Which statement best describes how internal audits and external audits complement each other in an organization?
A. Internal audits regularly review the organization's processes to identify issues and improvements, providing input that supports preparation for external audits
B. Internal audits mainly monitor external auditors' reports and action plans without conducting their own assessments
C. External audits focus on ongoing internal improvements while internal audits verify certification readiness
Answer: (SHOW ANSWER)
The correct answer is A, because internal and external audits serve different but complementary purposes within an ISO/IEC 27001-based ISMS. Internal audits are conducted by or on behalf of the organization to regularly assess the effectiveness, conformity, and continual improvement of the ISMS. Their results help management identify weaknesses, risks, and opportunities for improvement before they become systemic issues.
ISO/IEC 27001 requires organizations to conduct internal audits at planned intervals to ensure the ISMS conforms to both internal requirements and the standard. These audits provide valuable input into management reviews, corrective actions, and readiness for external audits. In this way, internal audits act as an early warning and improvement mechanism.
External audits, conducted by an independent certification body, rely partly on the maturity demonstrated through internal audit outcomes. They verify whether the organization's ISMS meets ISO/IEC 27001 requirements and whether internal audits are effective and properly implemented.
Option B is incorrect because internal audits are not passive reviews of external audit outputs; they are independent assessments with their own scope and objectives. Option C is incorrect because the roles are reversed: internal audits focus on ongoing internal improvement, while external audits focus on certification conformity.
Therefore, internal audits directly support and complement external audits by strengthening ISMS readiness and effectiveness.

NEW QUESTION: 10
Question:
Which of the following best defines managerial controls?
Freecram.net
A. Controls related to the management of personnel, including training of employees, management reviews, and internal audits
B. Controls related to organizational structure, such as segregation of duties, job rotations, job descriptions, and approval processes
C. Controls related to the use of technical measures or technologies, such as firewalls, alarm systems, surveillance cameras, and IDSs
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* Managerial controls (also called administrative controls) include policies, procedures, and processes to ensure effective security governance. These controls include training, internal audits, security awareness programs, and management reviews. These align with ISO/IEC 27001:2022 Annex A Control A.5.2 (Information Security Roles and Responsibilities) and A.5.3 (Segregation of Duties).
* B. Organizational structure controls relate to segregation of duties and job rotations, making them structural controls rather than purely managerial.
* C. Technical controls involve firewalls, IDSs, and other security mechanisms, which are not managerial but technical measures.

NEW QUESTION: 11
After completing Stage 1 and in preparation for a Stage 2 initial certification audit, the auditee informs the audit team leader that they wish to extend the audit scope to include two additional sites that have recently been acquired by the organisation. Considering this information, what action would you expect the audit team leader to take?
A. Arrange to complete a remote Stage 1 audit of the two sites using a video conferencing platform
B. Increase the length of the Stage 2 audit to include the extra sites
C. Inform the auditee that the audit team leader accepts the request
D. Obtain information about the additional sites to inform the individual(s) managing the audit programme
Answer: (SHOW ANSWER)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the audit team leader should obtain information about the additional sites to inform the individual(s) managing the audit programme, as this may affect the audit objectives, scope, criteria, duration, resources, and risks. The audit team leader should also review the audit plan and make any necessary adjustments in consultation with the auditee and the audit client1. References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 27, section
4.3.2.2.

NEW QUESTION: 12
Scenario:
Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively online and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.
Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personally identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.
Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.
Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week. Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.
Question:
According to Scenario 1, Northstorm reviewed users' access rights. What is the type and function of this security control?
A. Detective and administrative
B. Corrective and managerial
C. Legal and technical
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Security controls can be classified by type (administrative, technical, physical) and function (preventive, detective, corrective).
* A. Detective and administrative - Correct Answer. Reviewing access rights is an administrative control because it involves procedural security measures (such as policy enforcement and auditing). It is also a detective control because it helps identify inappropriate or unauthorized access by auditing and verifying user permissions.
* B. Corrective and managerial - Incorrect because reviewing user access rights does not correct an issue but rather detects potential unauthorized access. It is also administrative, not managerial.
* C. Legal and technical - Incorrect because reviewing user access rights is an administrative policy- based action, not a legal or technical control.
This aligns with ISO/IEC 27001:2022 Annex A Control A.5.18 (Access Rights), which mandates regular review of user access to prevent unauthorized access and enforce security policies.

NEW QUESTION: 13
Scenario 2: Knight is an electronics company from Northern California, US that develops video game consoles. Knight has more than 300 employees worldwide. On the fifth anniversary of their establishment, they have decided to deliver the G-Console, a new generation video game console aimed for worldwide markets. G-Console is considered to be the ultimate media machine of 2021 which will give the best gaming experience to players.
The console pack will include a pair of VR headset, two
games, and other gifts.
Over the years, the company has developed a good reputation by showing integrity, honesty, and respect toward their customers. This good reputation is one of the reasons why most passionate gamers aim to have Knight's G-console as soon as it is released in the market.
Besides being a very customer-oriented company, Knight
also gained wide recognition within the gaming industry because of the developing quality. Their prices are a bit higher than the reasonable standards allow.
Nonetheless, that is not considered an issue for most loyal customers of Knight, as their quality is top-notch.
Being one of the top video game console developers in the world, Knight is also often the center of attention for malicious activities. The company has had an operational ISMS for over a year. The ISMS scope includes all departments of Knight, except Finance and HR departments.

Recently, a number of Knight's files containing proprietary information were leaked by hackers. Knight's incident response team (IRT) immediately started to analyze every part of the system and the details of the incident.
The IRT's first suspicion was that Knight's employees used weak passwords and consequently were easily cracked by hackers who gained unauthorized access to their accounts. However, after carefully investigating the incident, the IRT determined that hackers accessed accounts by capturing the file transfer protocol (FTP) traffic.
FTP is a network protocol for transferring files between accounts. It uses clear text passwords for authentication.
Following the impact of this information security incident and with IRT's suggestion, Knight decided to replace the FTP with Secure Shell (SSH) protocol, so anyone capturing the traffic can only see encrypted data.
Following these changes, Knight conducted a risk assessment to verify that the implementation of controls had minimized the risk of similar incidents. The results of the process were approved by the ISMS project manager who claimed that the level of risk after the implementation of new controls was in accordance with the company's risk acceptance levels.
Based on this scenario, answer the following question:
Based on scenario 2, the ISMS project manager approved the results of risk assessment. Is this acceptable?
A. No, the risk remaining after the treatment of risk should be approved by the top management at any stage
B. No, the risk remaining after the implementation of new controls for the ISMS should be approved by the ISMS team
C. Yes, the risk remaining after the treatment of risk should be approved by the ISMS project manager
Answer: (SHOW ANSWER)
In the context of ISO/IEC 27001, the approval of the risk assessment and the acceptance of the remaining risk levels after treatment are typically responsibilities of the top management. This is because top management is accountable for the information security management system and its outcomes, and they have the authority to accept risks on behalf of the organization12. References: = The information provided is based on the standard practices of ISO/IEC 27001 risk assessment and treatment processes, which emphasize the role of top management in the approval and acceptance of risks

NEW QUESTION: 14
You are carrying out a third-party surveillance audit of a client's ISMS. You are currently in the secure storage area of the data centre where the organisation's customers are able to temporarily locate equipment coming into or going out of the site. The equipment is contained within locked cabinets and each cabinet is allocated to a single, specific client.
Out of the corner of your eye you spot movement near the external door of the storage area. This is followed by a loud noise. You ask the guide what is going on. They tell you that recent high rainfall has raised local river levels and caused an infestation of rats. The noise was a specialist pest control stunning device being triggered. You check the device in the corner and find there is a large immobile rat contained within it.
What three actions would be appropriate to take next?
A. Take no further action. This is an ISMS audit, not an environmental management system audit
B. Investigate whether pest infestation is an identified risk and if so, what risk treatment is to be applied
C. Determine whether the high levels of rainfall have had other impacts on data centre operations e.g.
damage to infrastructure, access issues for clients, invocation of business continuity arrangements
D. Raise a nonconformity against control 7.4 Physical Security monitoring
E. Raise a nonconformity against control 7.2 Physical Entry
F. Check with the guide that they intend to initiate the organisation's information security incident process
G. Inspect the client cabinets for signs of rodent ingress and record your findings as audit evidence
H. Assist the guide in humanely disposing of the rat and reset the device
Answer: B,C,F (LEAVE A REPLY)
The appropriate actions to take next are to investigate whether pest infestation is an identified risk and if so, what risk treatment is to be applied, to determine whether the high levels of rainfall have had other impacts on data centre operations, and to check with the guide that they intend to initiate the organisation's information security incident process. These actions are relevant to the ISMS audit objectives and criteria, as they relate to the organisation's risk assessment and treatment, security performance, and incident management processes.
The other actions are either not within the scope of the ISMS audit, not required by the ISO/IEC 27001 standard, or not the responsibility of the auditor. References: PECB Candidate Handbook1, page 21-22; ISO
/IEC 27001:2022 (en)2, clauses 6.1, 8.2, 9.1, and 10.2.

NEW QUESTION: 15
Question:

According to ISO/IEC 27001, Clause 5.1 (Leadership and Commitment), which of the following is NOT a responsibility of top management?
A. Ensuring the availability of resources for the ISMS and promoting continual improvement
B. Conducting regular internal audits to assess the effectiveness of the ISMS
C. Directing and supporting persons to contribute to the effectiveness of the ISMS
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
ISO/IEC 27001 Clause 5.1 (Leadership and Commitment) defines top management's role in ensuring the effectiveness of the Information Security Management System (ISMS). It requires top management to:
* Ensure the availability of resources for the ISMS (Correct Responsibility).
* Promote continual improvement of the ISMS (Correct Responsibility).
* Direct and support employees to contribute to ISMS effectiveness (Correct Responsibility).
B). Conducting regular internal audits - Incorrect Responsibility:
* Internal audits are not a direct responsibility of top management. Instead, Clause 9.2 (Internal Audit) requires audits to be conducted independently of management.
* Top management is responsible for ensuring audits are conducted but does not need to conduct them personally.
Thus, top management is responsible for oversight and support but not for conducting internal audits themselves.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 5.1 (Leadership and Commitment)
* ISO/IEC 27001:2022 Clause 9.2 (Internal Audit)

NEW QUESTION: 16
Question
The top management of a company has designated specific personnel within the company to be responsible for reporting on the performance of the ISMS. These individuals are tasked with gathering relevant ISMS data, preparing reports, and ensuring that necessary information reaches the top management.
Does this approach align with ISO/IEC 27001 requirements?
A. Yes, because the top management can assign responsibilities and authorities for reporting on the performance of the ISMS.
B. No, because only the top management is responsible for gathering data on the performance of the ISMS.
C. No, because only the Chief Information Security Officer should report on the performance of the ISMS.
Answer: (SHOW ANSWER)
This approach aligns with ISO/IEC 27001:2022 because the standard explicitly allows top management to assign responsibilities and authorities for the effective operation of the ISMS, including reporting on its performance. Clause 5.3 of ISO/IEC 27001 requires top management to ensure that roles, responsibilities, and authorities related to information security are assigned and communicated within the organization.
While top management remains ultimately accountable for the ISMS, the standard does not require them to personally gather data, prepare reports, or perform operational monitoring activities. In practice, these tasks are often delegated to ISMS managers, security teams, or other designated personnel who are better positioned to collect and analyze performance data. What matters is that the information reaches top management in a timely and accurate manner so they can fulfill their governance responsibilities.
Option B is incorrect because it misunderstands accountability versus responsibility. Top management is accountable for ISMS performance, but they are not required to perform all related tasks themselves. Option C is incorrect because ISO/IEC 27001 does not mandate that a Chief Information Security Officer must be the reporting authority. The organization is free to define roles based on its structure, size, and context.
Therefore, assigning specific personnel to report on ISMS performance is fully consistent with ISO/IEC
27001 requirements.

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
Question
An auditor is reviewing a company's financial transactions over the past year. They are using a technology that helps them detect unusual spending behaviors, such as repeated transactions just below the approval threshold, which could indicate fraudulent activity.
What technology is the auditor using in this case?
A. Data mining
B. Data management
C. Predictive analytics
Answer: (SHOW ANSWER)
Explanation (Audit & analytics perspective)
* Data mining focuses on discovering patterns, anomalies, and relationships in historical datasets.
* Identifying repeated transactions just below approval thresholds is a classic data mining technique.
* Predictive analytics focuses on forecasting future outcomes, not detecting historical anomalies.
Data management is concerned with storage and governance, not analysis.

NEW QUESTION: 18
Question
Company XYZ, a software development company certified under ISO/IEC 27001, informs the certification body a year after certification that they are not prepared for the scheduled surveillance audit and refuse to undergo it. What is the immediate consequence in this situation?
A. The certification is suspended
B. The current certification remains valid until the next surveillance audit
C. The company must initiate a formal transfer of certification to another certification body
Answer: (SHOW ANSWER)
The immediate consequence is suspension of certification, making option A correct. ISO/IEC 17021-1 clearly states that certified organizations must allow scheduled surveillance audits to verify continued conformity with the standard. Surveillance audits are mandatory and form part of the three-year certification cycle.
Refusing or failing to undergo a surveillance audit prevents the certification body from confirming that the ISMS remains effective and compliant. This creates a loss of confidence in the validity of the certification. As a result, certification bodies are required to suspend certification until the audit can be conducted and conformity re-established.
Option B is incorrect because certification validity is conditional upon ongoing surveillance. Certification does not remain valid if mandatory audits are refused. Option C is incorrect because transferring certification does not remove the obligation to undergo surveillance audits; a transfer would still require evidence of conformity and audit continuity.
Suspension is a protective mechanism to ensure that ISO/IEC 27001 certificates remain credible and trustworthy. If the organization later agrees to the audit and resolves issues, the certification may be reinstated. Therefore, refusal to undergo a surveillance audit leads to immediate suspension.

NEW QUESTION: 19
Which one of the following options best describes the purpose of a Stage 2 audit?
A. To check for legal compliance by the organisation
B. To ensure that the audit plan is carried out

C. To evaluate the implementation of the management system
D. To get to know the organisation's processes
Answer: C (LEAVE A REPLY)
The purpose of a Stage 2 audit is to evaluate the implementation of the management system, in this case, the ISMS, according to the requirements of ISO/IEC 27001:2022 and the organisation's own policies and procedures. The Stage 2 audit involves collecting evidence of the effectiveness and performance of the ISMS, as well as verifying the conformity and suitability of the organisation's controls. The Stage 2 audit also assesses the organisation's ability to achieve its information security objectives and to manage information security risks. References: = ISO/IEC 27006:2022, clause 9.2.2.2; PECB Candidate Handbook ISO 27001 Lead Auditor, page 28.

NEW QUESTION: 20
Scenario 5: Cobt. an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well- versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organizations internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification Sarah, an experienced auditor, was assigned to the audit Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes Therefore, her initial focus was to gather information on how the company manages its information security risks Sarah contacted Cobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence Moreover, Cobt raised concerns about the audit schedule, stating that it does not properly reflect the recent changes the company made It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the scenario above, answer the following question:
Question:
Based on Scenario 5, Sarah decided to withdraw from the audit before a certification agreement was signed. Is this acceptable?
A. Yes, Sarah can withdraw from the audit but only if the certification body approves her withdrawal
B. Yes, there is no relation between Sarah's withdrawal from the audit and the certification agreement
C. No, the certification agreement is directly tied to the auditor's presence
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:

Freecram.net

* B. Correct Answer: The certification agreement is between the certification body and the organization (Cobt), not the auditor. Therefore, Sarah's withdrawal does not impact the certification agreement itself.
* A. Incorrect: Sarah does not need approval from the certification body to withdraw, as she had not yet signed the certification agreement.
* C. Incorrect: The certification agreement is not dependent on a specific auditor; it is an agreement between the organization and the certification body.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2 (Internal Audit) & ISO 19011:2018 Clause 6.4.10 (Conducting Closing Meetings)

NEW QUESTION: 21
As the ISMS audit team leader, you are conducting a second-party audit of an international logistics organisation on behalf of an online retailer. During the audit, one of your team members reports a nonconformity relating to control 5.18 (Access rights) of Annex A of ISO/IEC 27001:2022. The control was justified in the Statement of Applicability. She found evidence that removing the server access protocols of 20 people who left in the last 3 months took up to 1 week whereas the policy required removing access within 24 hours of their departure.
Select the three most appropriate actions taken by the auditee to deal with this situation.
A. Change the process to ensure that leaver access protocols are removed before personnel leaves the premises
B. Ensure that removing the server access protocols of leavers from senior management positions is prioritised
C. Reprimand the IT team for failing to remove the access protocols in the required timescale
D. Investigate whether the delays in removing access protocols caused any security breaches
E. Monitor the ongoing process of removing leaver access protocols to determine whether it meets requirements
F. Employee more IT personnel to ensure that the specified timescale can be met.
G. Revisit the security risk assessment process to re-evaluate the timescale for the removal of leaver access rights
H. Extend the required removal period from 24 hours to 7 days
Answer: (SHOW ANSWER)

NEW QUESTION: 22
You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including misaddressed labels and, in 15% of cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).
You: Are items checked before being dispatched?
SM: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.
You: What action is taken when items are returned?
SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.
You raise a nonconformity. Referencing the scenario, which three of the following Annex A controls would you expect the auditee to have implemented when you conduct the follow-up audit?
* 5.11 Return of assets
A. 5.13 Labelling of information
B. 5.3 Segregation of duties
C. 5.32 Intellectual property rights
D. 5.34 Privacy and protection of personal identifiable information (PII)
E. 5.6 Contact with special interest groups
F. 6.3 Information security awareness, education, and training
G. 6.4 Disciplinary process
Answer: (SHOW ANSWER)
The three Annex A controls that you would expect the auditee to have implemented when you conduct the follow-up audit are:
* B. 5.13 Labelling of information

* E. 5.34 Privacy and protection of personal identifiable information (PII)
* G. 6.3 Information security awareness, education, and training
* B. This control requires the organisation to label information assets in accordance with the information classification scheme, and to handle them accordingly12. This control is relevant for the auditee because it could help them to avoid misaddressing labels and sending parcels to wrong destinations, which could compromise the confidentiality, integrity, and availability of the information assets. By labelling the information assets correctly, the auditee could also ensure that they are delivered to the intended recipients and that they are protected from unauthorized access, use, or disclosure.
* E. This control requires the organisation to protect the privacy and the rights of individuals whose personal identifiable information (PII) is processed by the organisation, and to comply with the applicable legal and contractual obligations13. This control is relevant for the auditee because it could help them to prevent the unauthorized use of residents' personal data by a supplier, which could violate the privacy and the rights of the residents and their family members, and expose the auditee to legal and reputational risks. By protecting the PII of the residents and their family members, the auditee could also enhance their trust and satisfaction, and avoid complaints and disputes.
* G. This control requires the organisation to ensure that all employees and contractors are aware of the information security policy, their roles and responsibilities, and the relevant information security procedures and controls14. This control is relevant for the auditee because it could help them to improve the information security culture and behaviour of their staff, and to reduce the human errors and negligence that could lead to information security incidents. By providing information security awareness, education, and training to their staff, the auditee could also increase their competence and performance, and ensure the effectiveness and efficiency of the information security processes and controls.
References:
1: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, Annex A 2: ISO/IEC 27002:2022 - Information technology - Security techniques - Code of practice for information security controls, clause 8.2.1 3: ISO/IEC 27002:
2022 - Information technology - Security techniques - Code of practice for information security controls, clause 18.1.4 4: ISO/IEC 27002:2022 - Information technology - Security techniques - Code of practice for information security controls, clause 7.2.2

NEW QUESTION: 23
Question:
During which stage of the audit do auditors identify key processes to be audited and prioritize based on materiality?
A. Initial contact
B. Stage 1 audit
C. Stage 2 audit
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The Stage 1 audit (preliminary assessment) focuses on understanding the organization and its processes, identifying key areas for in-depth auditing in Stage 2.
* Materiality-based prioritization occurs in Stage 1 to ensure the Stage 2 audit focuses on critical areas.
* A. Incorrect:
* Initial contact is only for scheduling and preliminary discussions.
* C. Incorrect:
* By Stage 2, the key areas should already be identified and the focus is on detailed auditing.
Relevant Standard Reference:
* ISO/IEC 27006:2020 Clause 9.2.2 (Stage 1 Audit and Planning for Stage 2 Audit)

NEW QUESTION: 24
As the Information Security Management System audit team leader, you are conducting a second-party audit of an international logistics company on behalf of an online retailer. During the audit, one of your team members reports a nonconformity relating to control 5.18 (Access rights) of Appendix A of ISO/IEC 27001:
2022. She found evidence that removing the server access protocols of 20 people who left in the last 3 months took up to 1 week whereas the policy required removing access within 24 hours of their departure.
When the auditee was asked why there was a delay in removing access they replied, 'no one was available in the IT department during that period as a result of COVID-19. As soon as an IT officer became available the rights were removed.
You note that she intends to raise a minor non-conformity against Access rights control (5.18). How should you respond to this?

A. Agree with the raising of a minor non-conformity but against control 5.15, not 5.18.
B. Disagree with the raising of a minor conformity as appropriate action was taken at the earliest opportunity Take no further action.
C. Agree with the raising of the minor non-conformity against 5.18.
D. Disagree with the raising of the minor nonconformity as appropriate action was taken at the earliest opportunity. Instead raise an opportunity for improvement.
E. Require additional audit evidence to be obtained before determining whether a non-conformity is appropriate.
F. Disagree with the raising of the minor nonconformity, there is sufficient evidence to justify an escalation to a major non-conformity.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Scenario 6: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti- malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.
Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles This phase was crucial for aligning the team with the audit's objectives and scope However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber Acrypt's policies This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.
The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO /IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.
The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.
The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert s objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.
Based on the scenario above, answer the following question:
Question:
Based on Scenario 6, is the audit team leader's decision regarding the technical expert's behavior acceptable?
A. No, the audit team leader should have reported the issue directly to the top management instead
B. No, questioning the expert's objectivity is not a valid reason for the audit team leader to discuss the matter with the certification body
C. Yes, if the auditor is skeptical about the technical expert's objectivity, he must discuss his concerns with the certification body
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* ISO 17021-1:2015 Clause 5.2.4 requires auditors to report impartiality concerns.
* The technical expert received consultancy fees from Cyber ACrypt, creating a conflict of interest.
* The certification body must be informed to ensure audit integrity.
* A. Incorrect:
* Reporting to top management does not resolve certification body independence concerns.
* B. Incorrect:

* Impartiality is a critical concern in ISO/IEC 27001 certification.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 5.2.4 (Ensuring Impartiality in Audits)

NEW QUESTION: 26
Scenario 5: Cobt. an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well- versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organizations internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification Sarah, an experienced auditor, was assigned to the audit Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes Therefore, her initial focus was to gather information on how the company manages its information security risks Sarah contacted Cobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence Moreover, Cobt raised concerns about the audit schedule, stating that it does not properly reflect the recent changes the company made It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the scenario above, answer the following question:
Question:
Based on Scenario 5, Cobt stated that the audit schedule did not properly reflect the recent changes they made in the audit scope. What should Sarah do in this case?
A. Change the audit schedule as requested by Cobt as the scope should reflect the status and importance of the activities to be audited
B. Continue the audit with the initial scope since Cobt can request a change in the audit scope only if there are recent changes in technologies in place
C. Change the audit schedule only if Cobt, Sarah, and the certification body agree on the changes in the audit scope
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer: Changes to the audit scope must be approved by the auditee, the auditor, and the certification body. This ensures fairness and maintains compliance with ISO 19011 guidelines on audit planning.
* A. Incorrect: The audit schedule cannot be changed solely at Cobt's request-approval is required.
* B. Incorrect: Audit scope is not limited to technological changes but includes organizational and procedural changes as well.
Relevant Standard Reference:
* ISO 19011:2018 Clause 5.5.2 (Determining the Audit Scope and Schedule)

NEW QUESTION: 27
AppFolk, a software development company, is seeking certification against ISO/IEC 27001. In the initial phases of the external audit, the certification body in discussion with the company excluded the marketing division from the audit scope, although they stated in their ISMS scope that the whole company is included. Is this acceptable?
A. Yes, audit and ISMS scope do not necessarily need to be the same
B. No, divisions that are not critical for the industrial sector in which the auditee operates can be excluded from the audit scope
C. No, audit scope should reflect all of the organization's divisions covered by the ISMS
Answer: (SHOW ANSWER)
No, the audit scope should reflect all of the organization's divisions that are covered by the ISMS. If the ISMS scope stated that it includes the whole company, the audit scope should align with this unless specifically justified and agreed upon by all stakeholders.

References: ISO/IEC 27001:2013, Clause 4.3 (Determining the scope of the information security management system)

NEW QUESTION: 28
Which two of the following standards are used as ISMS third-party certification audit criteria?
A. ISO/IEC 27002
B. ISO/IEC 20000-1
C. ISO 19011
D. ISO/IEC 27001
E. Relavent legal, statutory, and regulatory requirements
F. ISO/IEC 17021-1
Answer: (SHOW ANSWER)
The two standards that are used as ISMS third-party certification audit criteria are ISO/IEC 27001 and relevant legal, statutory, and regulatory requirements. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS)1. Relevant legal, statutory, and regulatory requirements are those that apply to the organization's information security aspects and objectives2. The other options are either not standards (E) or not directly related to the ISMS certification audit criteria (A, B, C, F). References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 1 \n2: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2

NEW QUESTION: 29
Scenario 3
NightCore, a multinational technology enterprise headquartered in the United States, specializes in e- commerce, cloud computing, digital streaming, and artificial intelligence (AI). After having an information security management system (ISMS) implemented for over a year, NightCore contracted a certification body to perform an audit for ISO/IEC 27001 certification.
The certification body formed a team of five auditors, with Jack as a team leader. Jack is renowned for his extensive auditing experience in risk management, information security controls, and incident management.
His skill set aligns well with the requirements of auditing principles and processes, enabling him to effectively comprehend the audit scope and apply relevant criteria effectively. Jack also demonstrates a solid understanding of NightCore's organizational structure, purpose, and management practices and the statutory and regulatory requirements applicable to its activities.
The audit carried out by the audit team followed a rational method to reach reliable and reproducible conclusions systematically. The audit team recognized that only information capable of being verified to some extent should be considered valid evidence. In some rare instances during the audit where the verification of certain information posed challenges and where its degree of verifiability was low, the auditors exercised their professional judgment to assess the reliability and determine the level of reliance that could be placed on such evidence.
During the audit, the auditors documented their observations and inspection notes regarding the operational planning and control of NightCore's ISMS operations. They also recorded observations of NightCore's inventory of information and associated assets. Additionally, the auditors reviewed the configuration of firewalls implemented to secure connections to network services.
As the audit approached its final stages, NightCore's commitment to upholding the highest levels of information security became evident. With ISO/IEC 27001 certification within reach, NightCore is well- positioned to achieve ISO/IEC 27001 certification, enhancing its reputation in the technology sector.
Question
What type of audit did NightCore undergo?
A. First party
B. Second party
C. Third party
Answer: (SHOW ANSWER)
NightCore underwent a third-party audit, making option C the correct answer. A third-party audit is conducted by an independent certification body for the purpose of assessing conformity against a recognized international standard, such as ISO/IEC 27001. This type of audit is required when an organization seeks formal certification.
In the scenario, NightCore explicitly contracted a certification body to perform an audit for ISO/IEC 27001 certification. The audit team was formed by the certification body, not by NightCore itself or by a customer or supplier. This independence is the defining characteristic of a third-party audit. The objective of such an audit is to determine whether the ISMS conforms to ISO/IEC 27001 requirements and whether certification can be granted.

Option A is incorrect because a first-party audit is an internal audit conducted by or on behalf of the organization itself. Although NightCore had conducted internal audits previously, the scenario clearly refers to a certification audit performed by an external body. Option B is incorrect because a second-party audit is conducted by an interested party, such as a customer auditing a supplier, which is not the case here.
Therefore, based on the involvement of an independent certification body and the goal of ISO/IEC 27001 certification, the audit conducted at NightCore is correctly classified as a third-party audit.

NEW QUESTION: 30

Question
Another auditor appointed by the certification body reviews the audit team leader's working documents before the audit conclusions are finalized. According to good auditing practice, which statement is correct?

Freecram.net

A. Such a review is acceptable if the reviewing auditor is appointed by the certification body and qualified to perform it
B. The audit team leader's work may only be reviewed after the audit conclusions have been finalized
C. The audit team leader alone is responsible for reviewing their own working documents without any external review
Answer: (SHOW ANSWER)
The correct answer is A, because peer review or independent review of audit working documents is an accepted and recommended auditing practice when performed by a qualified and authorized individual. ISO /IEC 17021-1 requires certification bodies to maintain quality assurance mechanisms, including review of audit documentation, to ensure audit consistency, impartiality, and technical validity.
Reviewing working documents before audit conclusions are finalized helps identify gaps, inconsistencies, or errors while corrective action is still possible. This strengthens the reliability of the audit outcome and supports sound certification decisions.
Option B is incorrect because limiting review to after conclusions are finalized reduces the effectiveness of quality control and may require rework. Option C is incorrect because auditors should not review their own work exclusively; independent review is a key safeguard against bias and oversight.
Therefore, a qualified auditor appointed by the certification body reviewing working documents prior to final conclusions is fully aligned with good auditing practice and accreditation requirements.

NEW QUESTION: 31

----------is an asset like other important business assets has value to an organization and consequently needs to be protected.
A. Infrastructure
B. Data
C. Information
D. Security
Answer: (SHOW ANSWER)
Information is an asset like other important business assets, as it has value to an organization and consequently needs to be protected. Information can be in any form, such as electronic, paper, or verbal. Information security is the protection of information from unauthorized access, use, disclosure, modification, or destruction2. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
Scenario 2:
Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces, dependencies between internal and outsourced activities, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.
Despite initial challenges, Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001 while incorporating additional sector-specific controls to enhance security. The team evaluated the applicability of these controls against internal and external factors, culminating in the development of a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.
As preparations for certification progressed, Brian, appointed as the team leader, adopted a self-directed risk assessment methodology to identify and evaluate the company's strategic issues and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and mission.
Question:
Based on Scenario 2, the Clinic decided that the ISMS would cover only key processes and departments. Is this acceptable?
A. Yes, but the decision to exclude other processes and departments must be justified
B. Yes, organizations may limit the scope of the ISMS, but they cannot request a certification audit if the ISMS scope does not include all processes and departments
C. No, Clinic must include all processes and departments in the scope, regardless of their importance or relevance to the ISMS
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer: ISO/IEC 27001 Clause 4.3 (Determining the Scope of the ISMS) allows organizations to limit the scope, provided that exclusions do not undermine security effectiveness and are justified.
* B. Incorrect: Organizations can request certification even if the ISMS scope is limited, as long as it is justified.
* C. Incorrect: ISO/IEC 27001 does not mandate full inclusion of all departments in the ISMS.
Clinic's decision is acceptable only if the exclusions are justified.

NEW QUESTION: 33
You are performing an ISMS audit at a European-based residential nursing home called ABC that provides healthcare services.
During the audit, you discovered evidence suggesting that ABC may be leaking personal data of residents' family members to a third party for marketing purposes, despite signed agreements prohibiting this.
Complaints were treated as nonconformities, and corrective actions were documented under procedure ISMS L2 10.1.
You decide to write a non-conformity. Select the best sentence for the nonconformity:
A. "When assessing the extent of action taken in response to a nonconformity, an auditor seeks evidence of corrective action that will allow recurrence of the issue."
B. "When conducting follow up audit of preventive action(s) taken in response to a nonconformity, an auditor seeks evidence confirming that there will be no recurrence of the Issue."
C. "When evaluating the action taken in response to a nonconformity an auditor seeks evidence of documented information that reduces the probability of a recurrence of the issue."
D. "When examining the completeness of action taken in response to a nonconformity, an auditor seeks an assurance from the auditee that they will prevent recurrence of the issue."
E. "When inspecting the extent of action taken in response to a nonconformity, an auditor seeks comfort that necessary corrections will prevent recurrence of the issue."
F. "When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue."
Answer: (SHOW ANSWER)
* ISO/IEC 27001:2022, clause 10.2 (Nonconformity and corrective action):
When a nonconformity occurs, the organization shall ... take action to control and correct it, and deal with the consequences; evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere; implement any action needed; review the effectiveness of any corrective action taken.
* The auditor's responsibility is to verify effectiveness of corrective actions. This means the auditor must look for evidence of change that actually addresses the root cause and prevents recurrence - not just temporary fixes, promises, or documentation.
* Let's analyse the distractors:
* A. Incorrect - corrective action should not allow recurrence.
* B. Incorrect - refers to preventive action, which ISO 27001:2022 no longer uses as a separate concept; instead, it is integrated into risk management.
* C. Weak - merely "reducing probability" is not sufficient; ISO 27001 requires elimination of causes to prevent recurrence.
* D. Incorrect - "assurance from the auditee" is not acceptable evidence; auditors need objective evidence, not verbal commitment.

* E. Incorrect - "comfort" is not an audit principle; ISO 19011 requires objective evidence.
* F. Correct - aligns directly with ISO 27001 clause 10.2: "review the effectiveness of any corrective action taken ... so that nonconformity does not recur." Thus, the correct nonconformity statement is:
"When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue."

NEW QUESTION: 34
Scenario 1: Fintive is a distinguished security provider for online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies that operate online and want to improve their information security, prevent fraud, and protect user information such as PII. Fintive centers its decision-making and operating process based on previous cases. They gather customer data, classify them depending on the case, and analyze them. The company needed a large number of employees to be able to conduct such complex analyses. After some years, however, the technology that assists in conducting such analyses advanced as well. Now, Fintive is planning on using a modern tool, a chatbot, to achieve pattern analyses toward preventing fraud in real-time. This tool would also be used to assist in improving customer service.
This initial idea was communicated to the software development team, who supported it and were assigned to work on this project. They began integrating the chatbot on their existing system. In addition, the team set an objective regarding the chatbot which was to answer 85% of all chat queries.
After the successful integration of the chatbot, the company immediately released it to their customers for use.
The chatbot, however, appeared to have some issues.
Due to insufficient testing and lack of samples provided to the chatbot during the training phase, in which it was supposed "to learn" the queries pattern, the chatbot failed to address user queries and provide the right answers. Furthermore, the chatbot sent random files to users when it received invalid inputs such as odd patterns of dots and special characters. Therefore, the chatbot was unable to properly answer customer queries and the traditional customer support was overwhelmed with chat queries and thus was unable to help customers with their requests.
Consequently, Fintive established a software development policy. This policy specified that whether the software is developed in-house or outsourced, it will undergo a black box testing prior to its implementation on operational systems.
According to scenario 1, the chatbot sent random files to users when it received invalid inputs. What impact might that lead to?
A. Leak of confidential information
B. Inability to provide service
C. Loss of reputation
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Scenario 3
NightCore, a multinational technology enterprise headquartered in the United States, specializes in e- commerce, cloud computing, digital streaming, and artificial intelligence (AI). After having an information security management system (ISMS) implemented for over a year, NightCore contracted a certification body to perform an audit for ISO/IEC 27001 certification.
The certification body formed a team of five auditors, with Jack as a team leader. Jack is renowned for his extensive auditing experience in risk management, information security controls, and incident management.
His skill set aligns well with the requirements of auditing principles and processes, enabling him to effectively comprehend the audit scope and apply relevant criteria effectively. Jack also demonstrates a solid understanding of NightCore's organizational structure, purpose, and management practices and the statutory and regulatory requirements applicable to its activities.
The audit carried out by the audit team followed a rational method to reach reliable and reproducible conclusions systematically. The audit team recognized that only information capable of being verified to some extent should be considered valid evidence. In some rare instances during the audit where the verification of certain information posed challenges and where its degree of verifiability was low, the auditors exercised their professional judgment to assess the reliability and determine the level of reliance that could be placed on such evidence.
During the audit, the auditors documented their observations and inspection notes regarding the operational planning and control of NightCore's ISMS operations. They also recorded observations of NightCore's inventory of information and associated assets. Additionally, the auditors reviewed the configuration of firewalls implemented to secure connections to network services.
As the audit approached its final stages, NightCore's commitment to upholding the highest levels of information security became evident. With ISO/IEC 27001 certification within reach, NightCore is well- positioned to achieve ISO/IEC 27001 certification, enhancing its reputation in the technology sector.
Question
During the audit at NightCore, the auditors focused on key areas of ISMS operations, including operational planning, asset inventory, and firewall configurations. What type of evidence did the auditors collect during the audit conducted at NightCore?
A. Analytical and documentary evidence
B. Physical and technical evidence

C. Mathematical evidence
Answer: (SHOW ANSWER)
The auditors primarily collected physical and technical evidence, making option B the correct answer.
Physical and technical evidence refers to evidence obtained through direct observation of systems, configurations, and operational practices, as well as inspection of tangible or technical elements within the organization's environment.
In the scenario, the auditors reviewed firewall configurations, examined operational planning and control activities, and inspected the inventory of information and associated assets. Firewall configurations are a clear example of technical evidence, as they involve system settings and security mechanisms that can be directly reviewed and validated. Asset inventories, while documented, are often verified through physical or system- level inspection to confirm their accuracy and completeness. Operational planning and control observations involve witnessing how processes are executed in practice, which also constitutes physical or technical evidence.
Option A is incorrect because analytical and documentary evidence would primarily involve reports, metrics, trend analysis, or formal documents without direct system inspection. While some documentation was reviewed, the scenario emphasizes inspection and observation of operational and technical controls. Option C is incorrect because mathematical evidence is not a recognized audit evidence category under ISO standards.
ISO 19011 recognizes observation and inspection as valid methods for collecting audit evidence, particularly when assessing the effectiveness of technical and operational controls. Therefore, the evidence collected in this audit is best classified as physical and technical evidence.

NEW QUESTION: 36
In the context of a third-party certification audit, confidentiality is an issue in an audit programme. Select two options which correctly state the function of confidentiality in an audit
A. Auditors are forced by regulatory requirements to maintain confidentiality in an audit
B. Observers in an audit team cannot access any confidential information
C. Confidentiality is one of the principles of audit conduct
D. Auditors should obtain the auditee's permission before using a camera or recording equipment
E. Audit information can be used for improving personal competence by the auditor
F. As an auditor is always accompanied by a guide, there is no risk to the auditee's sensitive information
Answer: C,D (LEAVE A REPLY)
Confidentiality is one of the principles of audit conduct that auditors should adhere to when performing audits. Confidentiality means that auditors should exercise discretion in the use and protection of information acquired in the course of their duties3. Auditors should respect the intellectual property rights of the auditee and other parties involved in the audit, and should not disclose any information that is sensitive, proprietary, or confidential without prior approval from the auditee or other authorized parties3. Auditors should also obtain the auditee's permission before using a camera or recording equipment during an audit, as these devices may capture confidential information or infringe on the privacy of individuals3. Therefore, these two options correctly state the function of confidentiality in an audit. The other options are either incorrect or irrelevant to confidentiality. For example, auditors are not forced by regulatory requirements to maintain confidentiality in an audit, but rather by ethical obligations and contractual agreements3. Observers in an audit team can access confidential information if they have signed a confidentiality agreement and have been authorized by the auditee3. Audit information can be used for improving personal competence by the auditor only if it does not compromise confidentiality or conflict with other interests3. As an auditor is always accompanied by a guide, there is still a risk to the auditee's sensitive information if the guide is not trustworthy or authorized to access such information3. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 37
Question
Who establishes the audit scope and audit criteria?
A. The audit team leader
B. The audit team after discussing with the auditee
C. The certification body
Answer: (SHOW ANSWER)
The correct answer is the certification body, because ISO/IEC 17021-1 clearly assigns responsibility for establishing the audit scope and audit criteria to the certification body, not to the audit team or the auditee.
The certification body is responsible for managing the certification process, ensuring consistency, impartiality, and compliance with accreditation requirements.
The audit scope defines the boundaries of the certification audit, including organizational units, locations, activities, and processes to be audited. The audit criteria define the set of policies, procedures, and requirements against which conformity is assessed, such as ISO/IEC 27001 requirements, statutory obligations, and internal ISMS policies. While the audit team leader may plan how the audit will be conducted within the defined scope, they do not determine the scope itself.

Option A is incorrect because the audit team leader's role is to manage the audit execution, prepare the audit plan, and coordinate audit activities, not to establish the official scope or criteria. Option B is incorrect because although discussions with the auditee are necessary to understand the organization and confirm scope feasibility, the final authority remains with the certification body.
This separation of responsibility ensures independence and prevents organizations from unduly influencing the certification boundaries. Therefore, the certification body is the entity that establishes the audit scope and audit criteria.

NEW QUESTION: 38
You receive the following mail from the IT support team: Dear User,Starting next week, we will be deleting all inactive email accounts in order to create spaceshare the below details in order to continue using your account. In case of no response,
Name:
Email ID:
Password:
DOB:
Kindly contact the webmail team for any further support. Thanks for your attention.
Which of the following is the best response?
A. Ignore the email
B. Respond it by saying that one should not share the password with anyone
C. One should not respond to these mails and report such email to your supervisor
Answer: (SHOW ANSWER)
The best response to the email from the IT support team asking for personal details is to not respond to the email and report it to your supervisor. The email is likely a phishing attempt, which is a form of social engineering that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information.
The IT support team should never ask for your password or other personal details via email, as this is a violation of information security policies and best practices. Ignoring the email or responding to it by saying that one should not share the password with anyone are not sufficient responses, as they do not alert the IT support team or your supervisor about the phishing attempt, which could affect other users as well. Reporting the email to your supervisor is a responsible action that could help prevent further damage or compromise of information. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO
/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Phishing?

NEW QUESTION: 39
Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.
Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments.
Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.
During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC
27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.
Based on the scenario above, answer the following question:

Question:
According to Scenario 9, the auditor decided to conduct the extension audit during the surveillance audit.
How do you define this situation?
A. Acceptable, as extension audits are conducted during the surveillance audit
B. Unacceptable, as the auditor cannot approve the extension audit
C. Unacceptable, as extension audits are only conducted after the second year of the initial certification audit
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO/IEC 17021-1 allows extension audits to be conducted alongside surveillance audits.
* This reduces redundancy and cost while maintaining compliance.
* B. Incorrect:
* Certification bodies have the authority to approve extension audits.
* C. Incorrect:
* Extensions are not restricted to the second year-they can occur at any time during the certification cycle.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.6.5 (Extension Audits During Surveillance)

NEW QUESTION: 40
OrgXY is an ISO/IEC 27001-certified software development company. A year after being certified, OrgXY's top management informed the certification body that the company was not ready for conducting the surveillance audit. What happens in this case?
Freecram.net
A. The certification is suspended
B. The current certification is used until the next surveillance audit
C. OrgXY transfers its registration to another certification body
Answer: (SHOW ANSWER)
If an organization like OrgXY informs the certification body that it is not ready to conduct the surveillance audit as scheduled, the certification may be suspended. This is because the surveillance audit is a critical part of the ongoing certification maintenance, required to ensure continued compliance with the standard.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, general guidelines on certification and surveillance requirements

NEW QUESTION: 41
Which three of the following options are an advantage of using a sampling plan for the audit?
A. Overrules the auditor's instincts
B. Use of the plan for consecutive audits
C. Provides a suitable understanding of the ISMS
D. Implements the audit plan efficiently
E. Gives confidence in the audit results
F. Misses key issues
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, a sampling plan is a method for selecting a representative subset of the audit evidence from a defined population1. A sampling plan can have several advantages for the audit, such as providing a suitable understanding of the ISMS by covering its key processes, activities, and controls; implementing the audit plan efficiently by optimizing the use of time and resources; and giving confidence in the

audit results by ensuring that the sample is sufficient, reliable, and unbiased1. Therefore, these three options are examples of advantages of using a sampling plan for the audit. The other options are not advantages, but rather disadvantages or risks of using a sampling plan. For example, overruling the auditor's instincts may lead to missing important evidence or issues that are not covered by the sampling plan; using the same plan for consecutive audits may reduce the effectiveness and validity of the audit results; and missing key issues may result from an inadequate or inappropriate sampling plan1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 42
You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre.
Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.
Select four options for the actions you could take.
A. Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared
B. Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit
C. Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity
D. Note the progress made but hold the audit open until all corrective action has been cleared
E. Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified
F. Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity
G. Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale
H. Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1. The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1.
Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:
Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame. The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.
Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.
Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.
Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised by implementing effective corrective actions for most of them and agreeing on a plan for the remaining one. The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

NEW QUESTION: 43
Question
Which statement below best describes the relationship between information security elements?
A. Threats exploit vulnerabilities to damage or destroy assets
B. Controls protect assets by reducing threats
C. Risk is a function of vulnerabilities that harm assets

Answer: (SHOW ANSWER)

The most accurate description of the relationship between information security elements is that threats exploit vulnerabilities to damage or destroy assets. This relationship forms the foundational model used in information security risk management, including ISO/IEC 27001:2022.

In this model, assets are anything of value to the organization, such as information, systems, services, or people. Vulnerabilities are weaknesses or gaps in protection that could be exploited. Threats are potential causes of an unwanted incident, such as malicious actors, malware, system failures, or human error. A risk materializes when a threat successfully exploits a vulnerability, leading to an impact on an asset.

Option A correctly captures this causal chain and reflects the risk assessment logic required by ISO/IEC

27001 clause 6.1.2, which requires organizations to identify threats, vulnerabilities, and impacts in combination.

Option B is incorrect because controls do not reduce threats directly; they primarily reduce vulnerabilities or mitigate impacts. Threats often exist outside the organization's control. Option C is also incorrect because risk is not solely a function of vulnerabilities; it is typically a combination of threats, vulnerabilities, likelihood, and impact.

Therefore, option A best represents the correct and complete relationship among the core information security elements.

NEW QUESTION: 44

You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including misaddressed labels and, in 15% of cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).

You: Are items checked before being dispatched?

SM: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.

You: What action is taken when items are returned?

SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.

You raise a nonconformity against ISO 27001:2022 based on the lack of control of the labelling process.

At the closing meeting, the Shipping Manager issues an apology to you that his comments may have been misunderstood. He says that he did not realise that there is a background IT process that automatically checks that the right label goes onto the right parcel otherwise the parcel is ejected at labelling. He asks that you withdraw your nonconformity.

Select three options of the correct responses that you as the audit team leader would make to the request of the Shipping Manager.

A. Advise the Shipping Manager that his request will be included in the audit report

B. Advise management that the new information provided will be discussed when the auditors have more time

C. Inform the Shipping Manager that the nonconformity is minor and should be quickly corrected

D. Ask the audit team members to state what they think should happen

E. Inform him of your understanding and withdraw the nonconformity

F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed

G. Advise the Shipping Manager that the nonconformity must stand since the evidence obtained for it was dear

H. Indicate that the nonconformity is evidence of a deeper system failure that needs to be rectified

Answer: (SHOW ANSWER)

* A. Advise the Shipping Manager that his request will be included in the audit report. This is true because the audit report should document all the relevant information and evidence related to the audit, including any requests or objections raised by the auditee. The audit report should also provide the rationale for the audit conclusions and recommendations12.
* B. Advise management that the new information provided will be discussed when the auditors have more time. This is true because the auditors should not make hasty decisions based on incomplete or unverified information. The auditors should review and evaluate the new information in a systematic and objective manner, and determine whether it affects the audit findings, nonconformities, or conclusions12.
* F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed. This is true because the auditors should acknowledge and appreciate the cooperation and transparency of the auditee, but also maintain their professional integrity and independence. The auditors should not withdraw a nonconformity unless they are satisfied that it was raised in error or that it has been effectively corrected and verified12.

References :=

* ISO 19011:2022 Guidelines for auditing management systems
* ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 45
Objectives, criteria, and scope are critical features of a third-party ISMS audit. Which two issues are audit objectives?
* Evaluate customer processes and functions
A. Assess conformity with ISO/IEC 27001 requirements
B. Fulfil the audit plan
C. Confirm sites operating the ISMS
D. Determine the scope of the ISMS
E. Review organisation efficiency
Answer: (SHOW ANSWER)
Audit objectives are the specific purposes or goals that the customer or the certification body wants to achieve through the audit. They define what the audit intends to accomplish and provide the basis for planning and conducting the audit. Audit objectives may vary depending on the type, scope, and criteria of the audit, but they should be clear, measurable, and achievable.
Some examples of audit objectives for a third-party ISMS audit are:
* Assess conformity with ISO/IEC 27001 requirements: This objective means that the audit aims to verify that the organisation's ISMS meets the requirements of the ISO/IEC 27001 standard, which specifies the best practices for establishing, implementing, maintaining, and improving an information security management system. The audit will evaluate the organisation's ISMS documentation, processes, controls, and performance against the standard's clauses and annex A controls.
* Confirm sites operating the ISMS: This objective means that the audit aims to confirm that the organisation's ISMS covers all the relevant sites or locations where the organisation operates or provides its services. The audit will verify that the scope of the ISMS is accurate and consistent with the organisation's context, objectives, and risks.
The other phrases are not audit objectives, but rather:
* Evaluate customer processes and functions: This is not an audit objective, but rather a possible audit criterion or a requirement that the organisation's processes and functions should meet. The audit criterion is the reference against which the audit evidence is compared to determine conformity or nonconformity. The audit criterion may include ISO/IEC 27001 requirements, customer requirements, or other applicable standards or regulations.
* Fulfil the audit plan: This is not an audit objective, but rather a task or an activity that the auditor performs during the audit. The audit plan is a document that describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. The auditor should follow and fulfil the audit plan to ensure that the audit is conducted effectively and efficiently.
* Determine the scope of the ISMS: This is not an audit objective, but rather a prerequisite or an input for conducting the audit. The scope of the ISMS is the extent and boundaries of the information security management system within the organisation. It defines what processes, activities, locations, assets, and stakeholders are included or excluded from the ISMS. The scope of the ISMS should be determined by the organisation before applying for certification or undergoing an audit.
* Review organisation efficiency: This is not an audit objective, but rather a possible outcome or a result of conducting an audit. The organisation efficiency is a measure of how well the organisation uses its resources to achieve its goals and objectives. The audit may help review and improve the organisation efficiency by identifying strengths, weaknesses, opportunities, and threats in its information security management system.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION: 46
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits.
Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.
The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.

Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.
Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.
Based on the scenario above, answer the following question:
Based on scenario 7, what should Lawsy do prior to the initiation of stage 2 audit?
A. Perform a quality review of audit findings from stage 1 audit
B. Define which audit test plans can be combined to verify compliance
C. Review and confirm the audit plan with the certification body
Answer: C (LEAVE A REPLY)
Prior to the initiation of stage 2 audit, Lawsy should review and confirm the audit plan with the certification body. This ensures that both parties agree on the objectives, scope, and procedures for the stage 2 audit, thus aligning expectations and facilitating a smoother audit process.
References: ISO 19011:2018, Guidelines for auditing management systems

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
Question
ABC Manufacturing operates in a highly regulated chemical industry. Despite having internal control mechanisms in place, the company faces challenges due to the complexity of the sector, leading to potential defects in its ISMS.
What type of risk does this scenario represent?
A. Inherent risk
B. Control risk
C. Detection risk
Answer: (SHOW ANSWER)
The scenario represents inherent risk, making option A the correct answer. Inherent risk refers to the susceptibility of a process, system, or organization to errors or failures due to its nature, environment, or complexity, independent of the effectiveness of internal controls.
ABC Manufacturing operates in a highly regulated and complex chemical industry. Such environments naturally involve complicated regulatory requirements, hazardous materials, and stringent compliance obligations. These characteristics increase the likelihood of errors or ISMS defects simply because of the industry's complexity, even when internal controls exist. This is the defining feature of inherent risk.
Option B is incorrect because control risk relates to the possibility that internal controls fail to prevent or detect issues. In the scenario, controls are in place, but the risk arises from the complexity of the industry itself rather than a failure of controls.
Option C is incorrect because detection risk concerns the auditor's ability to detect existing issues during an audit, not the organization's operational environment.
In ISO/IEC 27001 audits, understanding inherent risk is essential for planning audit focus and depth. Highly regulated industries naturally carry higher inherent risk due to complexity and compliance demands.
Therefore, the scenario clearly represents inherent risk.

NEW QUESTION: 48

You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including mis-addressed labels and, in 15% of company cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).
You: Are items checked before being dispatched?
SH: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.
You: What action is taken when items are returned?
SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.
You raise a nonconformity. Referencing the scenario, which six of the following Appendix A controls would you expect the auditee to have implemented when you conduct the follow-up audit?
A. 5.11 Return of assets
B. 8.12 Data leakage protection
C. 5.3 Segregation of duties
D. 6.3 Information security awareness, education, and training
E. 7.10 Storage media
F. 8.3 Information access restriction
G. 5.6 Contact with special interest groups
H. 6.4 Disciplinary process
I. 7.4 Physical security monitoring
J. 5.13 Labelling of information
K. 5.32 Intellectual property rights
Answer: (SHOW ANSWER)

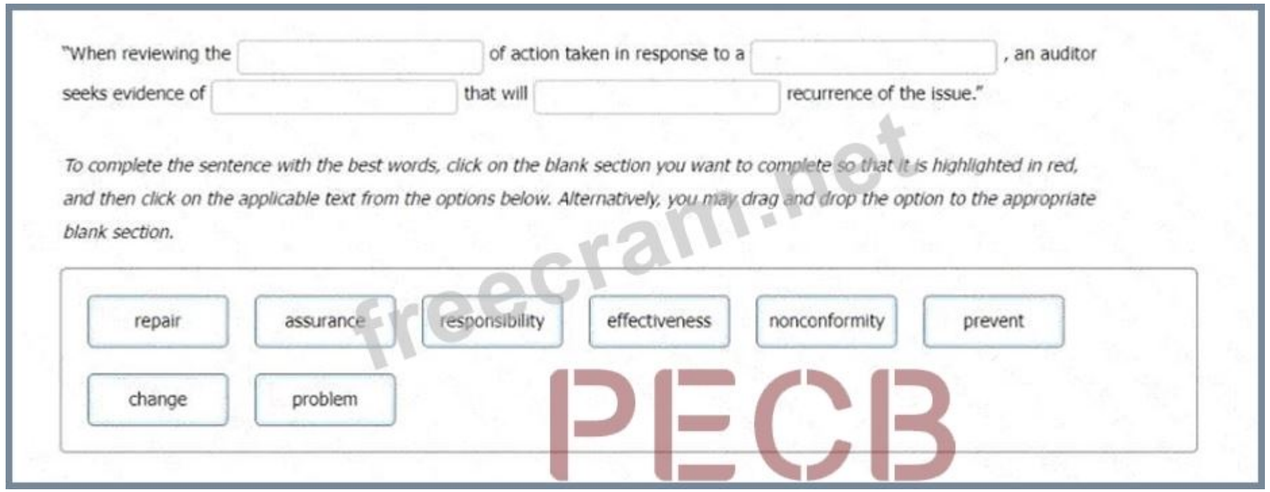
* B. 8.12 Data leakage protection. This is true because the auditee should have implemented measures to prevent unauthorized disclosure of sensitive information, such as personal data, medical records, or official documents, that are contained in the parcels. Data leakage protection could include encryption, authentication, access control, logging, and monitoring of data transfers12.
* D. 6.3 Information security awareness, education, and training. This is true because the auditee should have ensured that all employees and contractors involved in the shipping process are aware of the information security policies and procedures, and have received appropriate training on how to handle and protect the information assets in their custody. Information security awareness, education, and training could include induction programmes, periodic refreshers, awareness campaigns, e-learning modules, and feedback mechanisms13.
* E. 7.10 Storage media. This is true because the auditee should have implemented controls to protect the storage media that contain information assets from unauthorized access, misuse, theft, loss, or damage. Storage media could include paper documents, optical disks, magnetic tapes, flash drives, or hard disks14. Storage media controls could include physical locks, encryption, backup, disposal, or destruction14.
* F. 8.3 Information access restriction. This is true because the auditee should have implemented controls to restrict access to information assets based on the principle of least privilege and the need-to-know basis. Information access restriction could include identification, authentication, authorization, accountability, and auditability of users and systems that access information assets15.
* I. 7.4 Physical security monitoring. This is true because the auditee should have implemented controls to monitor the physical security of the premises where information assets are stored or processed. Physical security monitoring could include CCTV cameras, alarms, sensors, guards, or patrols16. Physical security monitoring could help detect and deter unauthorized physical access or intrusion attempts16.
* J. 5.13 Labelling of information. This is true because the auditee should have implemented controls to label information assets according to their classification level and handling instructions. Labelling of information could include markings, tags, stamps, stickers, or barcodes1 . Labelling of information could help identify and protect information assets from unauthorized disclosure or misuse1 .
References :=
* ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* ISO/IEC 27004:2022 Information technology - Security techniques - Information security management systems - Monitoring measurement analysis and evaluation
* ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management
* ISO/IEC 27006:2022 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
* [ISO/IEC 27007:2022 Information technology - Security techniques - Guidelines for information security management systems auditing]

NEW QUESTION: 49
You are performing an ISMS audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to verify the information security of the business continuity management process. During the audit, you learned that the organisation activated one of the business continuity plans (BCPs) to make sure the nursing service continued during the recent pandemic. You ask the Service Manager to explain how the organization manages information security during the business continuity management process.
The Service Manager presented the nursing service continuity plan for a pandemic and summarised the process as follows:
Stop the admission of any NEW residents.
70% of administration staff and 30% of medical staff will work from home.
Regular staff self-testing, including submitting a negative test report 1 day BEFORE they come to the office.
Install ABC's healthcare mobile app, tracking their footprint and presenting a GREEN Health Status QR-Code for checking on the spot.
You ask the Service Manager how to prevent non-relevant family members or interested parties from accessing residents' personal data when staff work from home. The Service Manager cannot answer and suggests the IT Security Manager should help with that.
You would like to further investigate other areas to collect more audit evidence. Select three options that will not be in your audit trail.
A. Collect more evidence on how information security protocols are maintained during disruption (relevant to control A.5.29)
B. Collect more evidence that staff only use IT equipment protected from malware when working from home (relevant to control A.8.7)
C. Collect more evidence by interviewing additional staff to ensure they are aware of the need to sometimes work from home (Relevant to clause 7.3)
D. Collect more evidence on how and when the Business Continuity Plan has been tested. (Relevant to control A.5.29)
E. Collect more evidence on how the organisation makes sure all staff periodically conduct a positive Covid test (Relevant to control A.7.2)
F. Collect more evidence on how the organisation manages information security on mobile devices and during teleworking (Relevant to control A.6.7)
G. Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home. (Relevant to clause 6)
H. Collect more evidence on what resources the organisation provides to support the staff working from home. (Relevant to clause 7.1)
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022 clause 6.1, the organization must establish, implement and maintain an information security risk management process that includes the following activities:
* establishing and maintaining information security risk criteria;
* ensuring that repeated information security risk assessments produce consistent, valid and comparable results;
* identifying the information security risks;
* analyzing the information security risks;
* evaluating the information security risks;
* treating the information security risks;
* accepting the information security risks and the residual information security risks;
* communicating and consulting with stakeholders throughout the process;
* monitoring and reviewing the information security risks and the risk treatment plan.
According to control A.5.29, the organization must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during a disruptive situation. The organization must also:
* determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster;
* establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation;
* verify the availability of information processing facilities.
Therefore, the following options will not be in your audit trail, as they are not relevant to the information security risk management process or the information security continuity process:
* E. Collect more evidence on how the organisation makes sure all staff periodically conduct a positive Covid test (Relevant to control A.7.2). This is not relevant to the information security aspects of business continuity management, as it is related to the health and safety of the staff, not the protection of information assets. Control A.7.2 is about screening of personnel prior to employment, not during employment.

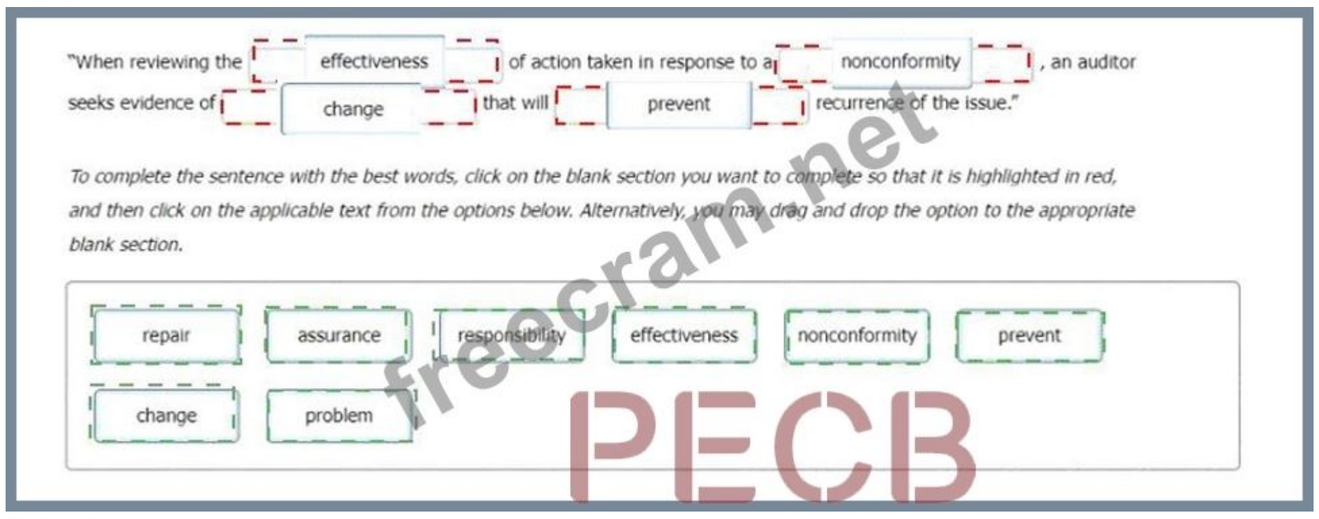
* G. Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home. (Relevant to clause 6). This is not relevant to the information security aspects of business continuity management, as it is related to the operational and financial aspects of the business, not the identification and treatment of information security risks. Clause 6 is about the information security risk management process, not the business risk management process.
* H. Collect more evidence on what resources the organisation provides to support the staff working from home. (Relevant to clause 7.1). This is not relevant to the information security aspects of business continuity management, as it is related to the general provision of resources for the ISMS, not the specific processes, procedures and controls to ensure the continuity of information security during a disruptive situation. Clause 7.1 is about determining and providing the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS, not the resources needed for the staff working from home.
References:
ISO/IEC 27001:2022, clauses 6.1, 7.1, and Annex A control A.5.29
[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 14-15, 17, 22-23 ISO 27001:2022 Annex A Control 5.29 - What's New?
ISO 22301 Business Continuity Management System

NEW QUESTION: 50
Which of the following is not a type of Information Security attack?
A. Legal Incidents
B. Vehicular Incidents
C. Technical Vulnerabilities
D. Privacy Incidents
Answer: (SHOW ANSWER)
Vehicular incidents are not a type of information security attack. A vehicular incident is an event that involves a vehicle or its driver causing damage or injury to people or property. A vehicular incident may have an impact on information security if it affects the availability or integrity of information or systems that are transported or accessed by vehicles, but it is not an intentional or malicious attack on information security.
Legal incidents are a type of information security attack that involve legal actions or disputes that may compromise the confidentiality or integrity of information or systems. Technical vulnerabilities are a type of information security attack that exploit weaknesses or flaws in software or hardware that may compromise the confidentiality, integrity, or availability of information or systems. Privacy incidents are a type of information security attack that involve unauthorized access or disclosure of personal or sensitive information that may compromise the confidentiality or integrity of information or systems. References: : CQI & IRCA ISO 27001:
2022 Lead Auditor Course Handbook, page 25. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

NEW QUESTION: 51
You are performing an ISMS audit at a European-based residential nursing home called ABC that provides healthcare services. The next step in your audit plan is to verify the effectiveness of the continual improvement process.
During the audit, you learned most of the residents' family members (90%) receive WeCare medical devices promotion advertisements through email and SMS once a week via ABC's healthcare mobile app. All of them do not agree on the use of the collected personal data for marketing or any other purposes than nursing and medical care on the signed service agreement with ABC. They have very strong reason to believe that ABC is leaking residents' and family members' personal information to a non-relevant third party and they have filed complaints.
The Service Manager says that, after investigation, all these complaints have been treated as nonconformities.
The corrective actions have been planned and implemented according to the nonconformity and corrective management procedure (Document reference ID: ISMS_L2_10.1, version 1).
You write a nonconformity which you will follow up on later. Select the words that best complete the sentence:



Answer:



Explanation:

One possible way to complete the sentence is:

"When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue." According to ISO/IEC 27001:2022, clause 10.1, the organization shall continually improve the suitability, adequacy, and effectiveness of the ISMS by evaluating the performance and the effectiveness of the ISMS, ensuring that the policy and objectives are aligned with the strategic direction of the organization, and taking actions to achieve the intended outcomes of the ISMS. One of the ways to achieve continual improvement is to identify and correct nonconformities and take actions to eliminate their causes and prevent their recurrence.

Therefore, when reviewing the effectiveness of the corrective actions, an auditor should look for evidence that the organization has analyzed the root cause of the nonconformity, implemented appropriate changes to the ISMS, and verified that the changes have resulted in the desired improvement and prevented the recurrence of the issue. References: =

* ISO/IEC 27001:2022, clause 10.1, Nonconformity and corrective action
* ISO/IEC 27001:2022, clause 10.2, Continual improvement

* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION: 52
Which of the options below is a control related to the management of personnel that aims to avoid the occurrence of incidents?
A. The organization regularly provides security awareness and training sessions for its employees
B. The organization always reviews the security policy after the integration of a new division to the organization
C. The organization conducts regular user access reviews to verify that only authorized employees have access to confidential information
Answer: (SHOW ANSWER)
Regular security awareness and training sessions for employees are a control measure aimed at preventing security incidents by ensuring that personnel are aware of information security threats and concerns, and understand their roles and responsibilities in safeguarding organizational assets. This proactive approach is designed to educate employees on the importance of security practices and to avoid the occurrence of security incidents. References: = This answer is based on the principles of personnel security management as outlined in ISO/IEC 27001, particularly in Annex A.7 which deals with human resource security before, during, and after employment, and Annex A.9 which focuses on access control and ensuring that employees have access only to the information that is necessary for their job role

NEW QUESTION: 53
Select two options that describe an advantage of using a checklist.
* Using the same checklist for every audit without review
A. Restricting interviews to nominated parties
B. Ensuring relevant audit trails are followed
C. Ensuring the audit plan is implemented
D. Reducing audit duration
E. Not varying from the checklist when necessary
Answer: (SHOW ANSWER)
A checklist is a tool that helps auditors to collect and verify information relevant to the audit objectives and scope. It can provide the following advantages:
* Ensuring relevant audit trails are followed: A checklist can help auditors to identify and trace the sources of evidence that support the conformity or nonconformity of the audited criteria. It can also help auditors to avoid missing or overlooking any important aspects of the audit.
* Ensuring the audit plan is implemented: A checklist can help auditors to follow and fulfil the audit plan, which describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. It can also help auditors to manage their time and resources effectively and efficiently.
The other options are not advantages of using a checklist, but rather:
* Using the same checklist for every audit without review: This is a disadvantage of using a checklist, as it can lead to a rigid and ineffective audit approach. A checklist should be tailored and adapted to each specific audit, taking into account the context, risks, and changes of the auditee and the audit criteria. A checklist should also be reviewed and updated periodically to ensure its validity and relevance.
* Restricting interviews to nominated parties: This is a disadvantage of using a checklist, as it can limit the scope and depth of the audit. A checklist should not prevent auditors from interviewing other relevant parties or sources of information that may provide valuable evidence or insights for the audit.
A checklist should be used as a guide, not as a constraint.
* Reducing audit duration: This is not necessarily an advantage of using a checklist, as it depends on various factors, such as the complexity, size, and maturity of the auditee's ISMS, the availability and quality of evidence, the competence and experience of the auditors, and the level of cooperation and communication between the auditors and the auditee. A checklist may help reduce audit duration by improving efficiency and organization, but it may also increase audit duration by requiring more evidence or verification.
* Not varying from the checklist when necessary: This is a disadvantage of using a checklist, as it can result in a superficial or incomplete audit. A checklist should not prevent auditors from exploring or investigating any issues or concerns that arise during the audit, even if they are not included in the checklist. A checklist should be used as a support, not as a substitute.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 6.2.2]

NEW QUESTION: 54
Scenario 3: Rebuildy is a construction company located in Bangkok.. Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.
The ISMS implementation outcomes are presented below
*Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.
*Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.
*All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.
*The information security policy is part of a security manual drafted based on best security practices Therefore, it is not a stand-alone document.
*Information security roles and responsibilities have been clearly stated in every employees job description
*Management reviews of the ISMS are conducted at planned intervals.
Rebuildy applied for certification after two midterm management reviews and one annual internal audit Before the certification audit one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.
At the beginning of the audit, the audit team interviewed the company's top management They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001 The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:
*An instance of improper user access control settings was detected within the company's financial reporting system.
*A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.
After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.
Based on the scenario above, answer the following question:
Question:
Based on the last paragraph of Scenario 3, what did the audit team leader commit?
A. Ordinary negligence
B. Gross negligence
C. Fraud
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Fraud (Correct Answer):
* The audit team leader knowingly falsified the audit report to downplay nonconformities.
* Fraud involves intentional deception or misrepresentation of information, making this a fraudulent act.
* A. Ordinary negligence (Incorrect):
* Ordinary negligence is a failure to exercise reasonable care, but this case involved intentional misconduct.
* B. Gross negligence (Incorrect):
* Gross negligence is extreme carelessness but does not involve deliberate misrepresentation.
Relevant Standard Reference:
* ISO 19011:2018 Clause 4 (Principles of Auditing: Integrity and Objectivity)

NEW QUESTION: 55
The purpose of a management system audit is to? Select 1
A. Evaluate the performance of an organisation's management system
B. Improve the performance of an organisation's management system
C. Manage the performance of an organisation's management system
D. Research the performance of an organisation's management system
Answer: (SHOW ANSWER)
A management system audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit criteria are a set of requirements that may include policies, procedures, standards, regulations, etc. The purpose of a management system audit is to evaluate the performance of an organisation's management system in terms of its effectiveness, efficiency, compliance, and improvement. A management system audit can also identify strengths, weaknesses, opportunities, and risks of the management system and provide recommendations for improvement.

NEW QUESTION: 56
Auditor competence is a combination of knowledge and skills. Which two of the following activities are predominately related to "knowledge"?
A. Understanding how to identify findings
B. Designing a checklist
C. Follow an audit trail deviating from the prepared checklist
D. Communicate with the auditee
E. Determining how to seek evidence from the auditee
F. Determining what evidence to gather
Answer: B,F (LEAVE A REPLY)
Knowledge is the understanding of facts, concepts, principles, theories and practices related to a specific subject or discipline. Skills are the ability to apply knowledge and use know-how to complete tasks and solve problems. According to ISO 19011:2018, the knowledge and skills of an auditor include the following:
* Knowledge of audit principles, procedures and methods
* Knowledge of management system standards and reference documents
* Knowledge of the organization's context, scope, processes and objectives
* Knowledge of relevant legal, regulatory and contractual requirements
* Knowledge of applicable industry, sector or technical disciplines
* Knowledge of risk management and risk-based thinking
* Skill in collecting and verifying information
* Skill in evaluating conformity and effectiveness of management systems
* Skill in reporting and communicating audit results
* Skill in managing audit activities and teams
Based on this, the activities that are predominately related to knowledge are designing a checklist and determining what evidence to gather, as they require the auditor to understand the audit criteria, scope, objectives and methods, as well as the organization's context, processes and risks. The other activities are more related to skills, as they involve applying knowledge and using know-how to perform tasks and solve problems during the audit.
References:
ISO 19011:2018, Guidelines for auditing management systems, clauses 7.2.1, 7.2.2 and 7.2.3 PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 9-10 and 16-17 ISO 9001 Auditing Practices Group Guidance on: Auditing Competence, pages 2-3 and 8

NEW QUESTION: 57

During discussions with the individual(s) managing the audit programme of a certification body, the Management System Representative of the client organisation asks for a specific auditor for the certification audit. Select two of the following options for how the individual(s) managing the audit programme should respond.

A. Advise the Management System Representative that his request can be accepted

B. Suggest that the Management System Representative chooses another certification body

C. State that his request will be considered but may not be taken up

D. Suggest asking the certification body management to permit the request

E. Advise the Management System Representative that the audit team selection is a decision that the audit programme manager needs to make based on the resources available

Answer: (SHOW ANSWER)

According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, a certification body should ensure that its auditors are competent, impartial, and independent from the auditee organization2. Therefore, if a Management System Representative of a client organization asks for a specific auditor for the certification audit, the individual(s) managing the audit programme should respond in a way that does not compromise these principles or create any conflict of interest or undue influence2. Two possible ways to respond are to state that his request will be considered but may not be taken up, as there may be other factors that affect the auditor selection process; or to advise him that the audit team selection is a decision that the audit programme manager needs to make based on the resources available, such as auditor availability, competence, location, etc2. The other options are not suitable ways to respond in this situation. For example, advising him that his request can be accepted may raise doubts about the objectivity and credibility of the auditor and the certification body; suggesting that he chooses another certification body may imply that his request is unreasonable or unethical; and suggesting asking the certification body management to permit his request may suggest that there is room for negotiation or manipulation in auditor selection2. References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 58

You are performing an ISMS audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to verify the information security incident management process. The IT Security Manager presents the information security incident management procedure (Document reference ID: ISMS_L2_16, version 4) and explains that the process is based on ISO/IEC 27035-1:2016.

You review the document and notice a statement "any information security weakness, event, and incident should be reported to the Point of Contact (PoC) within 1 hour after identification". When interviewing staff, you found that there were differences in the understanding of the meaning of "weakness, event, and incident".

The IT Security Manager explained that an online "information security handling" training seminar was conducted 6 months ago. All of the interviewed persons participated in and passed the reporting exercise and course assessment.

You are preparing the audit findings. Select two options that are correct.

A. There is a nonconformity (NC). The information security incident training has failed. This is not conforming with clause 7.2 and control A.6.3.

B. There is a nonconformity (NC). The terminology of the the incident management reporting process is unclear as evidenced by staff misunderstanding of the meaning of "weakness, event and incident". This is not conforming with clause 9.1 and control A.5.24.

C. There is an opportunity for improvement (OFI). The information security incident training effectiveness can be improved. This is relevant to clause 7.2 and control A.6.3.

D. There is an opportunity for improvement (OFI). The information security weaknesses, events, and incidents are reported. This is relevant to clause 9.1 and control A.5.24.

E. There is no nonconformance. The information security handling training has been effective. This conforms with clause 7.2 and control A.6.3.

F. There is no nonconformance. The information security weaknesses, events, and incidents are reported. This conforms with clause 9.1 and control A.5.24.

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022 clause 7.2, the organization must ensure that the persons doing work under its control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. The organization must also provide information security awareness education and training to its personnel and relevant interested parties. According to control A.6.3, the organization must ensure that all employees and contractors are made aware of the information security incident management procedures and their expected roles and responsibilities. Therefore, an opportunity for improvement (OFI) can be identified if the information security incident training effectiveness can be improved, as evidenced by the differences in the understanding of the meaning of "weakness, event, and incident" among the staff.

According to ISO/IEC 27001:2022 clause 9.1, the organization must monitor, measure, analyze and evaluate the information security performance and the effectiveness of the ISMS. The organization must also retain appropriate documented information as evidence of the monitoring and measurement results. According to control A.5.24, the organization must establish and maintain an information security incident management process that includes the following activities:

*reporting information security events and weaknesses;

*assessing and deciding on information security events;

*responding to information security incidents;

*learning from information security incidents;

*collecting evidence and disclosing information.
Therefore, a nonconformity (NC) can be identified if the terminology of the incident management reporting process is unclear, as evidenced by the staff misunderstanding of the meaning of "weakness, event, and incident". This could lead to inconsistent or inaccurate reporting, assessment, response, learning, and disclosure of information security incidents, which could affect the information security performance and the effectiveness of the ISMS.
References:
*ISO/IEC 27001:2022, clauses 7.2, 9.1, and Annex A controls A.5.24 and A.6.3
*[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 15-16, 18-19, 22-23
*ISO/IEC 27035-1:2016, clauses 4, 5, 6, 7, and 8
*ISO 27001 - Annex A.16: Information Security Incident Management
*ISO 27001:2022 Annex A Control 5.24 - What's New?

NEW QUESTION: 59
You are carrying out your first third-party ISMS surveillance audit as an audit team leader. You are presently in the auditee's data centre with another member of your audit team and the organisation's guide.
You request access to a locked room protected by a combination lock and iris scanner. In the corner of the room is a collection of hard drives piled on a desk. You ask the guide what the status of the drives is. He tells you the drives are redundant and awaiting disposal. They should have been picked up last week, but the organisation's external provider of secure destruction services was unable to source a driver due to staff sickness. He says this has recently become more common though he does not know why. He then presents you with a job ticket that confirms the pickup has been rescheduled for tomorrow.
Based on the scenario above which three of the following actions would you now take?
A. Ensure that the organisation's arrangements for the secure disposal and reuse of equipment have been adhered to.
B. Ensure that the organisation's arrangements for the life cycle management of storage media have been adhered to.
C. Raise a nonconformity against control A.7.5, 'protecting against physical and environmental threats' because the drives have been left exposed on the desktop.
D. Record a nonconformity against control A.5.13 'labelling of information' as the disk drives' status was unclear
E. Record the finding but note no further action is required as the pickup has now been rescheduled.
F. Record an opportunity for improvement in respect of the external provider's inventory management arrangements.
G. Follow an audit trail to determine whether the organisation is complying with its obligations in respect of control A.5.22 'monitoring, review and change management of supplier services'.
H. Raise a nonconformity against control A.7.7, 'clear desk and clear screen' because the drives have been left unprotected on the desktop.
Answer: (SHOW ANSWER)

NEW QUESTION: 60

Scenario 4: Branding is a marketing company that works with some of the most famous companies in the US.

To reduce internal costs. Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology. equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.

During the last audit. Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence based approach, particularly in light of two information security incidents reported by Techvology in the past year The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed upon standards The auditors also verified whether Techvology complied with the contractual requirements established between the two entities This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to. Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.

The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.

Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.

Based on the scenario above, answer the following question:

Question:

According to Scenario 4, what type of audit evidence did the auditors collect to determine the source of the information security incidents?

A. Verbal and documentary evidence

B. Confirmative and technical evidence

C. Analytical and mathematical evidence

Answer: (SHOW ANSWER)

Comprehensive and Detailed In-Depth Explanation:

* A. Correct Answer:

* Auditors conducted interviews (verbal evidence) and analyzed incident resolution records, employee training logs, and governance policies (documentary evidence).

* ISO 19011:2018 (Clause 6.4.7) states that audit evidence can be verbal, documented, observed, or analytical.

pass4cram.net

* B. Incorrect:
* Confirmative evidence involves third-party validation, which was not explicitly mentioned.
* C. Incorrect:
* Mathematical analysis was not conducted in this audit.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.7 (Audit Evidence Collection Methods)

NEW QUESTION: 61
Scenario 6: Sinvestment is an insurance company that offers home, commercial, and life insurance. The company was founded in North Carolina, but have recently expanded in other locations, including Europe and Africa.
Sinvestment is committed to complying with laws and regulations applicable to their industry and preventing any information security incident. They have implemented an ISMS based on ISO/IEC 27001 and have applied for ISO/IEC 27001 certification.
Two auditors were assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment. they started the audit activities. First, they reviewed the documentation required by the standard, including the declaration of the ISMS scope, information security policies, and internal audits reports. The review process was not easy because, although Sinvestment stated that they had a documentation procedure in place, not all documents had the same format.
Then, the audit team conducted several interviews with Sinvestment's top management to understand their role in the ISMS implementation. All activities of the stage 1 audit were performed remotely, except the review of documented information, which took place on-site, as requested by Sinvestment.
During this stage, the auditors found out that there was no documentation related to information security training and awareness program. When asked, Sinvestment's representatives stated that the company has provided information security training sessions to all employees. Stage 1 audit gave the audit team a general understanding of Sinvestment's operations and ISMS.
The stage 2 audit was conducted three weeks after stage 1 audit. The audit team observed that the marketing department (which was not included in the audit scope) had no procedures in place to control employees' access rights. Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the information security policy of the company, the issue was included in the audit report. In addition, during stage 2 audit, the audit team observed that Sinvestment did not record logs of user activities.
The procedures of the company stated that "Logs recording user activities should be retained and regularly reviewed," yet the company did not present any evidence of the implementation of such procedure.
During all audit activities, the auditors used observation, interviews, documented information review, analysis, and technical verification to collect information and evidence. All the audit findings during stages 1 and 2 were analyzed and the audit team decided to issue a positive recommendation for certification.
Based on the scenario above, answer the following question:
The audit team reviewed Sinvestment's documented information on-site, as requested by the company. Is this acceptable?
A. Yes, Sinvestment has the right to require that no document is carried off-site during the documented information review
B. No, Sinvestment cannot decide where the documentation review take place, since a confidentiality agreement was signed prior to stage 1 audit
C. No, the combination of on-site and off-site activities can impact the audit negatively
Answer: (SHOW ANSWER)
Yes, it is acceptable for Sinvestment to request that the review of documented information occur on-site. The company has the right to stipulate that no documents be carried off-site, especially to maintain control over sensitive information and ensure confidentiality, which aligns with the security controls expected in ISO/IEC
27001.
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
Select the words that best complete the sentence to describe an audit finding.

Select the words that best complete the sentence to describe an audit finding.

"An audit finding is the result of the [ ] of the collected audit [ ] against audit [ ]."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

statement	objectives	conclusions	responses	gathering	recommendations	criteria	evidence	evaluation

Answer:

Select the words that best complete the sentence to describe an audit finding.

"An audit finding is the result of the [evaluation] of the collected audit [evidence] against audit [criteria]."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

statement	objectives	conclusions	responses	gathering	recommendations	criteria	evidence	evaluation

Explanation:
"An audit finding is the result of the evaluation of the collected audit evidence against audit criteria." The words that best complete the sentence to describe an audit finding are evaluation and evidence. According to ISO 19011:2022, an audit finding is the result of the evaluation of the collected audit evidence against audit criteria12. The other options are either not related to the definition of an audit finding or do not fit the sentence grammatically. References: 1: ISO 19011:2022, Guidelines for auditing management systems, Clause 3.11 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 63
The auditor discovered that two out of 15 employees of the IT Department have not received adequate information security training. What does this represent?
A. Audit finding

B. Audit evidence
C. Information source
Answer: (SHOW ANSWER)
This scenario represents an "audit finding." An audit finding refers to results that indicate a deviation from the expected performance or standards. Discovering that two employees have not received the required training is an audit finding indicating noncompliance with the organization's training requirements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 64
You are an ISMS audit team leader assigned by your certification body to carry out a follow-up audit of a Data Centre client.
According to ISO 19011:2018, the purpose of a follow-up audit is to verify which one of the following?
A. The effectiveness of the management system
B. Implementation of ISMS objectives
C. Implementation of risk treatment plans
D. Completion and effectiveness of corrective actions
Answer: (SHOW ANSWER)
The purpose of a follow-up audit is to verify the completion and effectiveness of corrective actions taken by the auditee in response to the nonconformities identified in a previous audit1. A follow-up audit is a type of audit that is conducted after an initial audit, and it focuses on the specific areas where nonconformities were found and corrective actions were agreed upon2. A follow-up audit can be conducted as a separate audit or as part of a scheduled audit, depending on the nature and severity of the nonconformities and the audit programme objectives3.
The other options are not the purpose of a follow-up audit, but rather the purpose of other types of audits. For example:
*Option A is the purpose of a performance audit, which is a type of audit that evaluates the effectiveness of the management system in achieving its intended results4.
*Option B is the purpose of a compliance audit, which is a type of audit that verifies the conformity of the management system with the specified requirements, such as the ISMS objectives5.
*Option C is the purpose of a process audit, which is a type of audit that examines the inputs, activities, outputs, and interactions of a specific process within the management system, such as the risk treatment process.
References:
1: ISO 19011:2018, 6.7;
2: ISO 19011:2018, 3.7;
3: ISO 19011:2018, 5.5.2;
4: ISO 19011:2018,3.6;
5: ISO 19011:2018, 3.5;
6: ISO 19011:2018, 3.4;
7: ISO 19011:2018;
8: ISO 19011:2018;
9: ISO 19011:2018;
10: ISO 19011:2018;
11: ISO 19011:2018;
12: [ISO 19011:2018]

NEW QUESTION: 65
Question
A certification body decided to conduct an on-site evaluation of one of its auditors while they perform an ISO
/IEC 27001 certification audit for a client.
Is this permitted?

A. Yes, but the certification body must minimize disturbance to the normal processes of certification.
B. Yes, but the client must temporarily suspend business operations until the on-site evaluation is completed.
C. No, the evaluation must be conducted remotely to prevent disturbance to the normal processes of certification.
Answer: (SHOW ANSWER)
This activity is permitted, provided that the certification body minimizes disturbance to the certification process, making option A the correct answer. ISO/IEC 17021-1, which governs certification bodies providing management system certification, explicitly allows certification bodies to evaluate the competence and performance of their auditors. This includes on-site witnessing of auditors during actual certification audits.
The purpose of such evaluations is to ensure auditor competence, consistency, and adherence to certification procedures. ISO/IEC 17021-1 requires certification bodies to maintain confidence in their certification activities by monitoring and evaluating auditors in real audit situations. Conducting these evaluations on-site is a common and accepted practice, especially for initial competence assessments or periodic performance reviews.
However, the certification body must ensure that the evaluation does not interfere with the audit objectives or disrupt the client's operations. Option B is incorrect because there is no requirement or justification for suspending the client's business activities. Certification audits are designed to be conducted alongside normal operations whenever possible. Option C is incorrect because while remote evaluations may be used in some circumstances, the standard does not prohibit on-site evaluations.
Therefore, an on-site evaluation of an auditor during a certification audit is permitted, provided that it is carefully managed and does not disrupt the certification process or the auditee's normal operations.

NEW QUESTION: 66

Select the words that best complete the sentence to describe an audit finding.

"An audit finding is the result of the [ ] of the collected audit [ ] against audit [ ]."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

statement	evaluation	objectives	responses	evidence	conclusions	criteria	gathering	recommendations

Answer:

Select the words that best complete the sentence to describe an audit finding.

"An audit finding is the result of the [evaluation] of the collected audit [evidence] against audit [criteria]."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

statement	evaluation	objectives	responses	evidence	conclusions	criteria	gathering	recommendations

Explanation:
An audit finding is the result of the evaluation of the collected audit evidence against audit criteria.

NEW QUESTION: 67
Scenario 3: Rebuildy is a construction company located in Bangkok.. Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.
The ISMS implementation outcomes are presented below
*Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.
*Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.
*All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.
*The information security policy is part of a security manual drafted based on best security practices Therefore, it is not a stand-alone document.
*Information security roles and responsibilities have been clearly stated in every employees job description
*Management reviews of the ISMS are conducted at planned intervals.
Rebuildy applied for certification after two midterm management reviews and one annual internal audit Before the certification audit one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.
At the beginning of the audit, the audit team interviewed the company's top management They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001 The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report.
Among others, the following nonconformities were detected:
*An instance of improper user access control settings was detected within the company's financial reporting system.
*A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.
After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.
Based on the scenario above, answer the following question:

Question:
Which action described in Scenario 3 indicates that the audit team leader violated the independence principle?
A. The audit team leader sent a favorable report after discussing the audit conclusions with the top management
B. The audit team included the former employee's evidence in the audit report without revealing the source
C. The audit team leader revealed confidential information about Rebuildy to the former employee
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Independence is compromised when an auditor alters audit findings under pressure.
* The audit team leader misrepresented compliance, violating ISO 19011's principles of objectivity and integrity.
* B. Incorrect:
* Including anonymous evidence in an audit report is acceptable as long as it is verified.
* C. Incorrect:
* While revealing confidential information would be unethical, it was not mentioned in the scenario.
Relevant Standard Reference:
* ISO 19011:2018 Clause 4 (Principles of Auditing: Independence and Objectivity)

NEW QUESTION: 68
Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.
Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.
To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:
*How are responsibilities for IT and IT controls defined and assigned?
*How does Data Grid Inc. assess whether the controls have achieved the desired results?
*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?
*Are firewall-related controls implemented?
Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.
The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.
Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.
Based on this scenario, answer the following question:
What would prevent the misunderstanding between the certification body and the Data Grid Inc.?
Refer to scenario 5.
A. Validating the audit offer
B. Signing the certification agreement
C. Defining the audit schedule

Answer: (SHOW ANSWER)
Signing the certification agreement, which should clearly outline the audit objectives, scope, and responsibilities, would help prevent misunderstandings between the certification body and Data Grid Inc. A well-defined agreement ensures both parties have a clear understanding of what the audit will entail and what outputs are expected.
References: ISO/IEC 27006:2015, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

NEW QUESTION: 69
You are performing an ISMS audit at a residential nursing home that provides healthcare services.
The next step in your audit plan is to verify the information security incident management process.
The IT Security Manager presents the information security incident management procedure (Document reference ID:ISMS_L2_16, version 4).
You review the document and notice a statement "Any information security weakness, event, and incident should be reported to the Point of Contact (PoC) within 1 hour after identification". When interviewing staff, you found that there were differences in the understanding of the meaning of the phrase "weakness, event, and incident".
The IT Security Manager explained that an online "information security handling" training seminar was conducted 6 months ago. All the people interviewed participated in and passed the reporting exercise and course assessment.
You would like to investigate other areas further to collect more audit evidence. Select three options that would not be valid audit trails.
A. Collect more evidence on how areas subject to information security incidents are quarantined to maintain information security during disruption (relevant to control A.5.29)
B. Collect more evidence on how information security incidents are reported via appropriate channels (relevant to control A.6.8)
C. Collect more evidence on how the organisation conducts information security incident training and evaluates its effectiveness. (Relevant to clause 7.2)
D. Collect more evidence on how the organisation learns from information security incidents and makes improvements. (Relevant to control A.5.27)
E. Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
F. Collect more evidence on how the organisation tests the business continuity plan. (Relevant to control A.5.30)
G. Collect more evidence on whether terms and definitions are contained in the information security policy. (Relevant to control 5.32)
H. Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria. (Relevant to clause 8.13)
Answer: (SHOW ANSWER)
The three options that would not be valid audit trails are:
*Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
*Collect more evidence on whether terms and definitions are contained in the information security policy.
(Relevant to control 5.32)
*Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria. (Relevant to clause 8.13) These options are not valid audit trails because they are not directly related to the information security incident management process, which is the focus of the audit. The audit trails should be relevant to the objectives, scope, and criteria of the audit, and should provide sufficient and reliable evidence to support the audit findings and conclusions1.
Option E is not valid because the PoC is not a part of the information security incident management process, but rather a role that is responsible for reporting and escalating information security incidents to the appropriate authorities2. The audit trail should focus on how the PoC performs this function, not how the organisation manages the PoC.
Option G is not valid because the terms and definitions are not a part of the information security incident management process, but rather a part of the information security policy, which is a high-level document that defines the organisation's information security objectives, principles, and responsibilities3. The audit trail should focus on how the information security policy is communicated, implemented, and reviewed, not whether it contains terms and definitions.
Option H is not valid because ISO 27035 is not a part of the information security incident management process, but rather a guidance document that provides best practices for managing information security incidents4. The audit trail should focus on how the organisation follows the requirements of ISO/IEC 27001:
2022 for information security incident management, not whether it uses ISO 27035 as an internal audit criteria.
The other options are valid audit trails because they are related to the information security incident management process, and they can provide useful evidence to evaluate the conformity and effectiveness of the process. For example:
*Option A is valid because it relates to control A.5.29, which requires the organisation to establish procedures to isolate and quarantine areas subject to information security incidents, in order to prevent further damage and preserve evidence5. The audit trail should collect evidence on how the organisation implements and tests these procedures, and how they ensure the continuity of information security during disruption.
*Option B is valid because it relates to control A.6.8, which requires the organisation to establish mechanisms for reporting information security events and weaknesses, and to ensure that they are communicated in a timely manner to the appropriate levels within the organisation6. The audit trail should collect evidence on how the organisation defines and uses these mechanisms, and how they monitor and review the reporting process.

*Option C is valid because it relates to clause 7.2, which requires the organisation to provide information security awareness, education, and training to all persons under its control, and to evaluate the effectiveness of these activities7. The audit trail should collect evidence on how the organisation identifies the information security training needs, how they deliver and record the training, and how they measure the learning outcomes and feedback.
*Option D is valid because it relates to control A.5.27, which requires the organisation to learn from information security incidents and to implement corrective actions to prevent recurrence or reduce impact8.
The audit trail should collect evidence on how the organisation analyses and documents the root causes and consequences of information security incidents, how they identify and implement corrective actions, and how they verify the effectiveness of these actions.
*Option F is valid because it relates to control A.5.30, which requires the organisation to establish and maintain a business continuity plan to ensure the availability of information and information processing facilities in the event of a severe information security incident9. The audit trail should collect evidence on how the organisation develops and updates the business continuity plan, how they test and review the plan, and how they communicate and train the relevant personnel on the plan.
References:
1: ISO 19011:2018, 6.2;
2: ISO/IEC 27001:2022, A.6.8.1;
3: ISO/IEC 27001:2022, 5.2;
4: ISO/IEC 27035:2016, Introduction;
5: ISO/IEC 27001:2022, A.5.29;
6: ISO/IEC 27001:2022, A.6.8;
7: ISO/IEC 27001:2022, 7.2;
8: ISO/IEC 27001:2022, A.5.27;
9: ISO/IEC 27001:2022, A.5.30;
10: ISO 19011:2018;
11: ISO/IEC 27001:2022;
12: ISO/IEC 27001:2022;
13: ISO/IEC 27035:2016;
14: ISO/IEC 27001:2022;
15: ISO/IEC 27001:2022;
16: ISO/IEC 27001:2022;
17: ISO/IEC 27001:2022;
18: ISO/IEC 27001:2022

NEW QUESTION: 70
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.
The next step in your audit plan is to verify the information security on ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organization outsourced the mobile app development to a professional software development company with CMMI Level 5, ITSM (ISO
/IEC
20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified. The IT Manager presented the software security management procedure and summarised the process as follows:
The mobile app development shall adopt "security-by-design" and "security-by-default" principles, as a minimum. The following security functions for personal data protection shall be available:
Access control.
Personal data encryption, i.e., Advanced Encryption Standard (AES) algorithm, key lengths: 256 bits; and Personal data pseudonymization.
Vulnerability checked and no security backdoor
You sample the latest Mobile App Test report - details as follows:

arget of Test: ABC's healthcare mobile app, ersion 1	Test results	Test summary
ecurity test		
ersonal data encryption	Fail	Not able to perform the encryption.
ersonal data pseudonymisation	Fail	Not able to perform the pseudonymisation.
inal approval:		
		signed by
ervice Manager		

freecram.net
PECB

You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymization tests failed. Also, whether the Service Manager is authorized to approve the test.
The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymization functions failed is that these functions heavily slowed down the system and service performance. An extra
150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You sample one of the medical staff's mobile and found that ABC's healthcare mobile app, version
1.01 is installed. You found that version 1.01 has no test record.
The IT Manager explains that because of frequent ransomware attacks, the outsourced mobile app development company gave a free minor update on the tested software, performed an emergency release of the updated software, and gave a verbal guarantee that there will be no impact on any security functions. Based on his 20 years of information security experience, there is no need to re- test.
You are preparing the audit findings Select two options that are correct.
A. There is a nonconformity (NC). The IT. Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
B. There is a nonconformity (NC). The organisation does not control planned changes and review the consequences of unintended changes. (Relevant to clause 8.1)
C. There is an opportunity for improvement (OI). The IT Manager should make the decision to continue the service based on appropriate testing. (Relevant to clause 8.1, control A.8.30)
D. There is an opportunity for improvement (OI). The organisation selects an external service provider based on the extent of free services it will provide. (Relevant to clause 8.1, control A.5.21)
E. There is NO nonconformity (NC). The IT Manager demonstrates good leadership. (Relevant to clause
5.1, control 5.4)
F. There is NO nonconformity (NC). The IT Manager demonstrates he is fully competent. (Relevant to clause 7.2)
Answer: (SHOW ANSWER)
According to ISO/IEC 27001, organizations must control planned changes and review the consequences of unintended changes in order to ensure continued alignment with information security requirements. In this scenario, the organization failed to perform appropriate testing after an emergency update to the mobile app, which constitutes a nonconformity with clause 8.1 of the standard.
References:
- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor
ISO/IEC 27001 requires that organizations adhere to their established procedures for software security management. The IT Manager's approval of the app despite failed security tests and lack of proper documentation for the new version indicates noncompliance with the procedure, thus reflecting a nonconformity.
References:
- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor

NEW QUESTION: 71

Scenario 3
NightCore, a multinational technology enterprise headquartered in the United States, specializes in e- commerce, cloud computing, digital streaming, and artificial intelligence (AI). After having an information security management system (ISMS) implemented for over a year, NightCore contracted a certification body to perform an audit for ISO/IEC 27001 certification.
The certification body formed a team of five auditors, with Jack as a team leader. Jack is renowned for his extensive auditing experience in risk management, information security controls, and incident management.
His skill set aligns well with the requirements of auditing principles and processes, enabling him to effectively comprehend the audit scope and apply relevant criteria effectively. Jack also demonstrates a solid understanding of NightCore's organizational structure, purpose, and management practices and the statutory and regulatory requirements applicable to its activities.
The audit carried out by the audit team followed a rational method to reach reliable and reproducible conclusions systematically. The audit team recognized that only information capable of being verified to some extent should be considered valid evidence. In some rare instances during the audit where the verification of certain information posed challenges and where its degree of verifiability was low, the auditors exercised their professional judgment to assess the reliability and determine the level of reliance that could be placed on such evidence.
During the audit, the auditors documented their observations and inspection notes regarding the operational planning and control of NightCore's ISMS operations. They also recorded observations of NightCore's inventory of information and associated assets. Additionally, the auditors reviewed the configuration of firewalls implemented to secure connections to network services.
As the audit approached its final stages, NightCore's commitment to upholding the highest levels of information security became evident. With ISO/IEC 27001 certification within reach, NightCore is well- positioned to achieve ISO/IEC 27001 certification, enhancing its reputation in the technology sector.
Question
According to Scenario 3, did the auditors appropriately handle information that could only be verified to some extent?
A. Yes, as they utilized their professional judgment to evaluate the extent to which it could be relied upon.
B. No, as the auditors should have dismissed any information that could not be fully verified.
C. No, the auditors should have contacted external experts for verification.
Answer: (SHOW ANSWER)
The auditors handled partially verifiable information appropriately by applying professional judgment, which makes option A the correct answer. ISO 19011:2018 emphasizes that auditing is not a purely mechanical process and requires auditors to apply due professional care when evaluating evidence. Audit evidence is often based on samples and may vary in its degree of verifiability. The key requirement is that auditors assess the reliability, relevance, and sufficiency of the evidence before using it to support audit conclusions.
In the scenario, the audit team explicitly recognized that some information could only be verified to a limited extent and responded by carefully evaluating how much reliance could be placed on that information. This aligns with ISO 19011 principles, particularly the evidence-based approach and due professional care.
Auditors are expected to exercise judgment when full verification is impractical, provided they clearly understand the limitations of the evidence and do not overstate its reliability.
Option B is incorrect because ISO standards do not require auditors to discard all partially verifiable information. Doing so could lead to incomplete audit conclusions and an unrealistic audit process. Option C is also incorrect because while external experts may be used in certain specialized cases, ISO 19011 does not mandate their involvement whenever evidence is difficult to verify. The auditors' approach in the scenario demonstrates appropriate competence and professional judgment, consistent with ISO auditing guidance.

NEW QUESTION: 72
After conducting an external audit, the auditor decided that the internal auditor would follow-up on the implementation of corrective actions until the next surveillance audit. Is this acceptable?
A. No, only the external auditor should follow up on the implementation of corrective actions after the completion of the audit
B. Yes, the internal auditor may verify the implementation of corrective actions if it cannot be done by the external auditor
C. Yes, the internal auditor may follow-up on the implementation of corrective actions until a verification from the external auditor during the surveillance audit
Answer: (SHOW ANSWER)
Yes, it is acceptable for the internal auditor to follow-up on the implementation of corrective actions until verified by the external auditor during the next surveillance audit. This practice supports continuous improvement and ensures that corrective actions are effectively implemented and maintained over time.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, Clause 9.2 (Internal audit)

NEW QUESTION: 73
Scenario 7

Lawsy is a leading law firm with offices in Bangkok, Thailand. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services.
They believe they have a comfortable position in the market thanks to their commitment to implementing information security best practices and remaining up to date with technological developments.
Lawsy has rigorously implemented, evaluated, and conducted internal audits for the information security management system (ISMS) for two years. Now, they have applied for ISO/IEC 27001 certification at ISMA, a well-known and trusted certification body.
During the stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation phase. They also reviewed and evaluated the records from management reviews and internal audits. Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing insight into the internal audit plan and procedures.
The audit team continued verifying strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing the governance framework and the procedures. Following the completion of stage 1, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During the stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.
Later, the audit team found that Lawsy did not have procedures for using laptops outside the workplace, even though employees were allowed to take laptops outside the workplace. The company only provided general information about the use of laptops and relied on employees' common knowledge to protect the confidentiality and integrity of information stored on the laptops.
Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets the requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, the auditor photocopied and archived the examined employee training records after completing the audit.
Question
During the audit, the team reviewed a sample of training records from 15 out of 50 employees. What does this situation represent? Refer to the scenario.
A. Risk related to auditor
B. Sampling error
C. Inherent risk
Answer: (SHOW ANSWER)
This situation represents a sampling error, making option B the correct answer. ISO 19011:2018 explicitly states that management system audits are conducted using sampling techniques because it is impractical to examine all available information within the constraints of time and resources. When auditors select a subset of records, there is an inherent risk that the sample may not fully represent the entire population.
In this scenario, the audit team reviewed training records for 15 out of 50 employees to assess conformity with ISO/IEC 27001 training and awareness requirements. While this is an acceptable and standard audit practice, it introduces the possibility that the selected sample may not reflect gaps or issues present in the remaining records. This uncertainty is known as sampling risk or sampling error.
Option A is incorrect because a "risk related to the auditor" generally refers to competence, impartiality, or ethical behavior issues, none of which are indicated here. The auditors followed a recognized audit method.
Option C is incorrect because inherent risk relates to the nature of the organization or its environment, not to the audit technique used.
Sampling error does not imply that the audit conclusion is invalid; rather, it reflects a known limitation of audits that auditors must manage through professional judgment and appropriate sample selection. Therefore, reviewing a subset of training records represents sampling error.

NEW QUESTION: 74
Scenario 4
SendPay is a financial services company specializing in global money transfers through a network of agents and institutions. As a new company in the market, SendPay aims to deliver top-quality services with its fee- free digital platform, launched last year, enabling clients to send and receive money anytime via smartphones and laptops. At that time, SendPay outsourced software operations to an external team, which also managed the company's technology infrastructure.
Recently, the company applied for ISO/IEC 27001 certification after having an ISMS in place for almost a year.
During the audit, the auditors focused on reviewing SendPay's outsourced operations, specifically looking at the software development and technology infrastructure maintenance handled by the outsourced company.
They followed a structured approach, which included reviewing and evaluating SendPay's processes for monitoring the quality of these outsourced operations. This included verifying if the company met its contractual obligations, ensuring proper governance procedures for engaging outsourced entities, and assessing SendPay's plans in case of expected or unexpected termination of outsourcing agreements.
However, the auditors subtly noted that SendPay's protocols did not fully address contingencies for unanticipated cancellations of outsourcing agreements. Additionally, a technical expert appointed by SendPay assisted the auditors, providing specific knowledge and expertise related to the outsourced operations being audited.

The audit team calculated the number of training hours employees received on ISMS to ensure alignment with established objectives. They also computed the average resolution time of information security incidents based on a sample taken during the audit, which provided valuable insights into SendPay's incident management practices. In addition, the auditors evaluated the reliability of the evidence collected during the audit. They considered several factors influencing the reliability of audit evidence. For example, evidence from surveillance cameras provided more objective proof compared to photos. Timing also played a crucial role in reliability, with mechanisms like transaction recording enhancing the credibility of the evidence. SendPay uses cloud-based platforms to make its operations more efficient and scalable. However, during the audit, the auditors did not request SendPay to provide an inventory of their cloud activities due to resource limitations, relying instead on SendPay's representations.

Question

Did the audit at SendPay include all the necessary steps for auditing outsourced operations?

A. Yes, the audit examined all aspects of outsourced operations.

B. No, the audit overlooked crucial steps, such as reviewing termination plans.

C. No, as the audit team only focused on the steps related to monitoring the quality of outsourced operations.

Answer: (SHOW ANSWER)

The correct answer is B, because the audit did not fully address all necessary steps required for auditing outsourced operations under ISO/IEC 27001:2022. While the auditors reviewed several important aspects, including contractual obligations, governance arrangements, and quality monitoring processes, the scenario clearly states that SendPay's protocols did not fully address contingencies for unanticipated cancellations of outsourcing agreements. This represents a gap in the audit coverage.

ISO/IEC 27001:2022 requires organizations to ensure that information security requirements are addressed in supplier relationships throughout the entire lifecycle, including planning for termination. Annex A controls relating to supplier relationships require organizations to consider continuity, security responsibilities, and exit arrangements to protect information assets when outsourcing agreements end, whether expected or unexpected.

Although the auditors assessed monitoring mechanisms and contractual compliance, identifying that termination contingencies were not fully addressed indicates that this critical area was insufficiently covered.

Therefore, the audit did not include all necessary steps to fully evaluate outsourced operations. Option A is incorrect because the scenario explicitly identifies a missing element. Option C is incorrect because the audit went beyond quality monitoring and included governance, contractual obligations, and termination planning, even though that planning was incomplete.

Thus, the most accurate conclusion is that the audit overlooked crucial steps related to termination arrangements, making option B correct.

NEW QUESTION: 75

You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.

You are currently in a large room that is subdivided into several smaller rooms, each of which has a numeric combination lock and swipe card reader on the door. You notice two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorised electrical repairs.

You go to reception and ask to see the door access record for the client's suite. This indicates only one card was swiped. You ask the receptionist and they reply, "yes it's a common problem. We ask everyone to swipe their cards but with contractors especially, one tends to swipe and the rest simply 'tailgate' their way in" but we know who they are from the reception sign-in.

Based on the scenario above which one of the following actions would you now take?

A. Take no action. Irrespective of any recommendations, contractors will always act in this way

B. Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier

C. Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined

D. Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV

E. Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities

F. Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times

G. Raise a nonconformity against control A.7.2 'physical entry' as a secure area is not adequately protected

H. Tell the organisation they must write to their contractors, reminding them of the need to use access cards appropriately

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), control A.7.2 requires an organization to implement appropriate physical entry controls to prevent unauthorized access to secure areas1. The organization should define and document the criteria for granting and revoking access rights to secure areas, and should monitor and record the use of such access rights1. Therefore, when auditing the organization's application of control A.7.2, an ISMS auditor should verify that these aspects are met in accordance with the audit criteria.

Based on the scenario above, the auditor should raise a nonconformity against control A.7.2, as the secure area is not adequately protected from unauthorized access. The auditor should provide the following evidence and justification for the nonconformity:
* Evidence: The auditor observed two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorized electrical repairs. The auditor checked the door access record for the client's suite and found that only one card was swiped. The auditor asked the receptionist and was told that it was a common problem that contractors tend to swipe one card and tailgate their way in, but they were known from the reception sign-in.
* Justification: This evidence indicates that the organization has not implemented appropriate physical entry controls to prevent unauthorized access to secure areas, as required by control A.7.2. The organization has not defined and documented the criteria for granting and revoking access rights to secure areas, as there is no verification or authorization process for providing swipe cards and combination numbers to external contractors. The organization has not monitored and recorded the use of access rights to secure areas, as there is no mechanism to ensure that each individual swipes their card and enters their combination number before entering a secure area. The organization has relied on the reception sign-in as a means of identification, which is not sufficient or reliable for ensuring information security.
The other options are not valid actions for auditing control A.7.2, as they are not related to the control or its requirements, or they are not appropriate or effective for addressing the nonconformity. For example:
* Take no action: This option is not valid because it implies that the auditor ignores or accepts the nonconformity, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems.
* Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not supplier relationships. Control A.5.20 requires an organization to agree on information security requirements with suppliers that may access, process, store, communicate or provide IT infrastructure components for its information assets1. While this control may be relevant for ensuring information security in supplier relationships, it does not address the issue of unauthorized access to secure areas by external contractors.
* Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not working in secure areas. Control A:7.6 requires an organization to define and apply security measures for working in secure areas1.
While this control may be relevant for ensuring information security when working in secure areas, it does not address the issue of unauthorized access to secure areas by external contractors.
* Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV: This option is not valid because it does not address or resolve the nonconformity, but rather attempts to find alternative or compensating controls that may mitigate its impact or likelihood. While additional arrangements such as CCTV may be useful for verifying individual access to secure areas, they do not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may prevent or reduce its recurrence or severity. While accompanying contractors at all times when accessing secure facilities may be a good practice for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may increase awareness or compliance with the existing controls. While having a large sign in reception reminding everyone requiring access must use their swipe card at all times may be a helpful reminder for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Tell the organisation they must write to their contractors, reminding them of the need to use access cards appropriately: This option is not valid because it does not address or resolve the nonconformity, but rather instructs the organization to take a corrective action that may not be effective or sufficient for ensuring information security. While writing to contractors, reminding them of the need to use access cards appropriately may be a communication measure for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.
7.2.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 76
You are an experienced ISMS audit team leader. During the conducting of a third-party surveillance audit, you decide to test your auditee's knowledge of ISO/IEC 27001's risk management requirements.
You ask her a series of questions to which the answer is either 'that is true' or 'that is false'. Which four of the following should she answer 'that is true'?
A. The results of risk assessments must be maintained
B. Risk identification is used to determine the severity of an information security risk
C. ISO/IEC 27001 provides an outline approach for the management of risk
D. The organisation must produce a risk treatment plan for every business risk identified

E. The organisation must operate a risk treatment process to eliminate it's information security risks
F. The initial phase in an organisation's risk management process should be information security risk assessment
G. Risks assessments should be undertaken at monthly intervals
H. Risk assessments should be undertaken following significant changes
Answer: A,C,D,H (LEAVE A REPLY)
The following four statements are true according to ISO/IEC 27001's risk management requirements: 12
* The results of risk assessments must be maintained. This is true because clause 8.2.3 of ISO/IEC 27001:
2022 requires the organisation to retain documented information of the information security risk assessment process and the results12
* ISO/IEC 27001 provides an outline approach for the management of risk. This is true because clause
6.1.2 of ISO/IEC 27001:2022 specifies the general steps for the information security risk management process, which include establishing the risk criteria, assessing the risks, treating the risks, and monitoring and reviewing the risks12
* The organisation must produce a risk treatment plan for every business risk identified. This is true because clause 6.1.3 of ISO/IEC 27001:2022 requires the organisation to produce a risk treatment plan that defines the actions to be taken to address the unacceptable risks, the responsibilities, the expected dates, and the resources required12
* Risk assessments should be undertaken following significant changes. This is true because clause 8.2.4 of ISO/IEC 27001:2022 requires the organisation to review and update the risk assessment at planned intervals or when significant changes occur12 The following four statements are false according to ISO/IEC 27001's risk management requirements:
* Risk identification is used to determine the severity of an information security risk. This is false because risk identification is used to identify the assets, threats, vulnerabilities, and existing controls that are relevant to the information security risk management process. The severity of an information security risk is determined by the risk analysis, which evaluates the likelihood and impact of the risk scenarios12
* The organisation must operate a risk treatment process to eliminate its information security risks. This is false because the organisation can choose from four options to treat its information security risks:
avoid, transfer, mitigate, or accept. The organisation does not have to eliminate all its information security risks, but only those that are unacceptable according to its risk criteria12
* The initial phase in an organisation's risk management process should be information security risk assessment. This is false because the initial phase in an organisation's risk management process should be establishing the risk management framework, which includes defining the risk management policy, objectives, scope, roles, responsibilities, and criteria. The information security risk assessment is the second phase in the risk management process12
* Risks assessments should be undertaken at monthly intervals. This is false because there is no fixed frequency for conducting risk assessments in ISO/IEC 27001. The organisation should determine the appropriate intervals for reviewing and updating the risk assessment based on its risk appetite, risk profile, and operational context12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Scenario 3: Rebuildy is a construction company located in Bangkok.. Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.
The ISMS implementation outcomes are presented below
*Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.
*Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.
*All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.
*The information security policy is part of a security manual drafted based on best security practices Therefore, it is not a stand-alone document.
*Information security roles and responsibilities have been clearly stated in every employees job description
*Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit Before the certification audit one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.
At the beginning of the audit, the audit team interviewed the company's top management They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001 The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report.
Among others, the following nonconformities were detected:
*An instance of improper user access control settings was detected within the company's financial reporting system.
*A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.
After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.
Based on the scenario above, answer the following question:
Question:
Did the audit team adhere to audit best practices regarding the situation with the financial reporting system?
A. Yes, as it is beyond the scope of the audit
B. No, the audit team should have contacted the certification body and reported the situation
C. No, the audit team should have withdrawn from the audit due to the illegal nature of the act
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The financial reporting system issue is a critical security concern, and the audit team should have reported the situation to the certification body for further action.
* ISO 19011:2018 mandates auditors to escalate issues that impact compliance.
* A. Incorrect:
* Financial systems fall within ISMS scope if they contain sensitive data-it is not beyond the scope.
* C. Incorrect:
* Withdrawal is unnecessary unless legal violations prevent an effective audit.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2 (Internal Audit) & ISO 19011:2018 Clause 6.7 (Audit Follow-Up and Reporting of Serious Issues)

NEW QUESTION: 78
You are performing an ISMS audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to verify the information security of the business continuity management process.
During the audit, you learned that the organisation activated one of the business continuity plans (BCPs) to make sure the nursing service continued during the recent pandemic. You ask Service Manager to explain how the organisation manages information security during the business continuity management process.
The Service Manager presents the nursing service continuity plan for a pandemic and summarises the process as follows:
Stop the admission of any NEW residents.
70% of administration staff and 30% of medical staff will work from home.
Regular staff self-testing including submitting a negative test report 1 day BEFORE they come to the office.
Install ABC's healthcare mobile app, tracking their footprint and presenting a GREEN Health Status QR-Code for checking on the spot.

You ask the Service Manager how to prevent non-relevant family members or interested parties from accessing residents' personal data when staff work from home. The Service Manager cannot answer and suggests the n" Security Manager should help with that.
You would like to further investigate other areas to collect more audit evidence Select three options that will be in your audit trail.
A. Collect more evidence on how the organisation manages information security on mobile devices and during teleworking (Relevant to control A.6.7)
B. Collect more evidence by interviewing more staff about their feeling about working from home.
(Relevant to clause 4.2)
C. Collect more evidence on what resources the organisation provides to support the staff working from home. (Relevant to clause 7.1)
D. Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home. (Relevant to clause 6)
E. Collect more evidence on how and when the Business Continuity Wan has been tested. (Relevant to control A.5.29)
F. Collect more evidence on how the organisation makes sure only staff with a negative test result can enter the organisation (Relevant to control A.7.2)
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), control A.5.29 requires an organization to establish and maintain a business continuity management process to ensure the continued availability of information and information systems at the required level following disruptive incidents1. The organization should identify and prioritize critical information assets and processes, assess the risks and impacts of disruptive incidents, develop and implement business continuity plans (BCPs), test and review the BCPs, and ensure that relevant parties are aware of their roles and responsibilities1.
Therefore, when verifying the information security of the business continuity management process, an ISMS auditor should verify that these aspects are met in accordance with the audit criteria.
Three options that will be in the audit trail for verifying control A.5.29 are:
Collect more evidence on how the organisation manages information security on mobile devices and during teleworking (Relevant to control A.6.7): This option is relevant because it can provide evidence of how the organization has implemented appropriate controls to protect the confidentiality, integrity and availability of information and information systems when staff work from home using mobile devices, such as laptops, tablets or smartphones. This is related to control A.6.7, which requires an organization to establish a policy and procedures for teleworking and use of mobile devices1.
Collect more evidence on how and when the Business Continuity Plan has been tested (Relevant to control A.5.29): This option is relevant because it can provide evidence of how the organization has tested and reviewed the BCPs to ensure their effectiveness and suitability for different scenarios, such as a pandemic. This is related to control A.5.29, which requires an organization to test and review the BCPs at planned intervals or when significant changes occur1.
Collect more evidence on how the organisation makes sure only staff with a negative test result can enter the organisation (Relevant to control A.7.2): This option is relevant because it can provide evidence of how the organization has implemented appropriate controls to prevent or reduce the risk of infection or transmission of diseases among staff or residents, such as requiring regular staff self-testing and using a health status app. This is related to control A.7.2, which requires an organization to ensure that all employees and contractors are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational policies and procedures in this respect1.
The other options are not relevant to verifying control A.5.29, as they are not related to the control or its requirements. For example:
Collect more evidence by interviewing more staff about their feeling about working from home (Relevant to clause 4.2): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 4.2, which requires an organization to understand the needs and expectations of interested parties, but not specifically to control A.5.29.
Collect more evidence on what resources the organisation provides to support the staff working from home (Relevant to clause 7.1): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 7.1, which requires an organization to determine and provide the resources needed for its ISMS, but not specifically to control A.5.29.
Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home (Relevant to clause 6): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 6, which requires an organization to plan actions to address risks and opportunities for its ISMS, but not specifically to control A.5.29.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 79
Scenario 3
NightCore, a multinational technology enterprise headquartered in the United States, specializes in e- commerce, cloud computing, digital streaming, and artificial intelligence (AI). After having an information security management system (ISMS) implemented for over a year, NightCore contracted a certification body to perform an audit for ISO/IEC 27001 certification.
The certification body formed a team of five auditors, with Jack as a team leader. Jack is renowned for his extensive auditing experience in risk management, information security controls, and incident management.

His skill set aligns well with the requirements of auditing principles and processes, enabling him to effectively comprehend the audit scope and apply relevant criteria effectively. Jack also demonstrates a solid understanding of NightCore's organizational structure, purpose, and management practices, as well as the statutory and regulatory requirements applicable to its activities.
The audit carried out by the audit team followed a rational method to reach reliable and reproducible conclusions systematically. The audit team recognized that only information capable of being verified to some extent should be considered valid evidence. In some rare instances during the audit where the verification of certain information posed challenges and where its degree of verifiability was low, the auditors exercised their professional judgment to assess the reliability and determine the level of reliance that could be placed on such evidence.
During the audit, the auditors documented their observations and inspection notes regarding the operational planning and control of NightCore's ISMS operations. They also recorded observations of NightCore's inventory of information and associated assets. Additionally, the auditors reviewed the configuration of firewalls implemented to secure connections to network services.
As the audit approached its final stages, NightCore's commitment to upholding the highest levels of information security became evident. With ISO/IEC 27001 certification within reach, NightCore is well- positioned to achieve ISO/IEC 27001 certification, enhancing its reputation in the technology sector.
Question
Does Jack possess the necessary knowledge and skills required of an auditor? Refer to Scenario 3.
A. No, Jack's experience is limited to only a few areas of auditing which are not sufficient.
B. Yes, only due to Jack's understanding of the organization's structure and its management practices.
C. Yes, Jack possesses the necessary knowledge and skills required of an auditor.
Answer: (SHOW ANSWER)
Jack clearly possesses the necessary knowledge and skills required of an auditor, making option C the correct answer. ISO 19011:2018, which provides guidance on auditing management systems, defines auditor competence as a combination of knowledge, skills, and personal attributes applied during audit activities. The scenario explicitly demonstrates that Jack meets these competence requirements.
Jack has extensive experience in risk management, information security controls, and incident management, which are core knowledge areas for an ISO/IEC 27001 audit. These competencies enable him to understand ISMS requirements, assess controls, and evaluate incident handling processes. In addition, the scenario highlights his understanding of auditing principles and processes, including the use of systematic, rational methods to achieve reliable and reproducible audit conclusions. This directly aligns with ISO 19011 principles such as evidence-based auditing and due professional care.

NEW QUESTION: 80

Scenario 9: UpNet, a networking company, has been certified against ISO/IEC 27001. It provides network security, virtualization, cloud computing, network hardware, network management software, and networking technologies.
The company's recognition has increased drastically since gaining ISO/IEC 27001 certification. The certification confirmed the maturity of UpNefs operations and its compliance with a widely recognized and accepted standard.
But not everything ended after the certification. UpNet continually reviewed and enhanced its security controls and the overall effectiveness and efficiency of the ISMS by conducting internal audits. The top management was not willing to employ a full-time team of internal auditors, so they decided to outsource the internal audit function. This form of internal audits ensured independence, objectivity, and that they had an advisory role about the continual improvement of the ISMS.
Not long after the initial certification audit, the company created a new department specialized in data and storage products. They offered routers and switches optimized for data centers and software-based networking devices, such as network virtualization and network security appliances. This caused changes to the operations of the other departments already covered in the ISMS certification scope. Therefore. UpNet initiated a risk assessment process and an internal audit. Following the internal audit result, the company confirmed the effectiveness and efficiency of the existing and new processes and controls.
The top management decided to include the new department in the certification scope since it complies with ISO/IEC 27001 requirements. UpNet announced that it is ISO/IEC 27001 certified and the certification scope encompasses the whole company.
One year after the initial certification audit, the certification body conducted another audit of UpNefs ISMS.
This audit aimed to determine the UpNefs ISMS fulfillment of specified ISO/IEC 27001 requirements and ensure that the ISMS is being continually improved. The audit team confirmed that the certified ISMS continues to fulfill the requirements of the standard. Nonetheless, the new department caused a significant impact on governing the management system. Moreover, the certification body was not informed about any changes. Thus, the UpNefs certification was suspended.
Based on the scenario above, answer the following question:
Based on scenario 9, why was UpNefs certification suspended?

Freecram.net

A. Because UpNet used and applied the certification out of its scope
B. Because UpNet outsourced the internal audit function
C. Because UpNefs ISMS does not fulfill the requirements of the standard
Answer: (SHOW ANSWER)
UpNet's certification was suspended because the certification body was not informed about the significant changes caused by the new department, impacting the governance of the management system. ISO/IEC 27001 requires organizations to inform the certification body of any changes that significantly impact the ISMS.

NEW QUESTION: 81
Select the correct sequence for the information security risk assessment process in an ISMS.
To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank

1.
2.
3.
4.

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Identify the information security risks | Evaluate the information security risks | Analyse the information security risks | Establish information security criteria

Answer:

1. Establish information security criteria
2. Identify the information security risks
3. Analyse the information security risks
4. Evaluate the information security risks

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Identify the information security risks | Evaluate the information security risks | Analyse the information security risks | Establish information security criteria

Explanation:

According to ISO 27001:2022, the standard for information security management systems (ISMS), the correct sequence for the information security risk assessment process is as follows:

* Establish information security criteria
* Identify the information security risks
* Analyse the information security risks
* Evaluate the information security risks

freecram.net PECB

The first step is to establish the information security criteria, which include the risk assessment methodology, the risk acceptance criteria, and the risk evaluation criteria. These criteria define how the organization will perform the risk assessment, what level of risk is acceptable, and how the risks will be compared and prioritized.
The second step is to identify the information security risks, which involve identifying the assets, threats, vulnerabilities, and existing controls that are relevant to the ISMS. The organization should also identify the potential consequences and likelihood of each risk scenario.
The third step is to analyse the information security risks, which involve estimating the level of risk for each risk scenario based on the criteria established in the first step. The organization should also consider the sources of uncertainty and the confidence level of the risk estimation.
The fourth step is to evaluate the information security risks, which involve comparing the estimated risk levels with the risk acceptance criteria and determining whether the risks are acceptable or need treatment.
The organization should also prioritize the risks based on the risk evaluation criteria and the objectives of the ISMS.
References: ISO 27001:2022 Clause 6.1.2 Information security risk assessment, ISO 27001 Risk Assessment
& Risk Treatment: The Complete Guide - Advisera, ISO 27001 Risk Assessment: 7 Step Guide - IT Governance UK Blog

NEW QUESTION: 82
You are an experienced ISMS audit team leader guiding an auditor in training. Your team has just completed a third-party surveillance audit of a mobile telecom provider. The auditor in training asks you how you intend to prepare for the Closing meeting. Which four of the following are appropriate responses?
A. I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge the findings
B. I will instruct my audit team to wait outside the auditee's offices so we can leave as quickly as possible after the closing meeting. This saves our time and the client's time too
C. It is not necessary to prepare for the closing meeting. Once you have carried out as many audits as I have you already know what needs to be discussed
D. I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented
E. I will contact head office to ensure our invoice has been paid, If not, I will cancel the closing meeting and temporarily withhold the audit report
F. I will discuss any follow-up required with my audit team
G. I will review and, as appropriate, approve my teams audit conclusions
H. I will review the audit evidence and the audit findings with the rest of the team
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.6 requires the audit team leader to conduct a closing meeting with the auditee's representatives at the end of the audit to present the audit conclusions and any findings1. The closing meeting should also provide an opportunity for the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1. Therefore, when preparing for the closing meeting, an ISMS auditor should consider the following actions:
I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to collecting and evaluating audit evidence and reaching audit conclusions. The auditor should advise the auditee that the purpose of the closing meeting is for the audit team to communicate their findings, which are based on objective evidence and professional judgement. The auditor should also explain that it is not an opportunity for the auditee to challenge these findings, as they have already been discussed and confirmed during the audit. However, the auditor should also invite the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1.
I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented: This action is appropriate because it reflects the fact that the auditor has followed a planned and agreed audit programme and schedule. The auditor should schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented, in accordance with clause
6.6 of ISO 19011:20181. The auditor should also ensure that the closing meeting is attended by those responsible for managing or implementing the ISMS, as well as any other relevant parties1.
I will discuss any follow-up required with my audit team: This action is appropriate because it reflects the fact that the auditor has followed a risk-based approach to determining and reporting any follow-up actions required by the auditee or the certification body. The auditor should discuss any follow-up required with their audit team, such as verifying corrective actions for nonconformities or conducting a subsequent audit1. The auditor should also document any follow-up actions in the audit report1.
I will review and, as appropriate, approve my teams audit conclusions: This action is appropriate because it reflects the fact that the auditor has followed a rigorous and professional process to reaching and reporting audit conclusions. The auditor should review and, as appropriate, approve their teams audit conclusions, which are based on objective evidence and professional judgement. The auditor should also ensure that their teams audit conclusions are consistent with the audit objectives and scope, and reflect the overall performance and conformity of the ISMS1.

NEW QUESTION: 83

Scenario 1: Fintive is a distinguished security provider for online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies that operate online and want to improve their information security, prevent fraud, and protect user information such as PII. Fintive centers its decision-making and operating process based on previous cases. They gather customer data, classify them depending on the case, and analyze them. The company needed a large number of employees to be able to conduct such complex analyses. After some years, however, the technology that assists in conducting such analyses advanced as well. Now, Fintive is planning on using a modern tool, a chatbot, to achieve pattern analyses toward preventing fraud in real-time. This tool would also be used to assist in improving customer service.
This initial idea was communicated to the software development team, who supported it and were assigned to work on this project. They began integrating the chatbot on their existing system. In addition, the team set an objective regarding the chatbot which was to answer 85% of all chat queries.
After the successful integration of the chatbot, the company immediately released it to their customers for use.
The chatbot, however, appeared to have some issues.
Due to insufficient testing and lack of samples provided to the chatbot during the training phase, in which it was supposed "to learn" the queries pattern, the chatbot failed to address user queries and provide the right answers. Furthermore, the chatbot sent random files to users when it received invalid inputs such as odd patterns of dots and special characters. Therefore, the chatbot was unable to properly answer customer queries and the traditional customer support was overwhelmed with chat queries and thus was unable to help customers with their requests.
Consequently, Fintive established a software development policy. This policy specified that whether the software is developed in-house or outsourced, it will undergo a black box testing prior to its implementation on operational systems.
Based on this scenario, answer the following question:
Based on scenario 1, the chatbot was unable to properly answer customer queries. Which principle of information security has been affected in this case?
A. Availability
B. Integrity
C. Confidentiality
Answer: B (LEAVE A REPLY)
The integrity principle of information security has been affected in this case. The chatbot's inability to provide accurate answers and its unintended behavior (sending random files) due to insufficient testing and lack of proper training samples compromised the integrity of the system.

NEW QUESTION: 84
Scenario 2: Knight is an electronics company from Northern California, US that develops video game consoles. Knight has more than 300 employees worldwide. On the fifth anniversary of their establishment, they have decided to deliver the G-Console, a new generation video game console aimed for worldwide markets. G-Console is considered to be the ultimate media machine of 2021 which will give the best gaming experience to players.
The console pack will include a pair of VR headset, two
games, and other gifts.
Over the years, the company has developed a good reputation by showing integrity, honesty, and respect toward their customers. This good reputation is one of the reasons why most passionate gamers aim to have Knight's G-console as soon as it is released in the market.
Besides being a very customer-oriented company, Knight
also gained wide recognition within the gaming industry because of the developing quality. Their prices are a bit higher than the reasonable standards allow.
Nonetheless, that is not considered an issue for most loyal customers of Knight, as their quality is top-notch.
Being one of the top video game console developers in the world, Knight is also often the center of attention for malicious activities. The company has had an operational ISMS for over a year. The ISMS scope includes all departments of Knight, except Finance and HR departments.
Recently, a number of Knight's files containing proprietary information were leaked by hackers. Knight's incident response team (IRT) immediately started to analyze every part of the system and the details of the incident.
The IRT's first suspicion was that Knight's employees used weak passwords and consequently were easily cracked by hackers who gained unauthorized access to their accounts. However, after carefully investigating the incident, the IRT determined that hackers accessed accounts by capturing the file transfer protocol (FTP) traffic.
FTP is a network protocol for transferring files between accounts. It uses clear text passwords for authentication.
Following the impact of this information security incident and with IRT's suggestion, Knight decided to replace the FTP with Secure Shell (SSH) protocol, so anyone capturing the traffic can only see encrypted data.
Following these changes, Knight conducted a risk assessment to verify that the implementation of controls had minimized the risk of similar incidents. The results of the process were approved by the ISMS project manager who claimed that the level of risk after the implementation of new controls was in accordance with the company's risk acceptance levels.
Based on this scenario, answer the following question:

Based on scenario 2, Knight decided to replace the FTP with Secure Shell (SSH) protocol. Should the Statement of Applicability (SoA) be updated in this case?
A. No, the usage of SSH protocol is not an ISO/IEC 27001 requirement and; therefore, does not need to be included in the SoA
B. No, because the SoA should be updated only when new controls are added, not when old ones are canceled
C. Yes, the implementation of the new control should be justified and included in the SoA
Answer: (SHOW ANSWER)
The Statement of Applicability (SoA) is a core document within an ISMS that outlines the security controls an organization implements. When a new control, such as the SSH protocol, is implemented, it should be included in the SoA to reflect the current state of the ISMS. The SoA should be updated to justify the inclusion of the new control and to document how it is implemented within the organization12. References: = This guidance is based on the best practices for maintaining the SoA as per ISO/IEC 27001, which requires the SoA to be a living document that accurately reflects the security controls in use by the organization

NEW QUESTION: 85
An audit team leader is planning a follow-up audit after the completion of a third-party surveillance audit earlier in the year. They have decided they will verify the nonconformities that require corrections before they move on to consider corrective actions.
Based on the descriptions below, which four of the following are corrections for nonconformities identified at the surveillance?
A. A signature missing from a client's contract for the supply of data services was added
B. A software installation guide which had not been sent to the client along with their new system was posted out
C. An incorrectly dated purchase order for a new network switch was rectified
D. Data centre staff not carrying out backups in accordance with specified procedures were retrained
E. Hard drive HD302 which had been colour-coded green (available for use) instead of red (to be destroyed) was removed from the system
F. Scheduled management reviews, having been missed, were prioritised by the General Manager for holding on a specific date twice each following year
G. The documented process for product shipment, which did not reflect how this activity was conducted by the despatch team, was re-written and the team trained accordingly
H. The organisation, having failed to maintain its Schedule of Applicability, re-allocated responsibility for its updating to the Technical Director
Answer: (SHOW ANSWER)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, a correction is an action to eliminate a detected nonconformity, such as rework, repair, or replacement1. The examples of A, B, C, and E are corrections because they fix the errors or defects that caused the nonconformities, such as a missing signature, a missing guide, a wrong date, or a wrong colour code. The other examples (D, F, G, and H) are not corrections, but corrective actions, because they address the root causes of the nonconformities, such as inadequate training, poor planning, ineffective documentation, or unclear responsibility2. References: 1:
PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 35, section 4.5.12: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 36, section 4.5.2.

NEW QUESTION: 86
According to ISO/IEC 27001, an Information Security Management System seeks to protect which two of the following?
A. The accessibility of information
B. The authenticity of information
C. The confidentiality of information
D. The consistency of information
E. The integration of information
F. The integrity of information
Answer: (SHOW ANSWER)
ISO/IEC 27001 focuses on the core principles of the CIA triad:
*Confidentiality: Ensuring information is accessible only to authorized individuals.
*Integrity: Maintaining the accuracy and completeness of information, protecting it from unauthorized modification.
*Availability: Information should be accessible to authorized users when needed (this is also important, but not one of the choices in this specific question).
References:

*ISO/IEC 27001:2022, Section 4.2 (Understanding the needs and expectations of interested parties): This section highlights the importance of determining relevant interested parties and their requirements related to information security, which includes addressing confidentiality, integrity, and availability.
*PECB Candidate Handbook, ISO/IEC 27001 Lead Auditor: This handbook often emphasizes the foundational role of the CIA triad within an effective Information Security Management System (ISMS).

NEW QUESTION: 87
An organisation is looking for management system initial certification. Please identify the sequence of the activities to be undertaken by the organisation.
To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

An organisation is looking for management system initial certification. Please identify the sequence of the activities to be undertaken by the organisation.

1. Establish the management system
2.
3.
4.
5.

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Complete any corrective actions | Conduct supplier audits | Engage a Certification Body for stage 1 and stage 2 audits | Plan the audit programme | Conduct internal audits | Hold a Management Review

Answer:

An organisation is looking for management system initial certification. Please identify the sequence of the activities to be undertaken by the organisation.

1. Establish the management system
2. Plan the audit programme
3. Conduct internal audits
4. Hold a Management Review

Engage a Certification Body for stage 1 and stage 2 audits

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Complete any corrective actions | Conduct supplier audits | Engage a Certification Body for stage 1 and stage 2 audits | Plan the audit programme | Conduct internal audits | Hold a Management Review

Explanation:
The correct sequence of activities is:

* Establish the management system
* Plan the audit programme
* Conduct internal audits
* Hold a Management Review
* Engage a Certification Body for stage 1 and stage 2 audits
* Complete any corrective actions

Comprehensive but Short Explanation: = According to the PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, the steps for achieving certification are as follows1:

* Establish the management system: This involves defining the scope, objectives, policies, procedures, and controls of the ISMS, as well as ensuring the availability of resources and top management commitment.
* Plan the audit programme: This involves defining the audit objectives, criteria, scope, frequency, methods, and responsibilities for conducting internal audits of the ISMS.
* Conduct internal audits: This involves verifying the conformity and effectiveness of the ISMS, as well as identifying any nonconformities or opportunities for improvement.
* Hold a Management Review: This involves reviewing the performance and suitability of the ISMS, as well as deciding on any changes or actions needed to improve it.
* Engage a Certification Body for stage 1 and stage 2 audits: This involves selecting a reputable and accredited certification body to conduct an external audit of the ISMS, consisting of two stages: a documentation review and an on-site assessment.
* Complete any corrective actions: This involves addressing any nonconformities or findings identified by the certification body, and providing evidence of their implementation and effectiveness.

= 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, pages 25-26.

NEW QUESTION: 88

To verify conformity to control 8.15 Logging of ISO/IEC 27001 Annex A, the audit team verified a sample of server logs to determine if they can be edited or deleted. Which audit procedure was used?

A. Analysis
B. Sampling
C. Observation

Answer: (SHOW ANSWER)

The audit procedure used here is "analysis." The audit team analyzed server logs to verify if they can be edited or deleted, focusing on evaluating the logs' properties and the controls over their manipulation to ensure they comply with ISO/IEC 27001 requirements.

References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 89

Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.

Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments.

Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.

During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC 27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.

Based on the scenario above, answer the following question:

Question:
What action should be taken regarding Techmanic's certification?
A. Suspend the certification because they used the certification out of its scope
B. Withdraw the certification because they failed to resolve nonconformities related to hosting services
C. Transfer the certification because they were not granted the extension certification
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Techmanic misrepresented its certification scope, which is a violation of ISO certification rules.
* Suspension allows time for corrective action before withdrawal is considered.
* B. Incorrect:
* Certification withdrawal is only necessary if corrective actions fail after suspension.
* C. Incorrect:
* Transfer does not resolve misrepresentation issues.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.6.5 (Certification Suspension and Misrepresentation Issues)

NEW QUESTION: 90
Which two of the following work documents are not required for audit planning by an auditor conducting a certification audit?
FreeCram.net
A. An audit plan
B. A career history of the IT manager
C. A checklist
D. A list of external providers
E. A sample plan
F. An organisation's financial statement
Answer: (SHOW ANSWER)
Audit planning for certification audits is defined by ISO 19011:2018, clause 6.3 (Preparing audit activities) and ISO/IEC 27006.
Key audit planning documents include:
* Audit plan (mandatory, prepared by team leader)
* Checklists (supporting tool for consistency and coverage of requirements)
* List of external providers (required to check compliance with ISO/IEC 27001 Annex A.5.19 - supplier relationships and A.5.20 - supplier agreements)
* Sample plans (used when sampling evidence across sites, processes, or records is needed, especially in Stage 2 audits) However, the following are not required:
* B. Career history of the IT manager - Personnel competence may be verified during interviews and evidence review, but an auditor does not need career histories as part of audit planning. ISO 19011 only requires access to competence records if needed but not CVs.
* F. Organisation's financial statement - Financial performance is not part of ISMS audit planning unless it relates to identified risks or contractual obligations. ISO/IEC 27001 focuses on information security risks, not financial audit compliance.
ISO 19011:2018 (clause 6.3.2) clearly defines the required planning inputs as:
* Audit objectives, scope, and criteria
* Audit team roles and responsibilities
* Allocation of resources
* Information about the auditee's ISMS (e.g., documented scope, processes, external provider relationships, relevant legal/regulatory requirements) There is no mention of personnel CVs or financial statements being required.

Final Correct Answer: B and F
References:
ISO 19011:2018, clause 6.3 (Preparing audit activities)
ISO/IEC 27006:2015, section 9.2 (Audit planning requirements for ISMS certification bodies)

NEW QUESTION: 91
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. Confidentiality and nondisclosure agreements
B. How access to source code and development tools are managed
C. How power and data cables enter the building
D. How protection against malware is implemented
E. How the organisation evaluates its exposure to technical vulnerabilities
F. Information security awareness, education and training
G. The organisation's arrangements for information deletion
H. The organisation's business continuity arrangements
Answer: (SHOW ANSWER)
The four controls from the list that the auditor in training should review are:
*B. How access to source code and development tools are managed: This control requires the organisation to restrict and monitor the access to the source code and development tools that are used to create, modify, or maintain the software applications and systems that process or store the data of external clients. This is important for ensuring the integrity, confidentiality, and availability of the software and the data, as well as for preventing unauthorized changes, errors, or malicious code injection.
*D. How protection against malware is implemented: This control requires the organisation to implement appropriate measures to detect, prevent, and remove malware from the IT systems and devices that process or store the data of external clients. This includes using antivirus software, firewalls, email filtering, web filtering, and other tools to protect against viruses, worms, ransomware, spyware, and other malicious software. This is essential for safeguarding the data and the systems from corruption, theft, or damage caused by malware.
*E. How the organisation evaluates its exposure to technical vulnerabilities: This control requires the organisation to identify and assess the technical vulnerabilities that may affect the IT systems and devices that process or store the data of external clients. This includes using vulnerability scanning tools, penetration testing tools, threat intelligence sources, and other methods to discover and evaluate the weaknesses and gaps in the security of the systems and the devices. This is necessary for prioritizing and implementing the appropriate corrective actions and controls to mitigate the risks posed by the vulnerabilities.
*G. The organisation's arrangements for information deletion: This control requires the organisation to establish and implement policies and procedures for deleting the data of external clients from the IT systems and devices when it is no longer needed or required. This includes defining the criteria and methods for data deletion, such as secure erasure, encryption, or physical destruction. This is important for complying with the contractual obligations and the legal and regulatory requirements regarding the retention and disposal of the data, as well as for protecting the confidentiality and integrity of the data.
References: = ISO/IEC 27001:2022, Annex A, clauses A.8.9, A.8.10, A.8.11, and A.8.28; Understanding ISO
27001:2022: People, process, and technology, pages 6-7; What are the 11 new security controls in ISO 27001:
2022? - Advisera.

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92

Your organisation is currently seeking ISO/IEC27001:2022 certification. You have just qualified as an Internal ISMS auditor and the ICT Manager wants to use your newly acquired knowledge to assist him with the design of an information security incident management process.

He identifies the following stages in his planned process and asks you to confirm which order they should appear in.

Step 1	**Incident logging**
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	
Step 7	
Step 8	**Incident closure**

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whist resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Answer:

Step 1	**Incident log**
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	
Step 7	
Step 8	**Incident closure**

Incident categorisation – determine whether the incident is a hardware issue, network issue

Incident prioritisation – classify the incident as critical, high, medium, low

SLA management and escalation – ensure any service level agreements are adhered to whist resolution is being implemented. If a

Incident resolution – a temporary workaround or permanent resolution has been identified

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whist resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Explanation:

Step 1 = Incident logging Step 2 = Incident categorisation Step 3 = Incident prioritisation Step 4 = Incident assignment Step 5 = Task creation and management Step 6 = SLA management and escalation Step 7 = Incident resolution Step 8 = Incident closure The order of the stages in the information security incident management process should follow a logical sequence that ensures a quick, effective, and orderly response to the incidents, events, and weaknesses. The order should also be consistent with the best practices and guidance provided by ISO/IEC 27001:2022 and ISO

/IEC 27035:2022. Therefore, the following order is suggested:

* Step 1 = Incident logging: This step involves recording the details of the potential incident, event, or weakness, such as the date, time, source, description, impact, and reporter. This step is important to provide a traceable record of the incident and to facilitate the subsequent analysis and response. This step is related to control A.16.1.1 of ISO/IEC 27001:2022, which requires the organization to establish responsibilities and procedures for the management of information security incidents, events, and weaknesses. This step is also related to clause 6.2 of ISO/IEC 27035:2022, which provides guidance on how to log the incidents, events, and weaknesses.
* Step 2 = Incident categorisation: This step involves determining the type and nature of the incident, event, or weakness, such as whether it is a hardware issue, network issue, or software issue. This step is important to classify the incident and to assign it to the appropriate resolver or team. This step is related to control A.16.1.2 of ISO/IEC 27001:2022, which requires the organization to report information security events and weaknesses as quickly as possible through appropriate management channels. This step is also related to clause 6.3 of ISO/IEC 27035:2022, which provides guidance on how to categorize the incidents, events, and weaknesses.
* Step 3 = Incident prioritisation: This step involves assessing the severity and urgency of the incident, event, or weakness, and classifying it as critical, high, medium, or low. This step is important to prioritize the incident and to allocate the necessary resources and time for the response. This step is related to control A.16.1.3 of ISO/IEC 27001:2022, which requires the organization to assess and prioritize information security events and weaknesses in accordance with the defined criteria. This step is also related to clause 6.4 of ISO/IEC 27035:2022, which provides guidance on how to prioritize the incidents, events, and weaknesses.
* Step 4 = Incident assignment: This step involves passing the incident, event, or weakness to the individual or team who is best suited to resolve it, based on their skills, knowledge, and availability.

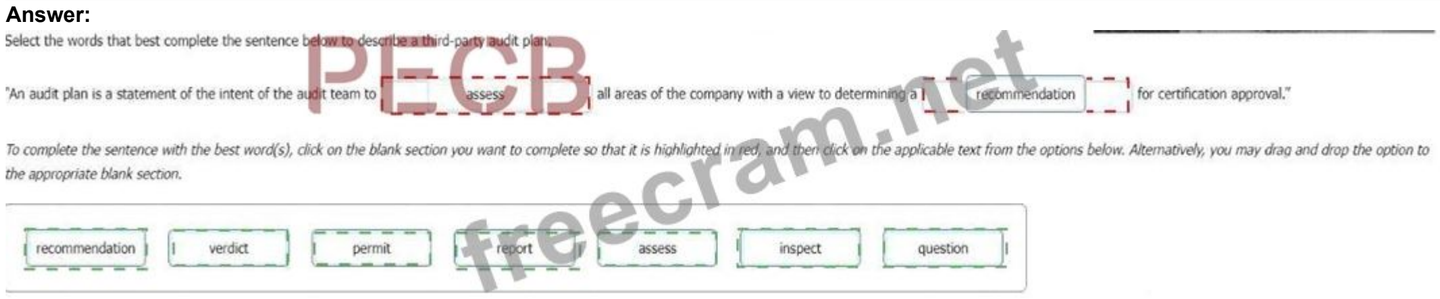
This step is important to ensure that the incident is handled by the right person or team and to avoid delays or confusion. This step is related to control A.16.1.4 of ISO/IEC 27001:2022, which requires the organization to respond to information security events and weaknesses in a timely manner, according to the agreed procedures. This step is also related to clause 6.5 of ISO/IEC 27035:2022, which provides guidance on how to assign the incidents, events, and weaknesses.

* Step 5 = Task creation and management: This step involves identifying and coordinating the work needed to resolve the incident, event, or weakness, such as performing root cause analysis, testing solutions, implementing changes, and documenting actions. This step is important to ensure that the incident is resolved effectively and efficiently, and that the actions are tracked and controlled. This step is related to control A.16.1.5 of ISO/IEC 27001:2022, which requires the organization to apply lessons learned from information security events and weaknesses to take corrective and preventive actions. This step is also related to clause 6.6 of ISO/IEC 27035:2022, which provides guidance on how to create and manage the tasks for the incidents, events, and weaknesses.

* Step 6 = SLA management and escalation: This step involves ensuring that any service level agreements (SLAs) are adhered to while the resolution is being implemented, and that the incident is escalated to a higher level of authority or support if a breach looks likely or occurs. This step is important to ensure that the incident is resolved within the agreed time frame and quality, and that any deviations or issues are communicated and addressed. This step is related to control A.16.1.6 of ISO /IEC 27001:2022, which requires the organization to communicate information security events and weaknesses to the relevant internal and external parties, as appropriate. This step is also related to clause 6.7 of ISO/IEC 27035:2022, which provides guidance on how to manage the SLAs and escalations for the incidents, events, and weaknesses.
* Step 7 = Incident resolution: This step involves applying a temporary workaround or a permanent solution to resolve the incident, event, or weakness, and restoring the normal operation of the information and information processing facilities. This step is important to ensure that the incident is resolved completely and satisfactorily, and that the information security is restored to the desired level.
This step is related to control A.16.1.7 of ISO/IEC 27001:2022, which requires the organization to identify the cause of information security events and weaknesses, and to take actions to prevent their recurrence or occurrence. This step is also related to clause 6.8 of ISO/IEC 27035:2022, which provides guidance on how to resolve the incidents, events, and weaknesses.
* Step 8 = Incident closure: This step involves closing the incident, event, or weakness, after verifying that it has been resolved satisfactorily, and that all the actions have been completed and documented.
This step is important to ensure that the incident is formally closed and that no further actions are required. This step is related to control A.16.1.8 of ISO/IEC 27001:2022, which requires the organization to collect evidence and document the information security events and weaknesses, and the actions taken. This step is also related to clause 6.9 of ISO/IEC 27035:2022, which provides guidance on how to close the incidents, events, and weaknesses.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6 ISO/IEC 27035:2022, Information technology - Security techniques - Information security incident management

NEW QUESTION: 93
Select the words that best complete the sentence below to describe a third-party audit plan.
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:



Explanation:
The words that best complete the sentence are assess and recommendation. The sentence would read as follows:

"An audit plan is a statement of the intent of the audit team to assess all areas of the company with a view to determining a recommendation for certification approval." According to the web search results from my predefined tool, a third-party audit plan is a document that describes the scope, objectives, criteria, and methodology of an external audit conducted by an independent certification body to verify the conformity of an organization's ISMS with the ISO 27001 standard12. The audit plan also includes the audit schedule, the audit team, the audit locations, and the audit deliverables23. One of the main deliverables of a third-party audit is the audit report, which summarizes the audit findings, the audit conclusions, and the audit recommendation34. The audit recommendation is the opinion of the audit team on whether the organization's ISMS meets the certification requirements and whether the certification should be granted, maintained, suspended, or withdrawn45. Therefore, the purpose of the audit plan is to state the intention of the audit team to assess all areas of the company, meaning to evaluate the performance and effectiveness of the ISMS, and to determine a recommendation for certification approval, meaning to provide a judgment on the certification status of the ISMS. The other words in the options, such as verdict, permit, report, inspect, and question, do not accurately reflect the meaning of the audit plan. A verdict is a formal decision made by a judge or a jury, not by an audit team. A permit is a legal authorization to do something, not a certification of conformity. A report is a document that presents the audit results, not the audit intention. An inspection is a visual examination of something, not a comprehensive assessment of an ISMS. A question is a request for information, not a determination of a recommendation.

NEW QUESTION: 94
Question:
A marketing agency has developed its risk assessment approach as part of the ISMS implementation. Is this acceptable?
A. Yes, any risk assessment methodology that complies with the ISO/IEC 27001 requirements can be used
B. Yes, only if the risk assessment methodology is aligned with recognized risk assessment methodologies
C. No, the risk assessment methodology provided by ISO/IEC 27001 should be used when implementing an ISMS
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
ISO/IEC 27001 does not prescribe a specific risk assessment methodology but instead provides general requirements for risk assessment. Organizations are free to develop their own risk assessment methods, as long as they:
* Identify risks and impacts on information security.
* Define risk criteria for evaluating risks.
* Implement risk treatment plans based on the organization's context.
A). Correct Answer:
* ISO/IEC 27001 Clause 6.1.2 (Information Security Risk Assessment) states that organizations may define their own risk assessment methodology.
* This approach must be systematic, measurable, and aligned with business objectives.
B). Incorrect:
* Organizations are not required to use a recognized methodology like OCTAVE, MEHARI, or EBIOS, as long as their approach meets ISO requirements.
C). Incorrect:
* ISO/IEC 27001 does not mandate a specific risk assessment method, only that a consistent and structured approach is used.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 6.1.2 (Information Security Risk Assessment Process)

NEW QUESTION: 95
Scenario:
After an information security incident, an organization created a comprehensive backup procedure involving regular, automated backups of all critical data to offsite storage locations. By doing so, which principle of information security is the organization applying in this case?
A. Integrity
B. Confidentiality
C. Availability
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
The CIA Triad (Confidentiality, Integrity, and Availability) is the foundation of information security principles.

* Availability ensures that data and services are accessible when needed. By implementing regular, automated backups and offsite storage, the organization ensures that critical data remains accessible even after a security incident (e.g., data loss, cyberattacks, or hardware failures). This aligns with ISO
/IEC 27001:2022 Annex A Control A.8.13 (Information Backup), which emphasizes maintaining and testing backups to ensure system resilience.
* Integrity ensures that data remains unaltered and accurate, but backups do not inherently enforce integrity unless accompanied by checksum or validation mechanisms.
* Confidentiality ensures that only authorized users can access data, which is not the primary goal of a backup procedure.

NEW QUESTION: 96
Scenario 3: Rebuildy is a construction company located in Bangkok.. Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.
The ISMS implementation outcomes are presented below
*Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.
*Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.
*All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.
*The information security policy is part of a security manual drafted based on best security practices Therefore, it is not a stand-alone document.
*Information security roles and responsibilities have been clearly stated in every employees job description
*Management reviews of the ISMS are conducted at planned intervals.
Rebuildy applied for certification after two midterm management reviews and one annual internal audit Before the certification audit one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.
At the beginning of the audit, the audit team interviewed the company's top management They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001 The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report.
Among others, the following nonconformities were detected:
*An instance of improper user access control settings was detected within the company's financial reporting system.
*A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.
After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.
Based on the scenario above, answer the following question:
Question:
Based on Scenario 3, the audit team used information obtained from interviews with top management to determine Rebuildy's conformity to several ISO/IEC 27001 clauses. Is this acceptable?
A. No, the audit team should have used only documentary evidence, such as policies and procedures, to determine conformity
B. Yes, the audit team obtained verbal evidence by written confirmations from the top management, which can be used to determine conformity to the standard
C. Yes, interviews with top management are the most reliable form of audit evidence and can be used to determine conformity to the standard without further verification
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Audit evidence can come from interviews, observations, and documentation.
* Verbal evidence from top management is acceptable if documented and confirmed in writing.
* A. Incorrect:

* ISO 19011 allows verbal evidence as long as it is substantiated.
* C. Incorrect:
* Interviews alone are not sufficient-additional verification is required.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.6 (Reviewing Documented Information)

NEW QUESTION: 97
Which three of the following work documents are not required for audit planning by an auditor conducting a certification audit?
A. An audit plan
B. A sample plan
C. An organisation's financial statement
D. A checklist
E. A career history of the IT manager
F. A list of external providers
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, an auditor conducting a certification audit should prepare for an audit by reviewing relevant information about the auditee's context and processes1. This may include reviewing documented information related to the audited management system (such as policies, procedures, manuals), previous audit reports and records (such as findings, nonconformities, corrective actions), relevant legal and regulatory requirements (such as laws, standards), relevant risks and opportunities (such as internal and external issues), relevant performance indicators (such as objectives, targets), etc1. Therefore, an auditor may need work documents such as an audit plan (which defines what will be done during an audit), a sample plan (which defines how many samples will be taken from a population), and a checklist (which helps to ensure that all relevant aspects are covered during an audit)1. However, an auditor does not need work documents such as an organisation's financial statement (which is not directly related to information security management), a career history of the IT manager (which is not relevant to assessing conformity with ISO/IEC 27001:2022), or a list of external providers (which is not necessary for planning an audit)1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 98
You are conducting a third-party surveillance audit when another member of the audit team approaches you seeking clarification. They have been asked to assess the organisation's application of control 5.7 - Threat Intelligence. They are aware that this is one of the new controls introduced in the 2022 edition of ISO/IEC
27001, and they want to make sure they audit the control correctly.
They have prepared a checklist to assist them with their audit and want you to confirm that their planned activities are aligned with the control's requirements.
Which three of the following options represent valid audit trails?
A. I will ensure that the task of producing threat intelligence is assigned to the organisation's internal audit team
B. I will ensure that the organisation's risk assessment process begins with effective threat intelligence
C. I will speak to top management to make sure all staff are aware of the importance of reporting threats
D. I will ensure that appropriate measures have been introduced to inform top management as to the effectiveness of current threat intelligence arrangements
E. I will check that the organisation has a fully documented threat intelligence process
F. I will check that threat intelligence is actively used to protect the confidentiality, integrity and availability of the organisation's information assets
G. I will review how information relating to information security threats is collected and evaluated to produce threat intelligence
H. I will determine whether internal and external sources of information are used in the production of threat intelligence
Answer: (SHOW ANSWER)
These three options represent valid audit trails for control 5.7, as they are aligned with the control's requirements and objectives. According to the web search results from my predefined tool, control 5.7 requires organisations to collect and analyse information relating to information security threats and use that information to take mitigation actions12. The control also specifies that threat intelligence should be relevant, perceptive, contextual, and actionable, and that it should be used to prevent, detect, or respond to threats34.

Therefore, the auditor should verify how the organisation collects, analyses, and produces threat intelligence, how it uses threat intelligence to protect its information assets, and how it monitors and evaluates the effectiveness of its threat intelligence arrangements. The other options are not valid audit trails, as they are either irrelevant, incorrect, or incomplete. For example:
*The task of producing threat intelligence is not assigned to the organisation's internal audit team, but to the person or team responsible for the ISMS, such as the information security manager or the information security committee5 .
*The organisation's risk assessment process does not begin with effective threat intelligence, but with the identification of the context, scope, and objectives of the ISMS . Threat intelligence is an input for the risk identification and analysis, but not the starting point of the risk assessment process.
*Speaking to top management to make sure all staff are aware of the importance of reporting threats is not sufficient to audit the control, as it does not address how the organisation collects, analyses, and produces threat intelligence, nor how it uses it to take mitigation actions. The auditor should also speak to the staff involved in the threat intelligence process, and review the relevant documents and records.
*Checking that the organisation has a fully documented threat intelligence process is not enough to audit the control, as it does not verify the implementation and effectiveness of the process. The auditor should also observe the process in action, and examine the outputs and outcomes of the process.
*Determining whether internal and external sources of information are used in the production of threat intelligence is a partial audit trail, as it only covers one aspect of the control. The auditor should also assess the quality, reliability, and relevance of the sources, and how the information is analysed and used.
References: = 1: ISO 27001:2022 Annex A 5.7 - Threat Intelligence - ISMS.online12: ISO 27001 Annex A
5.7 Threat Intelligence - High Table23: ISO/IEC 27001:2022 Information technology - Security techniques
- Information security management systems - Requirements, clause A.5.74: ISO 27002 Emphasizes Need For Threat Intelligence - Rapid745: ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 6.3.2. : ISO 27001 Statement of Applicability [Updated 2024] - Sprinto3 : ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, clause 6.1.1. : ISO 27001 Requirement 6.1.1 - Actions to address risks and opportunities | ISMS.online1

NEW QUESTION: 99
Which two of the following options are an advantage of using a sampling plan for the audit?
A. Overrules the auditor's instincts
B. Reduces the audit duration
C. Prevents conflict within the audit team
D. Gives confidence in the audit results
E. Implements the audit plan efficiently
F. Use of the plan for consecutive audits
Answer: (SHOW ANSWER)
A sampling plan for the audit is a method of selecting a representative subset of the audit evidence to evaluate the conformity of the ISMS1. The advantages of using a sampling plan are:
* It reduces the audit duration by focusing on the most relevant and significant aspects of the ISMS2.
* It gives confidence in the audit results by ensuring that the sample is sufficient, reliable, and unbiased3.
1: ISMS Auditing Guideline - ISO27000, page 9; 2: Internal Audit Plan - ISO Templates and Documents Download; 3: A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit, Step 4; : ISMS Auditing Guideline - ISO27000; : Internal Audit Plan - ISO Templates and Documents Download; : A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit

NEW QUESTION: 100

Scenario 1: Fintive is a distinguished security provider for online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies that operate online and want to improve their information security, prevent fraud, and protect user information such as PII. Fintive centers its decision-making and operating process based on previous cases. They gather customer data, classify them depending on the case, and analyze them. The company needed a large number of employees to be able to conduct such complex analyses. After some years, however, the technology that assists in conducting such analyses advanced as well. Now, Fintive is planning on using a modern tool, a chatbot, to achieve pattern analyses toward preventing fraud in real-time. This tool would also be used to assist in improving customer service.
This initial idea was communicated to the software development team, who supported it and were assigned to work on this project. They began integrating the chatbot on their existing system. In addition, the team set an objective regarding the chatbot which was to answer 85% of all chat queries. After the successful integration of the chatbot, the company immediately released it to their customers for use.
The chatbot, however, appeared to have some issues.
Due to insufficient testing and lack of samples provided to the chatbot during the training phase, in which it was supposed "to learn" the queries pattern, the chatbot failed to address user queries and provide the right answers. Furthermore, the chatbot sent random files to users when it received invalid inputs such as odd patterns of dots and special characters. Therefore, the chatbot was unable to properly answer customer queries and the traditional customer support was overwhelmed with chat queries and thus was unable to help customers with their requests.
Consequently, Fintive established a software development policy. This policy specified that whether the software is developed in-house or outsourced, it will undergo a black box testing prior to its implementation on operational systems.
What type of security control does the use of black box testing represent? Refer to scenario 1.

Freecram.net

A. Corrective and technical
B. Detective and managerial
C. Preventive and technical
Answer: (SHOW ANSWER)

NEW QUESTION: 101
You are an experience ISMS audit team leader carrying out a third-party certification audit of an organization specialising in the secure disposal of confidential documents and removable media. Both documents and media are shredded in military grade devices which make it impossible to reconstruct the original.
The audit has gone well and you are just about to start to write the audit report, 30 minutes before the closing meeting. At this point one of the organization's employees knocks on your door and asks if they can speak to you. They tell you that when things get busy her manager tells her to use a lower grade industrial shredder instead as the organisation has more of these and they operate faster. You were not informed about the existence or use of these machines by the auditee.
Select three options for how you should respond to this information.
A. Advise the individual managing the audit programme of any recommendation by you to conduct a further auditprior to certification
B. Cancel the production of the audit report and instead review the organization's contracts with its clients to determine whether they have permitted the use of lower grade machines
C. Consider the need for a subsequent audit within 4 weeks based on the additional information that has come to light
D. Do nothing. All audits are based on a sample and the sample you took did not include a planned review of the lower grade machines
E. Extend the certification audit duration to create additional time to audit the use of the lower grade machines
F. Raise a nonconformity against 8.1 Operational Planning and Control as the organization has not been open about its processes
G. Verify with the auditee that lower grade machines are used in certain circumstances
Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022 clause 8.1, the organization must plan, implement and control the processes needed to meet the information security requirements, and to implement the actions determined in clause 6.1. The organization must also ensure that the outsourced processes are controlled or influenced.
According to control A.5.24, the organization must establish and maintain an information security incident management process that includes reporting information security events and weaknesses. Therefore, the use of lower grade machines for the secure disposal of confidential documents and media could pose a significant information security risk and a potential breach of contract with the clients. The auditor should respond to this information by:
A. Advising the individual managing the audit programme of any recommendation by you to conduct a further audit prior to certification. This is in accordance with ISO/IEC 27006:2022 clause 7.4.3, which states that the audit team leader shall report to the certification body any situation that may significantly affect the audit conclusions or the certification decision, and propose any necessary changes to the audit plan.
C. Considering the need for a subsequent audit within 4 weeks based on the additional information that has come to light. This is in accordance with ISO/IEC 27006:2022 clause 7.5.2, which states that the audit team leader shall review the audit findings and any other appropriate information collected during the audit to determine the audit conclusions, and to identify any need for a subsequent audit.
G. Verifying with the auditee that lower grade machines are used in certain circumstances. This is in accordance with ISO/IEC 27006:2022 clause 7.4.2, which states that the audit team leader shall ensure that the audit is conducted in accordance with the audit plan, and that any changes to the plan are agreed upon and documented.
The other options are not appropriate responses, as they either ignore the information, exceed the scope of the audit, or prematurely raise a nonconformity without sufficient evidence. For example:
B. Cancelling the production of the audit report and instead reviewing the organization's contracts with its clients to determine whether they have permitted the use of lower grade machines. This is not a suitable response, as it would delay the audit process and the certification decision, and it would involve reviewing documents that are outside the scope of the ISMS audit. The auditor should focus on verifying the information security risk assessment and treatment process, and the information security incident management process, as they relate to the use of lower grade machines.
D. Doing nothing. All audits are based on a sample and the sample you took did not include a planned review of the lower grade machines. This is not a suitable response, as it would disregard a significant information security risk and a potential nonconformity that could affect the audit conclusions and the certification decision. The auditor should follow up on the information provided by the employee and verify its validity and impact.
E. Extending the certification audit duration to create additional time to audit the use of the lower grade machines. This is not a suitable response, as it would disrupt the audit schedule and the availability of the audit team and the auditee. The auditor should report the situation to the certification body and propose any necessary changes to the audit plan, such as conducting a subsequent audit.
F. Raising a nonconformity against 8.1 Operational Planning and Control as the organization has not been open about its processes. This is not a suitable response, as it would be based on a single source of information that has not been verified or corroborated. The auditor should collect sufficient and appropriate audit evidence to support any nonconformity, and should also consider the root cause and the severity of the nonconformity.
References:
ISO/IEC 27001:2022, clauses 8.1 and Annex A control A.5.24
ISO/IEC 27006:2022, clauses 7.4.2, 7.4.3, and 7.5.2
[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 18-19, 23-24 A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit ISO 27001 - Annex A.16: Information Security Incident Management

NEW QUESTION: 102
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services. You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.
To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.
Select three options for the audit evidence you need to find to verify the scope of the ISMS.
A. The auditee has identified the resident's needs and expectations on the facility and environmental safety
B. The auditee has ISO 9001 certification
C. The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling
D. The auditee has identified the resident's needs and expectations on how they should protect the resident's personal data
E. The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment
F. The auditee has identified the resident's needs and expectations on healthcare medical treatment services
G. The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located
H. The auditee is considering the purchase of a healthcare monitoring app from an external software company
Answer: (SHOW ANSWER)

According to ISO 27001:2022 clause 4.3, the organisation shall determine the scope of the information security management system (ISMS) by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organisations12 In this case, the ISMS scope covers an outsourced data center that hosts the artificial intelligence (AI) cloud server for healthcare monitoring and analysis of the residents' data. Therefore, the audit evidence you need to find to verify the scope of the ISMS should include:

* The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to comply with the relevant laws and regulations regarding the quality, safety, and privacy of healthcare services and patient data12
* The auditee has identified the resident's needs and expectations on how they should protect the resident' s personal data. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to ensure the confidentiality, integrity, and availability of the resident's personal data that is collected, processed, and stored by the electronic wristband and the AI cloud server12
* The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located. This is an interface and dependency with another organisation that affects the ISMS scope, as the auditee has to control the externally provided processes, products, and services that are relevant to the ISMS, and to implement appropriate contractual requirements related to information security12 The following options are not relevant or sufficient for verifying the scope of the ISMS:
* The auditee has identified the resident's needs and expectations on the facility and environmental safety. This is an external issue and an interested party requirement, but it does not affect the ISMS scope, as it is not related to information security12
* The auditee has ISO 9001 certification. This is an indication of the auditee's quality management system, but it does not verify the scope of the ISMS, as it is not related to information security12
* The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment. These are external issues and interested party requirements, but they do not affect the ISMS scope, as they are not related to information security12
* The auditee has identified the resident's needs and expectations on healthcare medical treatment services. These are external issues and interested party requirements, but they do not verify the scope of the ISMS, as they are not specific to information security12
* The auditee is considering the purchase of a healthcare monitoring app from an external software company. This is a potential change that may affect the ISMS scope in the future, but it does not verify the current scope of the ISMS, as it is not yet implemented or controlled12 References:

1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 103

Question:

What is the objective of penetration testing in the risk assessment process?

A. To conduct thorough code reviews

B. To identify potential failures in the ICT protection schemes

C. To physically inspect hardware components

Answer: (SHOW ANSWER)

Comprehensive and Detailed In-Depth Explanation:

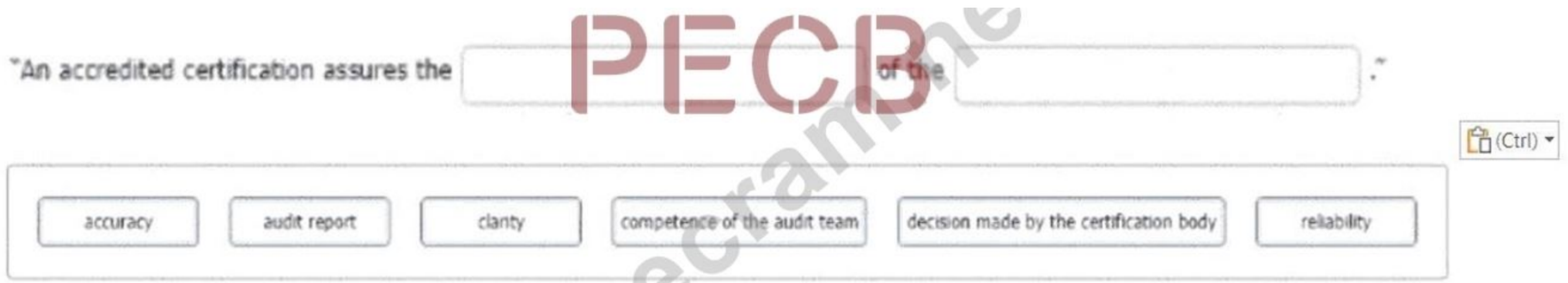
Penetration testing (pen testing) is a simulated cyberattack used to assess security weaknesses in an ICT system.

* B. Identifying failures in ICT protection schemes - Correct answer. The goal of penetration testing is to find vulnerabilities in networks, applications, and systems before attackers can exploit them. This aligns with ISO/IEC 27001:2022 Annex A Control A.8.16 (Monitoring Activities) and A.8.8 (Management of Technical Vulnerabilities).
* A. Code reviews are not the primary goal of pen testing; static analysis tools are used for code security.
* C. Physical inspections relate to hardware security audits, which are separate from penetration testing.

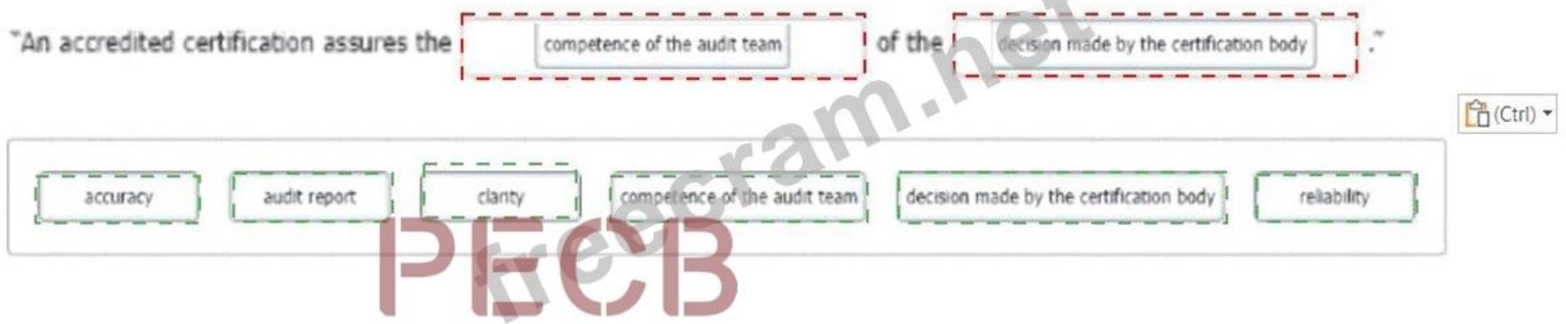
NEW QUESTION: 104

Select the words that best complete the sentence:

To complete the sentence with the word(s) click on the blank section you want to complete so that it is highlighted in red, and then click on the application text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.



Answer:



Explanation:
competence of the audit team and decision made by the certification body According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, an accredited certification means that the certification body has been evaluated by an accreditation body against recognized standards to demonstrate its competence, impartiality and performance capability1. Therefore, an accredited certification assures the competence of the audit team that conducts the audit in accordance with ISO 19011 and ISO/IEC 27001:2022, and the decision made by the certification body that grants or maintains the certification based on the audit evidence and findings2. References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 105
Scenario 1
Fintive is a distinguished security provider specializing in online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies operating online that seek to improve their information security, prevent fraud, and protect user information such as personally identifiable information (PII).
Fintive bases its decision-making and operational processes on previous cases, gathering customer data, classifying them according to the case, and analyzing them.
Initially, Fintive required a large number of employees to be able to conduct such complex analyses.
However, as technology advanced, the company recognized an opportunity to implement a modern tool - a chatbot - to achieve pattern analyses aimed at preventing fraud in real time. This tool would also assist in improving customer service.
The initial idea was communicated to the software development team, who supported the initiative and were assigned to work on the project. They began integrating the chatbot into the existing system and set an objective regarding the chatbot, which was to answer 85% of all chat queries.
After successfully integrating the chatbot, the company released it for customer use. However, the chatbot exhibited several issues. Due to insufficient testing and a lack of sample data provided during the training phase - when it was supposed to learn the query pattern - the chatbot failed to effectively address user queries. Additionally, it sent random files to users when it encountered invalid inputs, such as unusual patterns of dots and special characters.

Consequently, the chatbot could not effectively answer customer queries, overwhelming traditional customer support and preventing them from assisting customers with their requests.
Recognizing the potential risks, Fintive decided to implement a set of new controls. The measures included enabling comprehensive audit logging, configuring automated alert systems to flag unusual activities, performing periodic access reviews, and monitoring system behavior for anomalies. The objective was to identify unauthorized access, errors, or suspicious activities in a timely manner, ensuring that any potential issues could be quickly recognized and investigated before causing significant harm.
Question
Based on Scenario 1, what type of control did Fintive implement in response to the identified issues?
A. Preventive
B. Detective
C. Corrective
Answer: B (LEAVE A REPLY)
From Exact Extract:
1. Definition of control types (ISO-aligned understanding)
In information security management:
* Preventive controls are designed to prevent an incident from occurring.
* Detective controls are designed to identify and detect incidents or anomalies after or as they occur.
* Corrective controls are designed to correct issues after detection.
2. Analysis of the controls implemented by Fintive
The scenario explicitly states that Fintive implemented the following controls:
* Comprehensive audit logging
* Automated alert systems to flag unusual activities
* Periodic access reviews
* Monitoring system behavior for anomalies
All of these controls are designed to:
* Detect unauthorized access
* Detect errors
* Detect suspicious activities
* Enable investigation after detection
This aligns directly with detective controls, not preventive or corrective.
3. ISO/IEC 27002:2022 - Exact control alignment
The controls implemented correspond to Annex A technological and organisational detective controls, including:
* A.8.15 - Logging
Logging enables the detection and investigation of security events.
* A.8.16 - Monitoring activities
Monitoring is used to detect anomalous behaviour and potential security incidents.
* A.5.18 - Access rights (periodic reviews)
Access reviews detect inappropriate or excessive access.
These controls do not prevent the chatbot from malfunctioning, nor do they directly fix it - they detect issues so that action can be taken.
4. Why the other options are incorrect
* A. Preventive - IncorrectPreventive controls would include secure coding practices, input validation, sandboxing, or improved testing before release. These were not the controls described.
* C. Corrective - IncorrectCorrective controls would involve fixing the chatbot logic, retraining the model, or disabling unsafe features. The scenario explicitly focuses on detection and monitoring, not correction.
Auditor Conclusion

Fintive implemented detective controls to identify unauthorized access, errors, and suspicious activity arising from the chatbot's behaviour. This is consistent with ISO/IEC 27001:2022 risk treatment and monitoring requirements.

NEW QUESTION: 106
You are an experienced ISMS audit team leader guiding an auditor in training. You are testing her understanding of follow-up audits by asking her a series of questions to which the answer is either "true* or 'false'. Which four of the following questions should the answer be true"'
A. A follow-up audit may be carried out where nonconformities are major
B. A follow-up audit may be carried out where nonconformities are minor
C. The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified
D. The outcome of a follow-up audit could lower a major nonconformity to minor status
E. The outcome of a follow-up audit could be a recommendabon to suspend the client's certification
F. The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client
G. A follow-up audit is required in all instances where nonconformities have been identified
H. A follow-up audit is required only in instances where a major nonconformity has been identified
Answer: (SHOW ANSWER)
* A follow-up audit may be carried out where nonconformities are major. This is true because a major nonconformity is a situation that raises significant doubt about the ability of the organization's management system to achieve its intended results, and therefore requires immediate corrective action. A follow-up audit is necessary to verify the effectiveness of the corrective action and the conformity of the management system12.
* A follow-up audit may be carried out where nonconformities are minor. This is true because a minor nonconformity is a situation that does not affect the capability of the management system to achieve its intended results, but represents a deviation from the specified requirements. A follow-up audit may be conducted to check the implementation of the corrective action and the improvement of the management system12.
* The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified. This is true because the top management is responsible for ensuring the effectiveness and continual improvement of the management system, and the audit team leader is accountable for the audit process and the audit conclusions. The follow-up audit report should provide them with objective evidence of the status of the nonconformities and the corrective actions taken by the auditee13.
* The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client. This is true because the individual managing the audit programme is responsible for planning, implementing, monitoring and reviewing the audit activities, and the audit client is the organization or person requesting an audit. The follow-up audit report should inform them of the results of the follow-up audit and any changes in the certification status of the auditee13.
References :=
* ISO 19011:2022 Guidelines for auditing management systems
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
Which option below is NOT a role of the audit team leader?
A. Preventing and solving conflict during the audit
B. Setting up an ethics committee
C. Preparing and explaining the audit conclusions
Answer: (SHOW ANSWER)

The role of the audit team leader does not include setting up an ethics committee. The primary responsibilities of the audit team leader include planning the audit, directing the activities of the audit team, ensuring compliance with the auditing standards, managing conflicts that arise during the audit, and presenting audit conclusions.
References: ISO 19011:2018 Guidelines for auditing management systems

NEW QUESTION: 108
You are an experienced ISMS audit team leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-Do- Check-Act cycle in respect of the operation of the information security management system.
You do this by asking him to select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

Explanation:
* Review is the third stage of the Plan-Do-Check-Act (PDCA) cycle, which is a four-step model for implementing and improving an information security management system (ISMS) according to ISO /IEC 27001:202212. Review involves assessing and measuring the performance of the ISMS against the established policies, objectives, and criteria12.

* Assess is the verb that describes the action of reviewing the ISMS. Assess means to evaluate, analyze, or measure something in a systematic and objective manner3. Assessing the ISMS involves collecting and verifying audit evidence, identifying strengths and weaknesses, and determining the degree of conformity or nonconformity12.
* Regular is the adjective that describes the frequency or interval of reviewing the ISMS. Regular means occurring or done at fixed or uniform intervals4. Reviewing the ISMS at regular intervals means conducting internal audits and management reviews periodically, such as annually, quarterly, or monthly, depending on the needs and risks of the organization12.
* Suitability is one of the attributes that describes the quality or outcome of reviewing the ISMS. Suitability means being appropriate or fitting for a particular purpose, person, or situation5. Reviewing the ISMS for suitability means ensuring that it is aligned with the organization's strategic direction, business objectives, and information security requirements12.
References :=
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* Assess | Definition of Assess by Merriam-Webster
* Regular | Definition of Regular by Merriam-Webster
* Suitability | Definition of Suitability by Merriam-Webster

NEW QUESTION: 109
When an organisation needs to determine the resources required for the internal audit programme, which one of the following issues does not impact on the achievement of its intended results?
A. Availability of competent auditors and technical experts.
B. Access by the audit program manager to the competence records of the Information Security Management System manager.
C. Availability of the necessary documented information.
D. Impact of different time zones.
Answer: (SHOW ANSWER)
While competence is important for an effective ISMS, the specific competence records of the ISMS manager are less relevant when determining resources for the internal audit program. The focus should be on resources directly related to the audit process itself. Here's why the other options matter:
*A. Availability of competent auditors and technical experts: Crucial for conducting thorough audits and accurately assessing the ISMS.
*C. Availability of the necessary documented information: Essential for auditors to review policies, procedures, and records related to the ISMS.
*D. Impact of different time zones: Can affect scheduling, coordination, and communication during the audit, potentially requiring additional resources.
References:
*ISO/IEC 27001:2022, Section 9.2 (Internal Audit): Emphasizes the need for competent auditors and emphasizes planning the audit program.
*PECB Candidate Handbook, ISO/IEC 27001 Lead Auditor: Outlines the importance of having sufficient and appropriate resources for the internal audit program.

NEW QUESTION: 110

Scenario 6: Sinvestment is an insurance company that offers home, commercial, and life insurance. The company was founded in North Carolina, but have recently expanded in other locations, including Europe and Africa.
Sinvestment is committed to complying with laws and regulations applicable to their industry and preventing any information security incident. They have implemented an ISMS based on ISO/IEC 27001 and have applied for ISO/IEC 27001 certification.
Two auditors were assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment. they started the audit activities. First, they reviewed the documentation required by the standard, including the declaration of the ISMS scope, information security policies, and internal audits reports. The review process was not easy because, although Sinvestment stated that they had a documentation procedure in place, not all documents had the same format.
Then, the audit team conducted several interviews with Sinvestment's top management to understand their role in the ISMS implementation. All activities of the stage 1 audit were performed remotely, except the review of documented information, which took place on-site, as requested by Sinvestment.
During this stage, the auditors found out that there was no documentation related to information security training and awareness program. When asked, Sinvestment's representatives stated that the company has provided information security training sessions to all employees. Stage 1 audit gave the audit team a general understanding of Sinvestment's operations and ISMS.
The stage 2 audit was conducted three weeks after stage 1 audit. The audit team observed that the marketing department (which was not included in the audit scope) had no procedures in place to control employees' access rights. Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the information security policy of the company, the issue was included in the audit report. In addition, during stage 2 audit, the audit team observed that Sinvestment did not record logs of user activities.
The procedures of the company stated that "Logs recording user activities should be retained and regularly reviewed," yet the company did not present any evidence of the implementation of such procedure.
During all audit activities, the auditors used observation, interviews, documented information review, analysis, and technical verification to collect information and evidence. All the audit findings during stages 1 and 2 were analyzed and the audit team decided to issue a positive recommendation for certification.
Based on scenario 6, during stage 1 audit, the auditor found out that some documents regarding the ISMS had different format. What should the auditor do in this case?

Freepraniet

A. Verify if the documented information has the appropriate format and is in accordance with the company's documentation procedure since this is a requirement of the standard
B. Verify only if the information required by the standard is documented without taking into account the format since this is not a requirement of the standard
C. Document this observation as an issue that should be verified during stage 2 audit
Answer: (SHOW ANSWER)
The auditor should verify if the information required by the standard is documented, without necessarily focusing on the format, as long as the content meets the requirements of the standard. ISO/IEC 27001 does not mandate a specific format for documentation, only that necessary information is appropriately documented, maintained, and controlled.
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

NEW QUESTION: 111
You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.
The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.
Select three options that relate to ISO/IEC 27001:2022's requirements regarding external providers.

A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
E. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
F. I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest
Answer: (SHOW ANSWER)
* A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12
* B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12
* E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12
* F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO 27001:
2022:
* C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12
* D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12
* G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12
* H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 112

Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.
Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments.
Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.
During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC
27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.
Based on the scenario above, answer the following question:
Question:
Is questioning the independence of the internal auditor important given the inconsistencies found in the internal audit report?
A. No, internal auditors should only be independent when a surveillance audit relies on their findings
B. No, internal auditors cannot be independent since they have an advisory role
C. Yes, internal auditors must be independent of the audited activities
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* ISO/IEC 27001:2022 Clause 9.2.2 requires internal auditors to be independent of the activities they audit.
* Inconsistencies in the internal audit report raise valid concerns about independence.
* A. Incorrect:
* Internal auditors must always be independent, not just for surveillance audits.
* B. Incorrect:
* Internal auditors have a compliance role, not just an advisory role.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2.2 (Internal Auditor Independence)

NEW QUESTION: 113
Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.
Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.

To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:
*How are responsibilities for IT and IT controls defined and assigned?
*How does Data Grid Inc. assess whether the controls have achieved the desired results?
*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?
*Are firewall-related controls implemented?
Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.
The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.
Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.
Based on this scenario, answer the following question:
Based on scenario 5, the audit team assessed the ISMS as a whole, rather than assessing the effectiveness and conformity of each process. Is this acceptable?
A. Yes, due to time constraints for the audit completion, the audit team must obtain absolute assurance by assessing the ISMS as a whole
B. No, the audit team should obtain assurance that the ISMS conforms to the standard requirements by assessing each process
C. Yes, if the audit team has obtained a reasonable assurance that helps them evaluate the ISMS conformity
Answer: C (LEAVE A REPLY)
Yes, assessing the ISMS as a whole can be acceptable if the audit team obtains reasonable assurance that the system conforms to the standard requirements. The approach taken by the audit team must still ensure that all significant aspects of the ISMS are evaluated adequately, and if this is achieved through a holistic assessment, it is considered sufficient.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 114
You are an experienced ISMS audit team leader conducting a third-party surveillance audit of an internet services provider. You are reviewing the organization's risk assessment processes for conformity with ISO /IEC 27001:2022.
Which three of the following audit findings would prompt you to raise a nonconformity report?
A. Both systems contain additional information security risks which are not associated with preserving the confidentiality, integrity and accessibility of information
B. The organisation is treating information security risks in the order in which they are identified
C. The organisation's information security risk assessment process suggests each risk is allocated a risk owner
D. The organisation has not used RAG (Red, Amber, Green) to classify its' information security risks.
Instead, it has used a smiling emoji, a neutral face emoji and a sad face emoji
E. The organisation's risk assessment criteria have not been reviewed and approved by top management
F. The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
G. The organisation has assessed the probability of all of its information security risks as either 0%, 25%, 50%, 75% or 100%
H. There is a different system in place for assessing operational information security risks and for assessing strategic information security risks
Answer: (SHOW ANSWER)
The three audit findings that would prompt you to raise a nonconformity report are:
*The organisation is treating information security risks in the order in which they are identified
*The organisation's risk assessment criteria have not been reviewed and approved by top management
*The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk According to ISO/IEC 27001:2022, clause 6.1.2, the organisation must establish and maintain an information security risk management process that is consistent with the organisation's context and aligned with its overall risk management approach1. This process must include the following steps:

*Establishing the risk assessment criteria, which must be approved by top management and reflect the organisation's risk appetite and objectives2
*Identifying the information security risks, which must consider the assets, threats, vulnerabilities, impacts, and likelihoods3
*Analysing the information security risks, which must determine the levels of risk and compare them with the risk criteria4
*Evaluating the information security risks, which must prioritise the risks and decide whether they need treatment or not5 Therefore, the audit findings B, E, and F indicate that the organisation is not following the required steps of the information security risk management process, and thus are nonconformities with the standard.
The other audit findings are not necessarily nonconformities, as they may be acceptable depending on the organisation's context and justification. For example:
*Audit finding A may be acceptable if the organisation has identified and treated the additional information security risks that are relevant to its scope and objectives, and has documented the rationale for doing so6
*Audit finding C may be acceptable if the organisation has assigned clear roles and responsibilities for the information security risk management process, and has ensured that the risk owners have the authority and competence to manage the risks7
*Audit finding D may be acceptable if the organisation has defined and communicated the meaning and implications of the emoji-based risk classification, and has ensured that it is consistent with the risk criteria and the risk treatment process8
*Audit finding G may be acceptable if the organisation has justified the use of discrete values for the probability of the information security risks, and has ensured that they are realistic and consistent with the risk criteria and the risk analysis method9
*Audit finding H may be acceptable if the organisation has established and maintained different systems for assessing operational and strategic information security risks, and has ensured that they are integrated and aligned with the overall risk management approach and the ISMS objectives10 References: 1: ISO/IEC 27001:2022, 6.1.2; 2: ISO/IEC 27001:2022, 6.1.2 a); 3: ISO/IEC 27001:2022, 6.1.2 b); 4: ISO/IEC 27001:2022, 6.1.2 c); 5: ISO/IEC 27001:2022, 6.1.2 d); 6: ISO/IEC 27001:2022, A.0.2; 7: ISO
/IEC 27001:2022, 5.3; 8: ISO/IEC 27001:2022, 6.1.2 a) 2); 9: ISO/IEC 27001:2022, 6.1.2 c) 2); 10: ISO/IEC
27001:2022, 6.1.2 a) 1); : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC
27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; :
ISO/IEC 27001:2022; : ISO/IEC 27001:2022

NEW QUESTION: 115
Question
During a certification audit at Company X, the audit team leader noticed that some HR processes are excluded from the audit scope. However, these processes are included in the company's ISMS scope.
Is this acceptable?
A. Yes, the audit scope can be narrower than the ISMS scope, provided it aligns with the audit program and objectives.
B. No, all processes listed in the ISMS scope must be audited.
C. Yes, only IT-related processes must be included in the audit scope.
Answer: (SHOW ANSWER)
The correct answer is No, all processes listed in the ISMS scope must be audited, because the audit scope for certification must be consistent with the ISMS scope defined by the organization. ISO/IEC 27001 requires that the certification audit assess conformity of the entire ISMS as defined by its scope, not a selective subset of processes.
If HR processes are included in the ISMS scope, they are considered relevant to information security, for example through access management, onboarding and offboarding, training, and disciplinary procedures.
Excluding such processes from the audit would result in incomplete coverage and undermine the validity of the certification decision.
Option A is incorrect because while audit programs and objectives influence audit planning, they cannot override the requirement to audit the full ISMS scope. The audit scope cannot be narrower than the ISMS scope for a certification audit. Option C is incorrect because ISO/IEC 27001 applies to people, processes, and technology, not only IT-related processes.
ISO/IEC 17021-1 requires certification bodies to ensure that audits cover all elements of the management system within scope. Therefore, excluding HR processes that are part of the ISMS scope is not acceptable.

NEW QUESTION: 116
Scenario 8: Tessa. Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.
Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organization's security controls and its risk tolerance in accurately characterizing the risk level within an organization On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting They analyzed one of Michael s findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organization's daily operations, which he believed was caused by one of the organization's IT technicians As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit.
During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.
Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.
Based on the scenario above, answer the following question:
Question:
The audit team did not accept Clastus's additional information because they had already made the certification recommendation. Is this acceptable?
A. Yes, once the audit team decides on a certification recommendation, they cannot accept any additional information
B. No, the auditee can provide additional information if they disagree with the certification recommendation
C. No, the auditor should not consider revisions that resulted from discussions with the auditee in the certification recommendation decision
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* ISO 19011:2018 (Guidelines for Auditing) requires auditors to consider all relevant evidence before making a final recommendation.
* Clastus has the right to present additional evidence if they disagree with findings.
* A. Incorrect:
* Certification recommendations should remain open to valid new evidence until officially finalized.
* C. Incorrect:
* Auditors must consider revisions if they provide relevant clarification or evidence.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.6.3 (Handling Disputes and Additional Evidence in Audits)

NEW QUESTION: 117
Which is the glue that ties the triad together
A. Process
B. People
C. Collaboration
D. Technology
Answer: (SHOW ANSWER)
The triad refers to the three elements of information security: confidentiality, integrity and availability3. Technology is the glue that ties the triad together, as it provides the means to implement various controls and measures to protect information from unauthorized access, modification or loss3. References: ISO
/IEC 27001:2022 Lead Auditor Training Course - BSI

NEW QUESTION: 118
Which option below about the ISMS scope is correct?
A. ISMS scope should be available as documented information
B. ISMS scope should ensure continual improvement

C. ISMS scope should be compatible with the strategic orientation of the organization
Answer: (SHOW ANSWER)
According to ISO/IEC 27001, the scope of an ISMS must be defined and documented. This documentation should include the boundaries and applicability of the information security management system, which helps in defining what information, locations, and assets are covered under the ISMS.
References: ISO/IEC 27001:2013 Standard, Clause 4.3 (Determining the scope of the information security management system)

NEW QUESTION: 119
Question
Factors such as costs related to nonconformities or penalties in case of failure to comply with legal and contractual obligations are evaluated during the definition of which of the following?
A. Materiality
B. Audit risks
C. Reasonable assurance
Answer: (SHOW ANSWER)
The correct answer is Materiality, because materiality involves evaluating the significance and potential impact of issues identified during an audit, including financial, legal, contractual, and reputational consequences. In auditing, materiality helps determine which matters are important enough to influence audit conclusions or stakeholder decisions.
When defining materiality, auditors consider factors such as the cost of nonconformities, potential regulatory penalties, contractual breaches, and the broader business impact of noncompliance. For an ISO/IEC 27001 audit, this may include assessing whether failures in information security controls could lead to fines under data protection laws, loss of customer trust, or breach of service-level agreements. These considerations help auditors decide where to focus audit effort and how to prioritize findings.
Option B is incorrect because audit risk relates to the risk that auditors may reach incorrect conclusions due to inherent, control, or detection risks. While costs and penalties may influence risk assessment, they are not evaluated specifically when defining audit risk. Option C is incorrect because reasonable assurance refers to the level of confidence an audit can provide, not the evaluation of financial or legal impacts.
ISO 19011 supports the use of materiality concepts to ensure audits focus on issues that matter most to the organization and interested parties. Therefore, evaluating costs and penalties is directly linked to defining materiality.

NEW QUESTION: 120

Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.

Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments.

Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.

During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC

27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.

Based on the scenario above, answer the following question:

Question:

Which of the options below does an internal audit program NOT allow?

A. Verification of the effectiveness of corrective actions

B. The reduction of manual audit tasks

C. The prevention of nonconformities

Answer: (SHOW ANSWER)

Comprehensive and Detailed In-Depth Explanation:

* C. Correct Answer:

* Internal audits detect nonconformities but do not actively prevent them.

* A. Incorrect:

* Internal audits verify corrective actions.

* B. Incorrect:

* Technology can reduce manual tasks in internal audits.

Relevant Standard Reference:

* ISO 19011:2018 Clause 6.4.7 (Audit Program Limitations)

Freecram.net

NEW QUESTION: 121
Which two of the following are valid audit conclusions?
A. ISMS induction training does not provide guidance on malware prevention
B. The risk register had not been updated since June 202X
C. Corrective action was outstanding for two internal audits
D. The ISMS policy has been effectively communicated to the organisation
E. The organisation's ISMS objectives meet the requirements of ISO/IEC 27001:2022
F. The schedule of applicability was based on the 2013 edition of ISO/IEC 27001, not the 2022 edition
Answer: (SHOW ANSWER)
The two statements that are valid audit conclusions are:
*The ISMS policy has been effectively communicated to the organisation
*The organisation's ISMS objectives meet the requirements of ISO/IEC 27001:2022 According to ISO 19011:2018, an audit conclusion is the outcome of an audit, provided by the audit team after considering the audit objectives and all audit findings1. An audit conclusion can be positive or negative, depending on whether the audit criteria are fulfilled or not. An audit conclusion can also include recommendations for improvement or recognition of good practices.
The statements D and E are valid audit conclusions, because they express the outcome of the audit based on the audit criteria and findings. For example:
*Statement D is a positive audit conclusion, because it indicates that the organisation has fulfilled the requirement of clause 5.2.2 of ISO/IEC 27001:2022, which states that the ISMS policy must be communicated within the organisation and to relevant interested parties2. The audit team must have obtained sufficient and appropriate audit evidence to support this conclusion, such as records of communication, awareness activities, feedback, etc.
*Statement E is a positive audit conclusion, because it indicates that the organisation has fulfilled the requirement of clause 6.2 of ISO/IEC 27001:2022, which states that the organisation must establish ISMS objectives that are consistent with the ISMS policy and relevant to the information security risks3. The audit team must have obtained sufficient and appropriate audit evidence to support this conclusion, such as records of objective setting, risk assessment, alignment with policy, etc.
The other statements are not valid audit conclusions, because they do not express the outcome of the audit based on the audit criteria and findings. They are rather examples of audit findings, which are the results of the evaluation of the collected audit evidence against the audit criteria4. Audit findings can indicate either conformity or nonconformity with the audit criteria, or opportunities for improvement. For example:
*Statement A is a negative audit finding, because it indicates a nonconformity with the requirement of clause
7.2.2 of ISO/IEC 27001:2022, which states that the organisation must provide information security awareness education and training to persons under its control5. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement B is a negative audit finding, because it indicates a nonconformity with the requirement of clause
6.1.2 of ISO/IEC 27001:2022, which states that the organisation must maintain and review the information security risk assessment at planned intervals or when significant changes occur6. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement C is a negative audit finding, because it indicates a nonconformity with the requirement of clause
10.1 of ISO/IEC 27001:2022, which states that the organisation must take action to eliminate the causes of nonconformities and prevent recurrence7. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement F is a negative audit finding, because it indicates a nonconformity with the requirement of clause
6.1.3 of ISO/IEC 27001:2022, which states that the organisation must determine the controls that are necessary to implement the risk treatment plan, and document them in the statement of applicability8. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
References: 1: ISO 19011:2018, 3.15; 2: ISO/IEC 27001:2022, 5.2.2; 3: ISO/IEC 27001:2022, 6.2; 4: ISO
19011:2018, 3.14; 5: ISO/IEC 27001:2022, 7.2.2; 6: ISO/IEC 27001:2022, 6.1.2; 7: ISO/IEC 27001:2022,
10.1; 8: ISO/IEC 27001:2022, 6.1.3; : ISO 19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO
19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
Scenario 3: NightCore is a multinational technology company based in the United States that focuses on e-commerce, cloud computing, digital streaming, and artificial intelligence. After having an information security management system (ISMS) implemented for over 8 months, they contracted a certification body to conduct a third party audit in order to get certified against ISO/IEC 27001.
The certification body set up a team of seven auditors. Jack, the most experienced auditor, was assigned as the audit team leader. Over the years, he received many well known certifications, such as the ISO/IEC 27001 Lead Auditor, CISA, CISSP, and CISM.
Jack conducted thorough analyses on each phase of the ISMS audit, by studying and evaluating every information security requirement and control that was implemented by NightCore. During stage 2 audit. Jack detected several nonconformities.
After comparing the number of purchased invoices for software licenses with the software inventory, Jack found out that the company has been using the illegal versions of a software for many computers. He decided to ask for an explanation from the top management about this nonconformity and see whether they were aware about this. His next step was to audit NightCore's IT Department. The top management assigned Tom, NightCore's system administrator, to act as a guide and accompany Jack and the audit team toward the inner workings of their system and their digital assets infrastructure.
While interviewing a member of the Department of Finance, the auditors discovered that the company had recently made some unusual large transactions to one of their consultants. After gathering all the necessary details regarding the transactions. Jack decided to directly interview the top management.
When discussing about the first nonconformity, the top management told Jack that they willingly decided to use a copied software over the original one since it was cheaper. Jack explained to the top management of NightCore that using illegal versions of software is against the requirements of ISO/IEC 27001 and the national laws and regulations. However, they seemed to be fine with it.
Several months after the audit, Jack sold some of NightCore's information that he collected during the audit for a huge amount of money to competitors of NightCore.
Based on this scenario, answer the following question:
According to scenario 3, which audit principle has Jack compromised when he sold NightCore's information after the audit?
A. Independence
B. Integrity
C. Confidentiality
Answer: (SHOW ANSWER)
Jack compromised the audit principle of confidentiality by selling NightCore's information after the audit.
Confidentiality ensures that information is accessible only to those authorized to have access and is protected throughout its lifecycle.
References: ISO 19011:2018, Guidelines for auditing management systems, principles of auditing

NEW QUESTION: 123
Which statement below best describes the relationship between information security aspects?
A. Threats exploit vulnerabilities to damage or destroy assets
B. Controls protect assets by reducing threats
C. Risk is a function of vulnerabilities that harm assets
Answer: (SHOW ANSWER)
This statement encapsulates the relationship between threats, vulnerabilities, and assets within the context of information security. Threats are potential causes of an unwanted incident, which may result in harm to a system or organization. Vulnerabilities are weaknesses that can be exploited by threats to cause harm. Assets are valuable resources to an organization that need protection. Therefore, when threats exploit vulnerabilities, they can damage or destroy assets. References: = The explanation is based on the foundational concepts of information security as outlined in ISO/IEC 27001, which includes understanding the interplay between threats, vulnerabilities, and assets as part of an information security management system (ISMS)

NEW QUESTION: 124

The following are the guidelines to protect your password, except:
A. Don't use the same password for various company system security access
B. Do not share passwords with anyone
C. For easy recall, use the same password for company and personal accounts
D. Change a temporary password on first log-on
Answer: (SHOW ANSWER)
The following are guidelines to protect your password, except for easy recall use the same password for company and personal accounts; do not share passwords with anyone. Using the same password for company and personal accounts is not a guideline to protect your password, as it increases the risk of compromising your password if one of your accounts is hacked or breached. You should use different and unique passwords for each account, and change them regularly. Sharing passwords with anyone is not a guideline to protect your password, as it reduces the security and accountability of your password. You should keep your password confidential and never disclose it to anyone, even if they claim to be authorized or trustworthy. Don't use the same password for various company system security access is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if one of the systems is compromised or breached. You should use different and complex passwords for each system, and follow the password policies and standards of the organization. Change a temporary password on first log-on is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if the temporary password is intercepted or leaked. You should change the temporary password to a personal and secure password as soon as possible, and avoid using default or predictable passwords.
References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 43. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

NEW QUESTION: 125
Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.
Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.
To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:
*How are responsibilities for IT and IT controls defined and assigned?
*How does Data Grid Inc. assess whether the controls have achieved the desired results?
*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?
*Are firewall-related controls implemented?
Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.
The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.
Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.
Based on this scenario, answer the following question:
Data Grid Inc. is responsible for all the actions below, EXCEPT:
A. Specifying the audit criteria
B. Appointing the audit team
C. Defining the audit scope
Answer: (SHOW ANSWER)
In the context of ISO/IEC 27001 audits, the audit team is appointed by the certification body, not by the organization being audited. Data Grid Inc. is responsible for specifying the audit criteria and defining the audit scope, but not for appointing the audit team.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 126
Review the following statements and determine which two are false:
A. Conducting a technology check in advance of a virtual audit can improve the effectiveness and efficiency of the audit
B. During a virtual audit, auditees participating in interviews are strongly recommended to keep their webcam enabled
C. The number of days assigned to a third-party audit is determined by the auditee's availability
D. Due to confidentiality and security concerns, screen sharing during a virtual audit is one method by which the audit team can review the auditee's documentation
E. The selection of onsite, virtual or combination audits should take into consideration historical performance and previous audit results
F. Auditors approved for conducting onsite audits do not require additional training for virtual audits, as there are no significant differences in the skillset required
Answer: (SHOW ANSWER)
The number of days assigned to a third-party audit is not determined by the auditee's availability, but by the audit program, which considers the audit scope, objectives, criteria, risks, and resources12. The auditee's availability is only one factor that affects the audit planning and scheduling, but not the audit duration3.
Auditors approved for conducting onsite audits do require additional training for virtual audits, as there are significant differences in the skillset required. Virtual audits pose different challenges and opportunities than onsite audits, such as communication, technology, security, and evidence collection4 . Auditors need to be familiar with the tools and techniques for conducting remote audits, as well as the ethical and professional behavior expected in a virtual environment . References:
* PECB Candidate Handbook - ISO 27001 Lead Auditor, page 18
* ISO 19011:2018, Guidelines for auditing management systems, clause 5.3.2
* ISO 19011:2018, Guidelines for auditing management systems, clause 6.3.1
* Deloitte - Conducting a Virtual Internal Audit, page 1
* [A Guide to Conducting Effective and Efficient Remote Audits], page 1
* [ISO 19011:2018, Guidelines for auditing management systems], clause 7.2.3
* [Remote Auditing Best Practices & Checklist for Regulatory Compliance], page 1

NEW QUESTION: 127
An auditor of organisation A performs an audit of supplier B. Which two of the following actions is likely to represent a breach of confidentiality by the auditor after having identified findings in B's information security management system?
A. Shares the findings with other relevant managers in A
B. Shares the findings with B's Information Security Manager
C. Shares the findings with A's supplier evaluation team
D. Shares the findings with B's other customers
E. Shares the findings with B's certification body
F. Shares the findings with other relevant managers in B
Answer: (SHOW ANSWER)
According to the PECB Candidate Handbook1, one of the principles of auditing is confidentiality, which means that auditors should respect the confidentiality of information obtained during the audit and not disclose it to unauthorized parties. The handbook also states that auditors should only report audit results to those who have a legitimate need to know, such as the client, the auditee, and the certification body.
Therefore, sharing the findings with other relevant managers in A or B's other customers would be a breach of confidentiality, as they are not directly involved in the audit process or the information security management system of B. Sharing the findings with B's Information Security Manager or other relevant managers in B would be appropriate, as they are part of the auditee organization and responsible for the implementation and improvement of the ISMS. Sharing the findings with A's supplier evaluation team or B's certification body would also be acceptable, as they have a legitimate need to know the audit results for the purpose of supplier selection or certification, respectively. References: 1: PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 7-8.

NEW QUESTION: 128
Select the words that best complete the sentence:

Select the words that best complete the sentence:

"The purpose of a third-party audit is to _____ an organisation's _____ to inform _____ decision."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

approve | inspect | a compliance | an accreditation | products | evaluate | management system | a certification | processes

Answer:

Explanation:

A third-party audit is an independent assessment of an organisation's management system by an external auditor, who is not affiliated with the organisation or its customers. The auditor verifies that the management system meets the requirements of a specific standard, such as ISO 27001, and evaluates its effectiveness and performance. The auditor also identifies any strengths, weaknesses, opportunities, or risks of the management system, and provides recommendations for improvement. The purpose of a third-party audit is to provide an objective and impartial evaluation of the organisation's management system, and to inform a certification decision by a certification body. A certification body is an organisation that grants a certificate of conformity to the organisation, after reviewing the audit report and evidence, and confirming that the management system meets the certification criteria. A certification decision is the outcome of the certification process, which can be positive (granting, maintaining, renewing, or expanding the scope of certification) or negative (suspending, withdrawing, or reducing the scope of certification). References:

* PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
* ISO 19011:2018 - Guidelines for auditing management systems
* The ISO 27001 audit process | ISMS.online

NEW QUESTION: 129

Scenario 6: Sinvestment is an insurance company that offers home, commercial, and life insurance. The company was founded in North Carolina, but have recently expanded in other locations, including Europe and Africa.

Sinvestment is committed to complying with laws and regulations applicable to their industry and preventing any information security incident. They have implemented an ISMS based on ISO/IEC 27001 and have applied for ISO/IEC 27001 certification.
Two auditors were assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment. they started the audit activities. First, they reviewed the documentation required by the standard, including the declaration of the ISMS scope, information security policies, and internal audits reports. The review process was not easy because, although Sinvestment stated that they had a documentation procedure in place, not all documents had the same format.
Then, the audit team conducted several interviews with Sinvestment's top management to understand their role in the ISMS implementation. All activities of the stage 1 audit were performed remotely, except the review of documented information, which took place on-site, as requested by Sinvestment.
During this stage, the auditors found out that there was no documentation related to information security training and awareness program. When asked, Sinvestment's representatives stated that the company has provided information security training sessions to all employees. Stage 1 audit gave the audit team a general understanding of Sinvestment's operations and ISMS.
The stage 2 audit was conducted three weeks after stage 1 audit. The audit team observed that the marketing department (which was not included in the audit scope) had no procedures in place to control employees' access rights. Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the information security policy of the company, the issue was included in the audit report. In addition, during stage 2 audit, the audit team observed that Sinvestment did not record logs of user activities.
The procedures of the company stated that "Logs recording user activities should be retained and regularly reviewed," yet the company did not present any evidence of the implementation of such procedure.
During all audit activities, the auditors used observation, interviews, documented information review, analysis, and technical verification to collect information and evidence. All the audit findings during stages 1 and 2 were analyzed and the audit team decided to issue a positive recommendation for certification.
According to scenario 6, the marketing department employees were not following the access control policy.
Which option is correct in this case?
A. The marketing department is not included in the audit scope, so the issue should only be communicated to Sinvestment's representatives
B. The employees' access right control is included in Sinvestment's information security policy, so the issue must be communicated to Sinvestment's representatives and included in the audit report
C. Sinvestment is not controlling the employees' access rights, which represents a potential information security risk and should be reported as a major nonconformity
Answer: (SHOW ANSWER)
Even though the marketing department was not included in the audit scope, the issue of employees' access rights control must be communicated to Sinvestment's representatives and included in the audit report because it is part of Sinvestment's information security policy. It reflects on the overall adherence to the ISMS requirements.
References: ISO/IEC 27001:2013, Clause 9.2 (Internal audit)

NEW QUESTION: 130
Select two of the following options that are the responsibility of a legal technical expert on the audit team during a certification audit.
* Evaluating the auditee's legal knowledge
Freecram.net
A. Criticising the organisation's legal compliance issues
B. Debating complex legal points with the auditee
C. Advising on legal checkpoints for the audit team
D. Verifying the legal status of the organisation
E. Meeting the organisation's legal representative
Answer: (SHOW ANSWER)
A legal technical expert (LTE) is a person who provides specific knowledge or expertise related to the legal aspects of the information security management system (ISMS) during a certification audit. The LTE is not an auditor, but a member of the audit team who supports the auditors in collecting and evaluating the audit evidence. The LTE is not responsible for evaluating the auditee's legal knowledge, criticising the organisation' s legal compliance issues, or debating complex legal points with the auditee, as these tasks may be beyond the scope of the audit, or may compromise the objectivity and impartiality of the audit. The LTE is responsible for advising on legal checkpoints for the audit team, such as the applicable legal, regulatory, and contractual requirements, the relevant sources of information, the methods of verification, and the criteria of evaluation.
The LTE is also responsible for verifying the legal status of the organisation, such as the registration, licensing, authorisation, or accreditation of the organisation, and the compliance with the relevant laws and regulations. References:
* What is the role of a technical expert in ISO audit?

* Roles, Responsibilities & Authorities for ISO 27001 5.3
* Guide to Become an ISO 27001 Lead Auditor

NEW QUESTION: 131
Scenario 3: NightCore is a multinational technology company based in the United States that focuses on e-commerce, cloud computing, digital streaming, and artificial intelligence. After having an information security management system (ISMS) implemented for over 8 months, they contracted a certification body to conduct a third party audit in order to get certified against ISO/IEC 27001.
The certification body set up a team of seven auditors. Jack, the most experienced auditor, was assigned as the audit team leader. Over the years, he received many well known certifications, such as the ISO/IEC 27001 Lead Auditor, CISA, CISSP, and CISM.
Jack conducted thorough analyses on each phase of the ISMS audit, by studying and evaluating every information security requirement and control that was implemented by NightCore. During stage 2 audit. Jack detected several nonconformities. After comparing the number of purchased invoices for software licenses with the software inventory, Jack found out that the company has been using the illegal versions of a software for many computers. He decided to ask for an explanation from the top management about this nonconformity and see whether they were aware about this. His next step was to audit NightCore's IT Department. The top management assigned Tom, NightCore's system administrator, to act as a guide and accompany Jack and the audit team toward the inner workings of their system and their digital assets infrastructure.
While interviewing a member of the Department of Finance, the auditors discovered that the company had recently made some unusual large transactions to one of their consultants. After gathering all the necessary details regarding the transactions. Jack decided to directly interview the top management.
When discussing about the first nonconformity, the top management told Jack that they willingly decided to use a copied software over the original one since it was cheaper. Jack explained to the top management of NightCore that using illegal versions of software is against the requirements of ISO/IEC 27001 and the national laws and regulations. However, they seemed to be fine with it.
Several months after the audit, Jack sold some of NightCore's information that he collected during the audit for a huge amount of money to competitors of NightCore.
Based on this scenario, answer the following question:
Based on audit principles, should Jack contact the certification body regarding the second nonconformity?
Refer to scenario 3.
A. Yes, auditors should contact the ethics committee members of the certification body to obtain advice on such situation
B. Yes, auditors should communicate such situations to the certification body; however, the top management should not be informed
C. No, situations that may indicate financial crime are not the focus of an ISMS audit
Answer: (SHOW ANSWER)
Yes, Jack should communicate such situations to the certification body. It is essential for auditors to report potential nonconformities and ethical breaches to the certification body to maintain the integrity and credibility of the audit process, without necessarily informing top management of these steps.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 132
You are an experienced ISMS auditor conducting a third-party surveillance audit at an organisation which offers ICT reclamation services. ICT equipment which companies no longer require is processed by the organisation. It is either recommissioned and reused or is securely destroyed.
You notice two servers on a bench in the corner of the room. Both have stickers on them with the server's name, IP address and admin password. You ask the ICT Manager about them, and he tells you they were part of a shipment received yesterday from a regular customer.
Which one action should you take?
A. Ask the ICT Manager to record an information security incident and initiate the information security incident management process
B. Raise a nonconformity against control 5.31 'Legal, staturary, regulatory and contractual requirements'
C. Record what you have seen in your audit findings, but take no further action
D. Ask the auditee to remove the labels, then carry on with the audit
E. Raise a nonconformity against control 8.20 'network security' (networks and network devices shall be secured, managed and controlled to protect information in systems and applications)
F. Note the audit finding and check the process for dealing with incoming shipments relating to customer IT security
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Scenario 1: Fintive is a distinguished security provider for online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies that operate online and want to improve their information security, prevent fraud, and protect user information such as PII. Fintive centers its decision-making and operating process based on previous cases. They gather customer data, classify them depending on the case, and analyze them. The company needed a large number of employees to be able to conduct such complex analyses. After some years, however, the technology that assists in conducting such analyses advanced as well. Now, Fintive is planning on using a modern tool, a chatbot, to achieve pattern analyses toward preventing fraud in real-time. This tool would also be used to assist in improving customer service.
This initial idea was communicated to the software development team, who supported it and were assigned to work on this project. They began integrating the chatbot on their existing system. In addition, the team set an objective regarding the chatbot which was to answer 85% of all chat queries.
After the successful integration of the chatbot, the company immediately released it to their customers for use.
The chatbot, however, appeared to have some issues.
Due to insufficient testing and lack of samples provided to the chatbot during the training phase, in which it was supposed "to learn" the queries pattern, the chatbot failed to address user queries and provide the right answers. Furthermore, the chatbot sent random files to users when it received invalid inputs such as odd patterns of dots and special characters. Therefore, the chatbot was unable to properly answer customer queries and the traditional customer support was overwhelmed with chat queries and thus was unable to help customers with their requests.
Consequently, Fintive established a software development policy. This policy specified that whether the software is developed in-house or outsourced, it will undergo a black box testing prior to its implementation on operational systems.
Based on this scenario, answer the following question:
The chatbot was supposed "to learn" the queries pattern to address user queries and provide the right answers.
What type of technology enables
this?
A. Artificial intelligence
B. Cloud computing
C. Machine learning
Answer: (SHOW ANSWER)
Machine learning is a subset of artificial intelligence that involves the use of algorithms and statistical models to enable systems to improve their performance on a specific task over time with experience or data, without being explicitly programmed.
In the context of the scenario, machine learning would be the technology that allows the chatbot to learn from patterns in queries to provide the right answers.

NEW QUESTION: 134
Which two of the following options do not participate in a first-party audit?
A. A certification body auditor
B. An audit team from an accreditation body
C. An auditor certified by CQI and IRCA
D. An auditor from a consultancy organisation
E. An auditor trained in the CQI and IRCA scheme
F. An auditor trained in the organization
Answer: (SHOW ANSWER)
A first-party audit is an internal audit in which the organization's own staff or contractors check the conformity and effectiveness of the ISMS. A certification body auditor and an audit team from an accreditation body are external auditors who conduct audits for the purpose of certification or accreditation.
They do not participate in a first-party audit, but rather in a third-party audit. References: First & Second Party Audits - operational services, The ISO 27001 Audit Process | Blog | OneTrust, The ISO 27001 Audit Process | A Beginner's Guide - IAS USA

NEW QUESTION: 135
Question:

Which situation presented below represents a threat?
A. An employee accesses unauthorized files using their legitimate credentials
B. An organization fails to implement multi-factor authentication (MFA) for its cloud services
C. Cyber attackers infiltrated the network by exploiting a zero-day vulnerability in the organization's firewall software
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer - This is a Threat. A cyberattack exploiting a zero-day vulnerability is an active security threat, as it causes harm to the organization.
* A. Employee accessing unauthorized files is a vulnerability (insider risk) rather than an external threat.
* B. Lack of MFA is a security weakness (vulnerability), not a threat.
This aligns with ISO/IEC 27001:2022 Annex A Control A.8.25 (Assessment and Decision on Information Security Events).

NEW QUESTION: 136
You are an experienced ISMS audit team leader. You are providing an introduction to ISO/IEC 27001:2022 to a class of Quality Management System Auditors who are seeking to retrain to enable them to carry out information security management system audits.
You ask them which of the following characteristics of information does an information security management system seek to preserve?
Which three answers should they provide?
A. Clarity
B. Accessibility
C. Completeness
D. Importance
E. Availability
F. Confidentiality
G. Integrity
H. Efficiency
Answer: (SHOW ANSWER)
These three characteristics are the fundamental properties of information security, as defined by the ISO/IEC
27000 standard, which provides the overview and vocabulary of information security, cybersecurity, and privacy protection12. They are also the basis for the information security objectives and controls of the ISO
/IEC 27001 standard, which specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system34. The definitions of these characteristics are as follows12:
*Availability: The property of being accessible and usable upon demand by an authorized entity.
*Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
*Integrity: The property of safeguarding the accuracy and completeness of information and processing methods.
The other characteristics listed in the question, such as clarity, accessibility, completeness, importance, and efficiency, are not directly related to information security, although they may be relevant for other aspects of information management, such as quality, usability, or performance.
References: = 1: ISO/IEC 27000:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection - Overview and vocabulary, clause 32: ISO/IEC 27000:2022 (en), Information security, cybersecurity and privacy protection - Overview and vocabulary13: ISO/IEC
27001:2022 Information technology - Security techniques - Information security management systems - Requirements, clause 6.24: ISO/IEC 27001:2022 (en), Information security, cybersecurity and privacy protection - Information security management systems - Requirements1

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137
Scenario 5: Cobt. an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well- versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organizations internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification Sarah, an experienced auditor, was assigned to the audit Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes Therefore, her initial focus was to gather information on how the company manages its information security risks Sarah contacted Cobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence Moreover, Cobt raised concerns about the audit schedule, stating that it does not properly reflect the recent changes the company made It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the scenario above, answer the following question:
Question:
What type of risk did Cobt identify during the last risk assessment?
A. Inherent risk
B. Control risk
C. Detection risk
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* Detection Risk (Correct Answer) - Detection risk occurs when control mechanisms fail to identify significant defects or errors. Cobt identified that major defects were not detected or prevented by internal controls, making detection risk the correct answer.
* Inherent Risk refers to the likelihood of a security event occurring without considering any controls.
The scenario mentions control failures, not natural risks, so this is incorrect.
* Control Risk is the risk of controls failing to prevent a risk. However, the scenario specifically mentions that the defects were not detected, making detection risk the more precise answer.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 6.1.2 (Information Security Risk Assessment Process)

NEW QUESTION: 138
Which two of the following phrases would apply to "act" in relation to the Plan-Do-Check-Act cycle for a business process?
A. Auditing processes
B. Planning changes
C. Measuring objectives
D. Resetting objectives

E. Achieving improvements
F. Verifying training
Answer: (SHOW ANSWER)
The Act phase of the PDCA cycle is where the organisation takes actions to improve its processes and performance based on the results of the Check phase. This may involve resetting objectives to make them more realistic, achievable or challenging, or implementing changes to address the root causes of problems and achieve the desired outcomes. The Act phase is also where the organisation monitors the effects of the actions taken and evaluates their effectiveness and efficiency. The Act phase is important because it enables the organisation to learn from its experience and continually improve its ISMS. References: What is 'Plan, Do, Check, Act'? A framework for continuous improvement, PDCA in ISO27001 - Free guide to learn | Dr. Erdal Ozkaya, PECB Candidate Handbook ISO 27001 Lead Auditor (page 12)

NEW QUESTION: 139
Scenario 4
SendPay is a financial services company specializing in global money transfers through a network of agents and institutions. As a new company in the market, SendPay aims to deliver top-quality services with its fee- free digital platform, launched last year, enabling clients to send and receive money anytime via smartphones and laptops. At that time, SendPay outsourced software operations to an external team, which also managed the company's technology infrastructure.
Recently, the company applied for ISO/IEC 27001 certification after having an ISMS in place for almost a year.
During the audit, the auditors focused on reviewing SendPay's outsourced operations, specifically looking at the software development and technology infrastructure maintenance handled by the outsourced company.
They followed a structured approach, which included reviewing and evaluating SendPay's processes for monitoring the quality of these outsourced operations. This included verifying if the company met its contractual obligations, ensuring proper governance procedures for engaging outsourced entities, and assessing SendPay's plans in case of expected or unexpected termination of outsourcing agreements.
However, the auditors subtly noted that SendPay's protocols did not fully address contingencies for unanticipated cancellations of outsourcing agreements. Additionally, a technical expert appointed by SendPay assisted the auditors, providing specific knowledge and expertise related to the outsourced operations being audited.
The audit team calculated the number of training hours employees received on ISMS to ensure alignment with established objectives. They also computed the average resolution time of information security incidents based on a sample taken during the audit, which provided valuable insights into SendPay's incident management practices. In addition, the auditors evaluated the reliability of the evidence collected during the audit. They considered several factors influencing the reliability of audit evidence. For example, evidence from surveillance cameras provided more objective proof compared to photos. Timing also played a crucial role in reliability, with mechanisms like transaction recording enhancing the credibility of the evidence.
SendPay uses cloud-based platforms to make its operations more efficient and scalable. However, during the audit, the auditors did not request SendPay to provide an inventory of their cloud activities due to resource limitations, relying instead on SendPay's representations.
Question
Based on Scenario 4, is the involvement of all the parties acceptable during the auditing of the outsourced operations?
A. Yes, the involvement of all the parties is considered acceptable.
B. No, the involvement of the technical expert is not acceptable.
C. No, they should have involved only an observer.
Answer: (SHOW ANSWER)
The involvement of all the parties described in Scenario 4 is acceptable and aligns with ISO 19011:2018 guidance on auditing management systems, making option A the correct answer. ISO 19011 recognizes that audits may involve different participants beyond the audit team, including technical experts, guides, observers, and representatives of the auditee, provided their roles are clearly defined and managed.
In this scenario, a technical expert appointed by SendPay assisted the auditors by providing specific knowledge and expertise related to the outsourced software operations and technology infrastructure. This is explicitly permitted under ISO 19011, which allows the use of technical experts when specialized knowledge is required that the auditors themselves may not fully possess. The technical expert's role is to support the audit team with subject-matter expertise, not to influence audit conclusions or replace auditor judgment.
Option B is incorrect because ISO 19011 does not prohibit the involvement of technical experts. On the contrary, their involvement is encouraged when auditing complex or highly technical areas, such as outsourced IT operations and cloud-based services. Option C is also incorrect because limiting participation to observers would not provide the auditors with the necessary technical insight to effectively evaluate outsourced operations.
As long as the audit team leader maintains control of the audit process and ensures independence and objectivity, the involvement of auditors, auditee representatives, and technical experts is appropriate.
Therefore, the involvement of all the parties in this audit is acceptable under ISO auditing principles.

NEW QUESTION: 140

Question:
A cybersecurity company implemented an access control software that allows only authorized personnel to access sensitive files. Which type of control has the company implemented in this case?

freecram.net

A. Preventive control
B. Detective control
C. Corrective control
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Preventive Control - Correct Answer. Access control software is designed to prevent unauthorized access by enforcing authentication and authorization mechanisms. This aligns with ISO/IEC 27001:
2022 Annex A Control A.5.18 (Access Rights).
* B. Detective controls identify and log unauthorized access attempts, but do not prevent them.
* C. Corrective controls take action after a security event has occurred.

NEW QUESTION: 141
You are an experienced ISMS internal auditor.
You have just completed a scheduled information security audit of your organisation when the IT Manager approaches you and asks for your assistance in the revision of the company's Statement of Applicability.
The IT Manager is attempting to update the ISO/IEC 27001:2013 based Statement of Applicability to a Statement aligned to the 4 control themes present in ISO/IEC 27001:2022 (Organizational controls, People Controls, Physical Controls, Technical Controls).
The IT Manager is happy with their reassignment of controls, with the following exceptions. He asks you which of the four control categories each of the following should appear under.

PECB

How would you respond? Match the control description to the category.

8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected	
7.8 Equipment shall be sited securely and protected	
5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs	
6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises	

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Technological control | People control | Organizational control | Physical control

freecram.net

Answer:

How would you respond? Match the control description to the category.

8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected	Technological control
7.8 Equipment shall be sited securely and protected	Physical control
5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs	Organizational control
6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises	People control

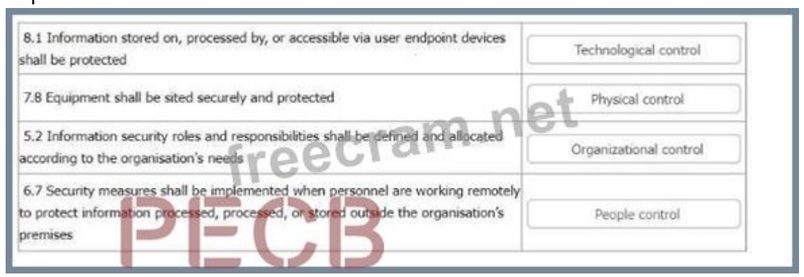
freecram.net

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Technological control | People control | Organizational control | Physical control

PECB

Explanation:



8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected
= Technological control 7.8 Equipment shall be sited securely and protected = Physical control 5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs = Organisational control 6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises = People control According to the web search results from my predefined tool, ISO 27001:2022 has restructured and consolidated the Annex A controls into four categories: organisational, people, physical, and technological12. These categories reflect the different aspects and dimensions of information security, and are aligned with the cybersecurity concepts of identify, protect, detect, respond, and recover3. The controls in each category are as follows4:

* Organisational controls: These are controls that relate to the governance, management, and coordination of information security activities within the organisation. They include controls such as information security policies, roles and responsibilities, risk assessment and treatment, performance evaluation, and improvement.
* People controls: These are controls that relate to the behaviour, awareness, and competence of the people involved in information security, both within and outside the organisation. They include controls such as human resource security, training and awareness, access control, incident management, and business continuity.
* Physical controls: These are controls that relate to the protection of physical assets and environments that store, process, or transmit information. They include controls such as physical security, environmental security, equipment security, and media security.
* Technological controls: These are controls that relate to the use of technology to implement, monitor, and maintain information security. They include controls such as cryptography, network security, system security, application security, and threat intelligence.

Based on these categories, the controls listed in the question can be matched as follows:

* 8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected: This is a technological control, as it involves the use of technology to protect information on devices such as laptops, smartphones, tablets, etc. It may include measures such as encryption, authentication, antivirus, firewall, etc.
* 7.8 Equipment shall be sited securely and protected: This is a physical control, as it involves the protection of physical assets and environments that store, process, or transmit information. It may include measures such as locks, alarms, CCTV, fire suppression, etc.
* 5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs: This is an organisational control, as it involves the governance, management, and coordination of information security activities within the organisation. It may include measures such as defining the authority and accountability of information security personnel, establishing reporting lines and communication channels, assigning tasks and duties, etc.
* 6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises: This is a people control, as it involves the behaviour, awareness, and competence of the people involved in information security, both within and outside the organisation. It may include measures such as providing guidance and training on remote working, enforcing policies and procedures, monitoring and auditing remote activities, etc.
= 1: A Breakdown of ISO 27001:2022 Annex A Controls - BARR Advisory42: ISO 27001:2022 Annex A Controls - What's New? | ISMS.Online13: How many controls are there in ISO 27001:2022? - Strike Graph34: ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A.

NEW QUESTION: 142
The auditor should consider (1)-------when determining the (2)--------
A. (1) Standard requirements. (2) audit criteria
B. (1) Audit risks, (2) audit objectives
C. (1) Penalties related to legal noncompliance, (2) materiality
Answer: (SHOW ANSWER)
The auditor should consider "audit risks" when determining the "audit objectives." Understanding the risks associated with the audit helps define the objectives clearly, ensuring that the audit focuses on the most significant areas of concern, aligns with the audit scope, and adequately addresses the risks identified.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 143
Which three of the following phrases are objectives' in relation to an audit?
A. International Standard
B. Identify opportunities for improvement
C. Confirm the scope of the management system
D. Management policy
E. Complete audit on time
F. Regulatory requirements
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, the audit objectives are defined by the audit client and may include determining the extent of conformity or nonconformity of the audited management system against the audit criteria, evaluating the ability of the audited management system to ensure that the organization meets applicable statutory, regulatory and contractual requirements, identifying potential improvement opportunities for the audited management system, and facilitating continual improvement of the audited management system1. Therefore, these three phrases are examples of objectives in relation to an audit. The other options are not objectives, but rather elements or factors that may influence or affect an audit. For example, an international standard is a source of audit criteria, a management policy is a part of the audited management system, and completing an audit on time is a requirement for an effective audit. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 144
You are an experienced audit team leader guiding an auditor in training, Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.

A. The development and maintenance of an information asset inventory
B. Rules for transferring information within the organisation and to other organisations
C. Confidentiality and nondisclosure agreements
D. How protection against malware is implemented
E. Access to and from the loading bay
F. The conducting of verification checks on personnel
G. Remote working arrangements
H. How information security has been addressed within supplier agreements
I. How the organisation evaluates its exposure to technical vulnerabilities
J. The organisation's business continuity arrangements
K. The organisation's arrangements for information deletion
L. Information security awareness, education and training
M. How access to source code and development tools are managed
N. The operation of the site CCTV and door control systems
O. The organisation's arrangements for maintaining equipment
P. How power and data cables enter the building
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), an organization should select and implement appropriate controls to achieve its information security objectives1. The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS1. The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls2. Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:
* How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems2. This control is related to control A.12.2.1 of ISO/IEC 27002:20132.
* How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures2. This control is related to control A.12.6.1 of ISO/IEC 27002:20132.
* How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or systems that are developed or maintained by the organization or its external providers2. This control is related to control A:14.2.5 of ISO/IEC 27002:20132.
* The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed2. This control is related to control A.11.1.4 of ISO/IEC 27002:20132.
The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance of an information asset inventory (related to control A.
8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION: 145
Scenario 1
Fintive is a distinguished security provider specializing in online payments and protection solutions. Founded in 1999 by Thomas Fin in San Jose, California, Fintive offers services to companies operating online that seek to improve their information security, prevent fraud, and protect user information such as personally identifiable information (PII).

Fintive bases its decision-making and operational processes on previous cases, gathering customer data, classifying them according to the case, and analyzing them.
Initially, Fintive required a large number of employees to be able to conduct such complex analyses.
However, as technology advanced, the company recognized an opportunity to implement a modern tool - a chatbot - to achieve pattern analyses aimed at preventing fraud in real time. This tool would also assist in improving customer service.
The initial idea was communicated to the software development team, who supported the initiative and were assigned to work on the project. They began integrating the chatbot into the existing system and set an objective regarding the chatbot, which was to answer 85% of all chat queries.
After successfully integrating the chatbot, the company released it for customer use. However, the chatbot exhibited several issues. Due to insufficient testing and a lack of sample data provided during the training phase - when it was supposed to learn the query pattern - the chatbot failed to effectively address user queries. Additionally, it sent random files to users when it encountered invalid inputs, such as unusual patterns of dots and special characters.
Consequently, the chatbot could not effectively answer customer queries, overwhelming traditional customer support and preventing them from assisting customers with their requests.
Recognizing the potential risks, Fintive decided to implement a set of new controls. The measures included enabling comprehensive audit logging, configuring automated alert systems to flag unusual activities, performing periodic access reviews, and monitoring system behavior for anomalies. The objective was to identify unauthorized access, errors, or suspicious activities in a timely manner, ensuring that any potential issues could be quickly recognized and investigated before causing significant harm.
Question
According to Scenario 1, which of the following could be a potential impact of the chatbot issues?
A. Temporary slowdown in internal system updates with no effect on users
B. A breach of customer privacy due to the potential exposure of sensitive files
C. Minor delays in customer service response times due to the chatbot malfunction
Answer: (SHOW ANSWER)
From Exact Extract:
1. Identification of potential impact
The scenario clearly states that the chatbot:
* Sent random files to users
* Encountered invalid inputs
* Processed personally identifiable information (PII)
* Operated in a live customer-facing environment
Sending random files to users represents a direct risk of unauthorized disclosure of information, which could include:
* Customer records
* Sensitive operational data
* Personally identifiable information (PII)
This constitutes a customer privacy breach, which is a serious information security impact.
2. ISO/IEC 27001:2022 - Impact on confidentiality
Under ISO/IEC 27001:2022, one of the core objectives of an ISMS is to protect confidentiality, especially where PII is involved.
* Clause 6.1.2 (Information security risk assessment) requires organizations to identify risks related to loss of confidentiality.
* Clause 6.1.3 (Information security risk treatment) requires controls to be implemented where such risks exist.
A system that distributes random files creates a high-impact confidentiality risk.
3. ISO/IEC 27002:2022 - Privacy and PII protection
This scenario directly impacts Annex A control A.5.34 - Privacy and protection of PII, which requires organizations to:
Protect personal data against unauthorized access, disclosure, or misuse.
The chatbot's behaviour violates the intent of this control and demonstrates a clear privacy impact.
4. Why the other options are incorrect
* A. Temporary slowdown in internal system updatesThis is not supported by the scenario. There is no reference to internal system updates being affected.
* C. Minor delays in customer service response timesWhile customer support was overwhelmed, the scenario describes a much more severe impact - uncontrolled file transmission and potential data exposure. This understates the risk.

Auditor Conclusion
The most significant and realistic impact arising from the chatbot issues is a breach of customer privacy due to the potential exposure of sensitive files. This aligns with ISO/IEC 27001's focus on protecting confidentiality and PII.

NEW QUESTION: 146
Question:
Which option below is correct about the audit plan?
A. The audit plan involves the use of several audit procedures
B. The audit plan should be flexible to allow for modifications
C. The auditee's top management prepares the audit plan
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Audit plans must remain flexible to adapt to unforeseen findings and risks.
* ISO 19011:2018 specifies that audit planning should allow dynamic adjustments.
* A. Incorrect:
* Audit procedures are part of execution, not planning.
* C. Incorrect:
* The audit team, not top management, prepares the audit plan.
Relevant Standard Reference:
* ISO 19011:2018 Clause 5.4 (Audit Planning Flexibility)

NEW QUESTION: 147
Scenario 8: EsBank provides banking and financial solutions to the Estonian banking sector since September
2010. The company has a network of 30 branches with over 100 ATMs across the country.
Operating in a highly regulated industry, EsBank must comply with many laws and regulations regarding the security and privacy of data. They need to manage information security across their operations by implementing technical and nontechnical controls. EsBank decided to implement an ISMS based on ISO/IEC
27001 because it provided better security, more risk control, and compliance with key requirements of laws and regulations.
Nine months after the successful implementation of the ISMS, EsBank decided to pursue certification of their ISMS by an independent certification body against ISO/IEC 27001 .The certification audit included all of EsBank's systems, processes, and technologies.
The stage 1 and stage 2 audits were conducted jointly and several nonconformities were detected. The first nonconformity was related to EsBank's labeling of information. The company had an information classification scheme but there was no information labeling procedure. As a result, documents requiring the same level of protection would be labeled differently (sometimes as confidential, other times sensitive).
Considering that all the documents were also stored electronically, the nonconformity also impacted media handling. The audit team used sampling and concluded that 50 of 200 removable media stored sensitive information mistakenly classified as confidential. According to the information classification scheme, confidential information is allowed to be stored in removable media, whereas storing sensitive information is strictly prohibited. This marked the other nonconformity.
They drafted the nonconformity report and discussed the audit conclusions with EsBank's representatives, who agreed to submit an action plan for the detected nonconformities within two months.
EsBank accepted the audit team leader's proposed solution. They resolved the nonconformities by drafting a procedure for information labeling based on the classification scheme for both physical and electronic formats. The removable media procedure was also updated based on this procedure.
Two weeks after the audit completion, EsBank submitted a general action plan. There, they addressed the detected nonconformities and the corrective actions taken, but did not include any details on systems, controls, or operations impacted. The audit team evaluated the action plan and concluded that it would resolve the nonconformities. Yet, EsBank received an unfavorable recommendation for certification.
Based on the scenario above, answer the following question:
Based on scenario 8, EsBank submitted a general action plan. Is this acceptable?
A. Yes, nonconformities with the same root cause should have a general action plan

B. No, an action plan should only address one nonconformity
C. No, a general action plan does not enable the correction of nonconformities
Answer: (SHOW ANSWER)
No, a general action plan is not acceptable in this context because it lacks specific details on systems, controls, or operations impacted by the nonconformities. An effective action plan should detail the specific corrective actions for each nonconformity to ensure comprehensive resolution and prevent recurrence.

NEW QUESTION: 148
Which two activities align with the "Check" stage of the Plan-Do-Check-Act cycle when applied to the process of managing an internal audit program as described in ISO 19011?
A. Retains records of internal audits
B. Define audit criteria and scope for each internal audit
C. Update the internal audit programme
D. Establish a risk-based internal audit programme
E. Conduct internal audits
F. Verify effectiveness of the internal audit programme
G. Review trends in internal audit result
Answer: (SHOW ANSWER)
The Check stage of the PDCA cycle involves monitoring and measuring the performance of the process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines1. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer feedback1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 149
Scenario 9: UpNet, a networking company, has been certified against ISO/IEC 27001. It provides network security, virtualization, cloud computing, network hardware, network management software, and networking technologies.
The company's recognition has increased drastically since gaining ISO/IEC 27001 certification. The certification confirmed the maturity of UpNefs operations and its compliance with a widely recognized and accepted standard.
But not everything ended after the certification. UpNet continually reviewed and enhanced its security controls and the overall effectiveness and efficiency of the ISMS by conducting internal audits. The top management was not willing to employ a full-time team of internal auditors, so they decided to outsource the internal audit function. This form of internal audits ensured independence, objectivity, and that they had an advisory role about the continual improvement of the ISMS.
Not long after the initial certification audit, the company created a new department specialized in data and storage products. They offered routers and switches optimized for data centers and software-based networking devices, such as network virtualization and network security appliances. This caused changes to the operations of the other departments already covered in the ISMS certification scope.
Therefore. UpNet initiated a risk assessment process and an internal audit. Following the internal audit result, the company confirmed the effectiveness and efficiency of the existing and new processes and controls.
The top management decided to include the new department in the certification scope since it complies with ISO/IEC 27001 requirements. UpNet announced that it is ISO/IEC 27001 certified and the certification scope encompasses the whole company.
One year after the initial certification audit, the certification body conducted another audit of UpNefs ISMS.
This audit aimed to determine the UpNefs ISMS fulfillment of specified ISO/IEC 27001 requirements and ensure that the ISMS is being continually improved. The audit team confirmed that the certified ISMS continues to fulfill the requirements of the standard. Nonetheless, the new department caused a significant impact on governing the management system. Moreover, the certification body was not informed about any changes. Thus, the UpNefs certification was suspended.
Based on the scenario above, answer the following question:
What type of audit is illustrated in the last paragraph of scenario 9?
A. Surveillance audit
B. Internal audit
C. Recertification audit
Answer: (SHOW ANSWER)
The audit described in the last paragraph of scenario 9 is a surveillance audit. This type of audit is conducted periodically to ensure that the certified ISMS continues to fulfill the requirements of the standard after the initial certification.

NEW QUESTION: 150

Scenario 5
CyberShielding Systems Inc. provides security services spanning the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. CyberShielding Systems Inc. has helped various companies secure their networks for two decades through advanced products and services. Having achieved a reputation in the information and network security sector, CyberShielding Systems Inc. decided to implement a security information management system (ISMS) based on ISO/IEC 27001 and obtain a certification to better secure its internal and customer assets and gain a competitive advantage.
The certification body initiated the process by selecting the audit team for CyberShielding Systems Inc.'s ISO
/IEC 27001 certification. They provided the company with the name and background information of each audit member. However, upon review, CyberShielding Systems Inc. discovered that one of the auditors did not hold the security clearance required by them. Consequently, the company objected to the appointment of this auditor. Upon review, the certification body replaced the auditor in response to CyberShielding Systems Inc.'s objection.
As part of the audit process, CyberShielding Systems Inc.'s approach to risk and opportunity determination was assessed as a standalone activity. This involved examining the organization's methods for identifying and managing risks and opportunities. The audit team's core objectives encompassed providing assurance on the effectiveness of CyberShielding Systems Inc.'s risk and opportunity identification mechanisms and reviewing the organization's strategies for addressing these determined risks and opportunities. During this, the audit team also identified a risk due to a lack of oversight in the firewall configuration review process, where changes were implemented without proper approval, potentially exposing the company to vulnerabilities. This finding highlighted the need for stronger internal controls to prevent such issues.
The audit team accessed process descriptions and organizational charts to understand the main business processes and controls. They performed a limited analysis of the IT risks and controls because their access to the IT infrastructure and applications was limited by third-party service provider restrictions. However, the audit team stated that the risk of a significant defect occurring in CyberShielding's ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by questioning CyberShielding representatives on IT responsibilities, control effectiveness, and anti-malware measures. CyberShielding's representatives provided sufficient and appropriate evidence to address all these questions.
Despite the agreement signed before the audit, which outlined the audit scope, criteria, and objectives, the audit was primarily focused on assessing conformity with established criteria and ensuring compliance with statutory and regulatory requirements.
Question
Was the audit team's assessment of CyberShielding Systems Inc.'s risk and opportunity determination conducted in accordance with established auditing norms? Refer to Scenario 5.

Freecram.net

A. Yes, conducting the assessment independently is a recommended practice.

B. No, unless CyberShielding Systems Inc. explicitly requested an independent assessment.

C. No, conducting standalone assessments is not recommended; it should be implicit during the entire audit of a management system.

Answer: (SHOW ANSWER)

The audit team's approach to assessing risk and opportunity determination as a standalone activity is in line with established auditing norms, making option A the correct answer. ISO/IEC 27001:2022 requires organizations to identify risks and opportunities related to the ISMS and to plan actions to address them. From an audit perspective, ISO 19011 allows auditors to structure audit activities in a way that ensures effective coverage of critical requirements.

Assessing risk and opportunity determination independently does not violate auditing principles, provided it remains connected to the overall management system context. In practice, auditors often examine risk management as a distinct audit trail because it is a foundational element that influences many other ISMS processes, including control selection, operational planning, and continual improvement. Conducting a focused assessment enables auditors to evaluate whether risks are identified systematically, whether opportunities are considered, and whether treatment plans are appropriate and effective.
Option C is incorrect because although risk and opportunity management should be embedded throughout the ISMS, auditing it as a standalone activity does not contradict this principle. It is an audit structuring decision rather than a management system design issue. Option B is incorrect because auditors do not require explicit auditee requests to structure audit activities independently; they are responsible for designing the audit approach.
Therefore, the audit team's standalone assessment of risk and opportunity determination aligns with recommended auditing practices.

NEW QUESTION: 151
Scenario 2
Knight is an electronics company based in Northern California, the US that develops video game consoles.
With over 300 employees globally, Knight is celebrating its fifth anniversary by launching the G-Console, a next-generation gaming system aimed at international markets. G-Console is considered to be the ultimate media machine of 2021, and it will give players the best gaming experience. The console pack will include a pair of VR headsets, two games, and other gifts.
Over the years, the company has developed a strong reputation for integrity, honesty, and respect toward their customers. Besides being a very customer-oriented company, Knight also gained wide recognition within the gaming industry because of its quality.
As one of the leading video game console developers in the world, Knight often finds itself a target for malicious activities. Therefore, it has implemented an information security management system (ISMS) based on ISO/IEC 27001, and its scope was communicated to employees of the company over a weekly meeting.
Recently, however, Knight experienced a security breach when hackers leaked proprietary information. In response, the incident response team (IRT) immediately began a thorough investigation of the system and the specifics of the incident.
Initially, the IRT suspected that employees may have used weak passwords, allowing hackers to easily access their accounts. Upon further investigation, it was revealed that the hackers captured traffic from the file transfer protocol (FTP), which transmits data using clear-text passwords for authentication.
In light of this security incident, and following the IRT's recommendations, Knight decided to replace the FTP with Secure Shell (SSH) protocol. This change ensures that any captured traffic is encrypted, significantly improving security.
After implementing these changes, Knight conducted a risk assessment to verify that the implementation of controls had minimized the risk of similar incidents. Based on the results of the risk assessment, they chose a risk treatment option to treat the risk.
Question
What does the IRT's findings about FTP represent in terms of information security?
A. Vulnerability
B. Risk
C. Threat
Answer: (SHOW ANSWER)
The IRT's finding that FTP transmits authentication credentials in clear text represents a vulnerability in information security terms. A vulnerability is defined as a weakness in an asset, system, or control that can be exploited by a threat. In this scenario, FTP itself is not a threat, nor is it the risk; rather, it is the technical weakness that enabled the attackers to succeed.
The attackers (hackers) are the threat, and the potential loss of proprietary information is the impact. The risk arises from the combination of the threat exploiting the vulnerability and causing harm. However, the question specifically asks what the IRT's finding about FTP represents, and that finding is the identification of a weakness in the system design. The use of clear-text authentication is a well-known security weakness, making it easier for attackers to capture credentials through network traffic interception.
ISO/IEC 27001:2022 risk assessment logic requires organizations to distinguish clearly between threats, vulnerabilities, and risks during incident analysis. The IRT did exactly this by identifying that the protocol itself lacked encryption, which is a vulnerability. This is further supported by the corrective action taken:
replacing FTP with SSH. SSH provides encrypted communication, which directly addresses the vulnerability by removing the weakness that allowed credential exposure.
Therefore, the IRT's findings correctly identify FTP as a vulnerability, making option A the correct answer.

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
A property of Information that has the ability to prove occurrence of a claimed event.
A. Electronic chain letters
B. Integrity
C. Availability
D. Accessibility
Answer: (SHOW ANSWER)
A property of information that has the ability to prove occurrence of a claimed event is integrity. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Integrity also implies that information and systems can be verified and validated as authentic and accurate. Electronic chain letters are not a property of information, but a type of spam or hoax message that may contain malicious or misleading content. Availability means that service should be accessible at the required time and usable only by the authorized entity. Accessibility is not a property of information, but a characteristic of usability that refers to how easy it is for users to access and interact with information and systems. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

NEW QUESTION: 153
Question:
Three auditors were assigned to conduct a certification audit in Company X. Before the audit commenced, the certification body provided the auditors' names and background information to Company X. Company X requested the replacement of one of the auditors because they are a former employee. Is this acceptable?
A. A situation of conflict of interest is a valid reason to request the replacement of the auditor
B. No, the auditee can request the replacement of the auditor only if a valid reason is presented such as unprofessional conduct or situations with real conflict of interest
C. No, the auditee cannot request the replacement of auditors
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* ISO/IEC 17021-1 (Conformity assessment - Requirements for bodies providing audit and certification of management systems) states that the auditee may request a replacement of an auditor only for valid reasons.
* A former employee of the company serving as an auditor presents a potential conflict of interest (real or perceived).
* Therefore, Company X's request is valid.
* A. Incorrect:
* While a conflict of interest is a valid reason, the replacement must be based on an objective, justified claim, and not just personal preference.
* C. Incorrect:
* Auditees can request an auditor's replacement, but only under justified circumstances.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.1.3 (Impartiality and Objectivity of Auditors)

NEW QUESTION: 154
Which one option best describes the purpose of retaining documented information related to the Information Security Management System (ISMS) of an organisation?
A. To ensure that all workers will follow the established procedure.

B. To show compliance with legal requirements.
C. To show objective evidence to third-party auditors.
D. To the extent necessary, to have confidence that the processes have been carried out as planned.
Answer: (SHOW ANSWER)
The purpose of retaining documented information related to the ISMS of an organisation is to the extent necessary, to have confidence that the processes have been carried out as planned. This means that the documented information provides evidence of the conformity and effectiveness of the ISMS, as well as the achievement of the information security objectives and the continual improvement of the ISMS. Documented information also supports the analysis and evaluation of the ISMS performance and the identification of opportunities for improvement. References: = ISO/IEC 27001:2022, clause 7.5.1; PECB Candidate Handbook ISO 27001 Lead Auditor, page 17.

NEW QUESTION: 155
What is meant by the term 'Corrective Action'? Select one
A. Action is taken to prevent a nonconformity or an incident from occurring
B. Action is taken to eliminate the cause(s) of a nonconformity or an incident
C. Action is taken by management to respond to a nonconformity
D. Action is taken to fix a nonconformity or an incident
Answer: (SHOW ANSWER)
Corrective action is a process of identifying and eliminating the root causes of nonconformities or incidents that have occurred or could potentially occur, in order to prevent their recurrence or occurrence. Corrective action is part of the improvement requirement of ISO 27001 and follows a standard workflow of identification, evaluation, implementation, review and documentation of corrections and corrective actions.
References: Procedure for Corrective Action, Nonconformity & Corrective Action For ISO 27001 Requirement 10.1, PECB Candidate Handbook ISO 27001 Lead Auditor (page 12)

NEW QUESTION: 156
You have to carry out a third-party virtual audit. Which two of the following issues would you need to inform the auditee about before you start conducting the audit ?
* You will ask to see the ID card of the person that is on the screen.
A. You will take photos of every person you interview.
B. You will ask those being interviewed to state their name and position beforehand.
C. You will ask for a 360-degree view of the room where the audit is being carried out.
D. You will not record any part of the audit, unless permitted.
E. You expect the auditee to have assessed all risks associated with online activities.
Answer: (SHOW ANSWER)
A third-party virtual audit is an external audit conducted by an independent certification body using remote technology such as video conferencing, screen sharing, and electronic document exchange. The purpose of a third-party virtual audit is to verify the conformity and effectiveness of the information security management system (ISMS) and to issue a certificate of compliance12 Before you start conducting the audit, you would need to inform the auditee about the following issues: 12
* You will ask those being interviewed to state their name and position beforehand, i.e., to confirm their identity and role in the ISMS. This is to ensure that you are interviewing the relevant personnel and that they are authorized to provide information and evidence for the audit.
* You will ask for a 360-degree view of the room where the audit is being carried out, i.e., to verify the physical and environmental security of the audit location. This is to ensure that there are no unauthorized persons or devices in the vicinity that could compromise the confidentiality, integrity, or availability of the information being audited.
The other issues are not relevant or appropriate for a third-party virtual audit, because:
* You will ask to see the ID card of the person that is on the screen, i.e., to verify their identity. This is not necessary if you have already asked them to state their name and position beforehand, and if you have access to the auditee's organizational chart or staff directory. Asking to see the ID card could also be seen as intrusive or disrespectful by the auditee.
* You will take photos of every person you interview, i.e., to document the audit process. This is not advisable as it could violate the privacy or consent of the auditee and the interviewees. Taking photos could also be seen as unprofessional or suspicious by the auditee. You should rely on the audit records and evidence provided by the auditee and the audit tool instead.
* You will not record any part of the audit, unless permitted, i.e., to respect the auditee's preferences and rights. This is not a valid issue to inform the auditee about, as you should always record the audit for quality assurance and verification purposes. Recording the audit is also a requirement of the ISO/IEC

27001 standard and the certification body. You should inform the auditee that you will record the audit and obtain their consent before the audit begins.
* You expect the auditee to have assessed all risks associated with online activities, i.e., to ensure the security of the audit process. This is not an issue to inform the auditee about, as it is part of the auditee' s responsibility and obligation to have a risk assessment and treatment process for their ISMS. You should assess the auditee's risk management practices and controls during the audit, not before it.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 157
An audit finding is the result of the evaluation of the collected audit evidence against audit criteria. Evaluate the following potential formats of audit evidence and select the two that are acceptable.
A. Unsigned hand written changes to test results
B. Statement of facts by the IT manager
C. Documented information on results of IT audits
D. Statements by a system engineer that cannot be verified
E. Observation of a previously recorded video demonstrating the performance of a hazardous activity
F. An audio recording of a dialog between the IT manager and a system engineer
Answer: (SHOW ANSWER)
According to the ISO/IEC 27001 Lead Auditor exam preparation guide1, audit evidence can be in various formats, such as records, statements of fact, or other information that is relevant and verifiable. Audit evidence can be collected by means of interviews, observation, sampling, testing, or other techniques.
However, not all formats of audit evidence are acceptable or reliable. For example, unsigned hand written changes to test results (A) are not verifiable and may indicate tampering or falsification. Statements by a system engineer that cannot be verified (D) are also not reliable and may be biased or inaccurate. An audio recording of a dialog between the IT manager and a system engineer (F) may not be relevant to the audit criteria or may violate the confidentiality or consent of the parties involved. A statement of facts by the IT manager (B) may be relevant and verifiable, but it is not sufficient as audit evidence unless it is supported by other sources of information. Therefore, the two acceptable formats of audit evidence are documented information on results of IT audits and observation of a previously recorded video demonstrating the performance of a hazardous activity (E), as they are relevant to the audit criteria and can be verified by other means. References: 1: https://pecb.com/pdf/exam-preparation-guides/pecb-iso-iec-27001-lead-auditor-exam- preparation-guide.pdf (page 9)

NEW QUESTION: 158
You are an experienced audit team leader conducting a third-party surveillance audit of an organisation that designs websites for its clients. You are currently reviewing the organisation's Statement of Applicability.
Based on the requirements of ISO/IEC 27001, which two of the following observations about the Statement of Applicability are false?
A. The Statement of Applicability must include Organisational, Physical, People and Technological controls that are necessary
B. Justification is only required for any controls that the organisations choses to exclude
C. The Statement of Applicability is owned and amended by the organisation's top management
D. Justification for both the inclusion and exclusion of Annex A controls in the Statement of Applicability is required
E. Additional controls not included in Appendix A may be added to the Statement of Applicability if the organisation choses to do so
F. A Statement of Applicability must be produced by organisations seeking ISO/IEC 27001 conformity
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Audit methods can be either with or without interaction with individuals representing the auditee. Which two of the following methods are with interaction?
A. Sampling (e.g. products)
B. Observing work performed via live video streaming
C. Reviewing checklists with auditee
D. Checking legal compliance with local authorities
E. Conducting interviews

F. Analysing documents provided in advance of the audit

Answer: (SHOW ANSWER)

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, audit methods can be classified into two categories: with or without interaction with individuals representing the auditee (page 12).

Audit methods with interaction include reviewing checklists with auditee and conducting interviews, as they involve direct communication and feedback from the auditee. Audit methods without interaction include sampling (e.g. products), observing work performed via live video streaming, checking legal compliance with local authorities, and analysing documents provided in advance of the audit, as they do not require any dialogue or exchange with the auditee. References: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 12.

NEW QUESTION: 160

You are an experienced ISMS audit team leader providing instruction to a class of auditors in training. The subject of today's lesson is the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022.

You provide the class with a series of activities. You then ask the class to sort these activities into the order in which they appear in the standard.

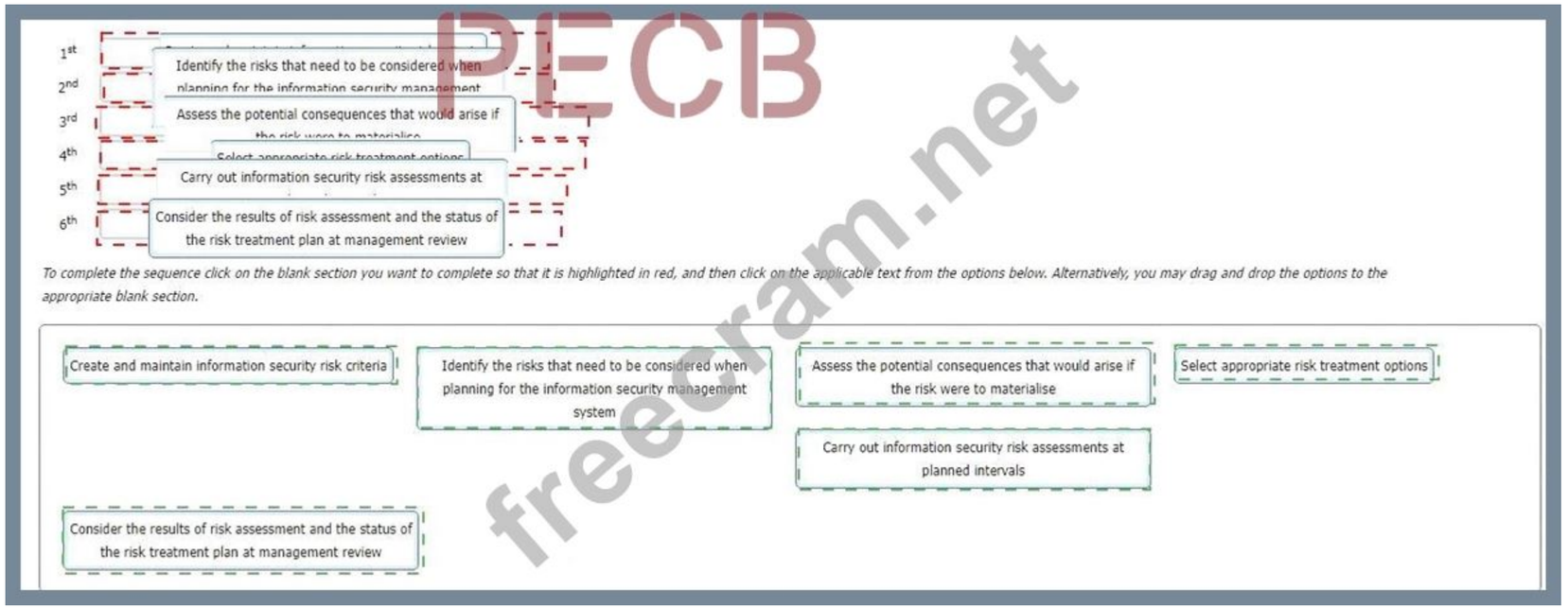
What is the correct sequence they should report back to you?

1st
2nd
3rd
4th
5th
6th

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

- Create and maintain information security risk criteria
- Identify the risks that need to be considered when planning for the information security management system
- Assess the potential consequences that would arise if the risk were to materialise
- Select appropriate risk treatment options
- Carry out information security risk assessments at planned intervals
- Consider the results of risk assessment and the status of the risk treatment plan at management review

Answer:



Explanation:

The correct sequence of activities for the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022 is as follows:

1st: Create and maintain information security risk criteria 2nd: Identify the risks that need to be considered when planning for the information security management system 3rd: Assess the potential consequences that would arise if the risk were to materialise 4th: Select appropriate risk treatment options 5th: Carry out information security risk assessments at planned intervals 6th: Consider the results of risk assessment and the status of the risk treatment plan at management review This sequence is based on the information security risk management process described in ISO/IEC 27001:

2022 clause 6.1, which includes the following activities:

* establishing and maintaining information security risk criteria;
* ensuring that repeated information security risk assessments produce consistent, valid and comparable results;
* identifying the information security risks;
* analyzing the information security risks;
* evaluating the information security risks;
* treating the information security risks;

* accepting the information security risks and the residual information security risks;
* communicating and consulting with stakeholders throughout the process;
* monitoring and reviewing the information security risks and the risk treatment plan.
References:
ISO/IEC 27001:2022, clause 6.1
[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 14-15
ISO 27001 Risk Management in Plain English

NEW QUESTION: 161
Question:
What is the main reason for sending an engagement letter before the initial contact with the auditee?
A. To confirm the authority to conduct the audit
B. To provide initial audit details and schedule the initial contact
C. To establish the audit objectives
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The engagement letter serves to inform the auditee about the audit details, including:
* Audit scope
* Audit schedule
* Expectations from both parties
* It formally introduces the audit process and schedules the initial contact.
* A. Incorrect:
* The authority to conduct the audit is established by the certification body's agreement, not just the engagement letter.
* C. Incorrect:
* Audit objectives are determined in the planning phase and are not the primary function of the engagement letter.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.2 (Initiating the Audit)

NEW QUESTION: 162
You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.
You are currently in a large room that is subdivided into several smaller rooms, each of which has a numeric combination lock and swipe card reader on the door. You notice two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorised electrical repairs.
You go to reception and ask to see the door access record for the client's suite. This indicates only one card was swiped. You ask the receptionist and they reply, "yes it's a common problem. We ask everyone to swipe their cards but with contractors especially, one tends to swipe and the rest simply 'tailgate' their way in" but we know who they are from the reception sign-in.
Based on the scenario above which one of the following actions would you now take?
A. Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times
B. Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV
C. Raise a nonconformity against control A.7.1 'security perimiters' as a secure area is not adequately protected
D. Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined
E. Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier

F. Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities

Answer: (SHOW ANSWER)

The best action to take in this scenario is to determine whether any additional effective arrangements are in place to verify individual access to secure areas, such as CCTV. This action is consistent with the audit principle of evidence-based approach, which requires the auditor to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions1. By verifying the existence and effectiveness of other security controls, the auditor can assess the extent and impact of the nonconformity observed, and determine the appropriate audit finding and recommendation.

The other options are not the best actions to take in this scenario, because they are either premature or inappropriate. For example:

*Option A is inappropriate, because it is not the auditor's role to suggest specific solutions or improvements to the auditee, but rather to report the audit findings and recommendations based on the audit criteria and objectives2. A large sign in reception may not be an effective or feasible solution to address the issue of tailgating, and it may not reflect the root cause of the problem.

*Option C is premature, because it assumes that the control A.7.1 'security perimeters' is not adequately implemented, without verifying the existence and effectiveness of other security controls that may compensate for the observed nonconformity. The auditor should not jump to conclusions based on a single observation, but rather gather sufficient and appropriate audit evidence to support the audit finding3.

*Option D is premature, because it assumes that the control A.7.6 'working in secure areas' is not adequately implemented, without verifying the existence and effectiveness of other security controls that may compensate for the observed nonconformity. The auditor should not jump to conclusions based on a single observation, but rather gather sufficient and appropriate audit evidence to support the audit finding3.

*Option E is inappropriate, because it is not related to the observed nonconformity, which is about the access control to secure areas, not the information security requirements agreed upon with the supplier. The auditor should not raise a nonconformity based on irrelevant or incorrect audit criteria4.

*Option F is inappropriate, because it is not the auditor's role to suggest specific solutions or improvements to the auditee, but rather to report the audit findings and recommendations based on the audit criteria and objectives2. Requiring contractors to be accompanied at all times when accessing secure facilities may not be an effective or feasible solution to address the issue of tailgating, and it may not reflect the root cause of the problem.

References: 1: ISO 19011:2018, 5.2; 2: ISO 19011:2018, 6.6; 3: ISO 19011:2018, 6.2; 4: ISO 19011:2018,
6.3; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018

NEW QUESTION: 163

You are performing an ISMS audit at a nursing home where residents always wear an electronic wristband for monitoring their location, heartbeat, and blood pressure. The wristband automatically uploads this data to a cloud server for healthcare monitoring and analysis by staff.

You now wish to verify that the information security policy and objectives have been established by top management. You are sampling the mobile device policy and identify a security objective of this policy is "to ensure the security of teleworking and use of mobile devices" The policy states the following controls will be applied in order to achieve this.

Personal mobile devices are prohibited from connecting to the nursing home network, processing, and storing residents' data.

The company's mobile devices within the ISMS scope shall be registered in the asset register.

The company's mobile devices shall implement or enable physical protection, i.e., pin-code protected screen lock/unlock, facial or fingerprint to unlock the device.

The company's mobile devices shall have a regular backup.

To verify that the mobile device policy and objectives are implemented and effective, select three options for your audit trail.

A. Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home

B. Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home

C. Review the internal audit report to make sure the IT department has been audited

D. Review the asset register to make sure all personal mobile devices are registered

E. Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register

F. Review the asset register to make sure all company's mobile devices are registered

G. Interview the supplier of the devices to make sure they are aware of the ISMS policy

H. Interview top management to verify their involvement in establishing the information security policy and the information security objectives

Answer: (SHOW ANSWER)

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 5.2 requires top management to establish an information security policy that provides the framework for setting information security objectives1. Clause 6.2 requires top management to ensure that the information security objectives are established at relevant functions and levels1. Therefore, when verifying that the information security policy and objectives have been established by top management, an ISMS auditor should review relevant documents and records that demonstrate top management's involvement and commitment.

To verify that the mobile device policy and objectives are implemented and effective, an ISMS auditor should review relevant documents and records that demonstrate how the policy and objectives are communicated, monitored, measured, analyzed, and evaluated. The auditor should also sample and verify the implementation of the controls that are stated in the policy.
Three options for the audit trail that are relevant to verifying the mobile device policy and objectives are:
* Review the internal audit report to make sure the IT department has been audited: This option is relevant because it can provide evidence of how the IT department, which is responsible for managing the mobile devices and their security, has been evaluated for its conformity and effectiveness in implementing the mobile device policy and objectives. The internal audit report can also reveal any nonconformities, corrective actions, or opportunities for improvement related to the mobile device policy and objectives.
* Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register: This option is relevant because it can provide evidence of how the mobile devices that are used by the medical staff, who are involved in processing and storing residents' data, are registered in the asset register and have physical protection enabled. This can verify the implementation and effectiveness of two of the controls that are stated in the mobile device policy.
* Review the asset register to make sure all company's mobile devices are registered: This option is relevant because it can provide evidence of how the company's mobile devices that are within the ISMS scope are identified and accounted for. This can verify the implementation and effectiveness of one of the controls that are stated in the mobile device policy.
The other options for the audit trail are not relevant to verifying the mobile device policy and objectives, as they are not related to the policy or objectives or their implementation or effectiveness. For example:
* Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding physical security or access control, but not specifically to mobile devices.
* Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security awareness or compliance, but not specifically to mobile devices.
* Interview the supplier of the devices to make sure they are aware of the ISMS policy: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security within supplier relationships, but not specifically to mobile devices.
* Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to verifying that the information security policy and objectives have been established by top management, but not specifically to mobile devices.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 164
The data centre at which you work is currently seeking ISO/IEC27001:2022 certification. In preparation for your initial certification visit, several internal audits have been carried out by a colleague working at another data centre within your Group.
They secured their own ISO/IEC 27001:2022 certificate earlier in the year.
You have just qualified as an Internal ISMS auditor and your manager has asked you to review the audit process and audit findings as a final check before the external Certification Body arrives.
Which four of the following would cause you concern in respect of conformity to ISO/IEC 27001:2022 requirements?
A. Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date.
B. The audit programme has not been signed as 'approved by Top Management.
C. The audit programme shows management reviews taking place at irregular intervals during the year.
D. The audit process states the results of audits will be made available to 'relevant' managers, not top management.
E. The audit programme does not reference audit methods or audit responsibilities.
F. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as *. PDF documents on the organisation's intranet.
G. The audit programme does not take into account the results of previous audits.
H. The audit programme does not take into account the relative importance of information security processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Question
An organization depends on a single server to manage all incoming traffic, creating a potential single point of failure. If the server experiences malfunction or downtime, it could disrupt services.
What does this scenario present, and which aspect of information security is primarily affected?
A. A risk, impacting availability

B. A misconfiguration, impacting availability
C. A system error, impacting authentication
Answer: (SHOW ANSWER)
This scenario presents a risk that primarily impacts availability, which is one of the three core information security principles alongside confidentiality and integrity. Relying on a single server to manage all incoming traffic introduces a single point of failure, meaning that if the server fails, services become unavailable.
From an ISO/IEC 27001 perspective, this is clearly a risk, not merely a misconfiguration or a system error. A risk exists because there is a reasonable likelihood that the server could fail and a significant impact if it does, namely service disruption. ISO/IEC 27001 clause 6.1.2 requires organizations to identify such risks that could affect the availability of information and services.
Option B is incorrect because while misconfiguration can cause outages, the scenario does not describe an incorrect configuration; it describes an architectural dependency. Option C is incorrect because authentication is not the primary concern; the issue affects the ability to deliver services at all, regardless of user authentication.
Availability is explicitly addressed in ISO/IEC 27002:2022 through controls such as redundancy and capacity management. The absence of redundancy increases availability risk. Therefore, the scenario correctly represents a risk impacting availability, making option A the best answer.

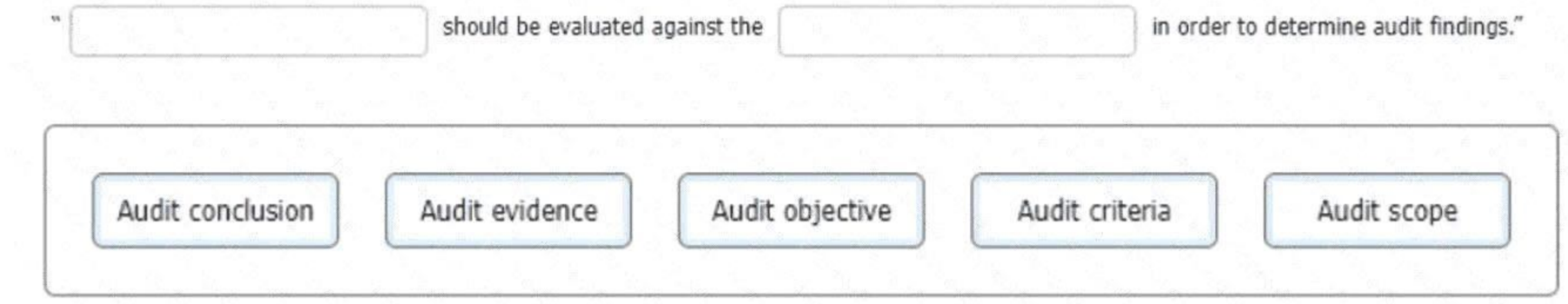
NEW QUESTION: 166
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits.
Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.
The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.
Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.
Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.
Based on the scenario above, answer the following question:
The audit team photocopied the examined employee training records to support their conclusion. Should the audit team obtain an approval from Lawsy before taking this action? Refer to scenario 7.
A. Yes. the audit team should obtain the approval of the auditee when verifying the existence of a process in all cases, including when taking notes and photocopying documents
B. Yes, the audit team can photocopy documents observed during the audit if the auditee agrees to it
C. No, the audit team has the authority to photocopy documents in order to verify the conformity of a certain document to the audit criteria
Answer: (SHOW ANSWER)
Yes, the audit team should obtain approval from Lawsy before photocopying documents. This is a best practice to ensure that the auditee agrees to the duplication of documents, which might contain sensitive or confidential information. Although auditors can observe and note down information, copying documents typically requires explicit permission to maintain trust and ensure compliance with confidentiality agreements.
References: ISO 19011:2018, Guidelines for auditing management systems

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

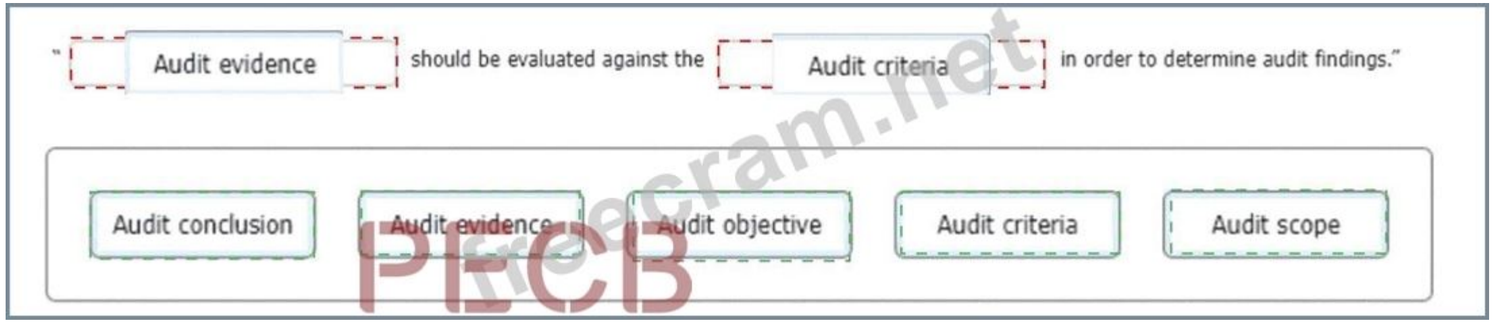
NEW QUESTION: 167
You are conducting an ISMS audit. The next step in your audit plan is to verify that the organisation's information security risk treatment plan has been established and implemented properly. You decide to interview the IT security manager.
You: Can you please explain how the organisation performs its information security risk assessment and treatment process?
IT Security Manager: We follow the information security risk management procedure which generates a risk treatment plan.
Narrator: You review risk treatment plan No. 123 relating to the planned installation of an electronic (invisible) fence to improve the physical security of the nursing home. You found the risk treatment plan was approved by IT Security Manager.
You: Who is responsible for physical security risks?
IT Security Manager: The Facility Manager is responsible for the physical security risk. The IT department helps them to monitor the alarm. The Facility Manager is authorized to approve the budget for risk treatment plan No. 123.
You: What residual information security risks exist after risk treatment plan No. 123 was implemented?
IT Security Manager: There is no information for the acceptance of residual information security risks as far as I know.
You prepare your audit findings. Select three options for findings that are justified in the scenario.
A. Nonconformity (NC) - The information for the acceptance of residual information security risks should be updated after the risk treatment is implemented. Clause 6.1.3.f
B. There is an opportunity for improvement (OI) to conduct security checks on the perimetre fence
C. There is an opportunity for improvement (OI) once the Electronic (invisible) fence is installed.
Residents' physical security is improved
D. Nonconformity (NC) - Top management must ensure that the resources needed for the ISMS are available. Clause 5.1.c
E. Nonconformity (NC) - The IT security manager should be aware of and understand his authority and area of responsibility. Clause 7.3
F. Nonconformity (NC) - The organization should provide the resources needed for the continual improvement of the ISMS. Clause 7.1
G. Nonconformity (NC) - The risk treatment plan No. 123 should be approved by the risk owner, the Facility Manager in this case. Clause 6.1.3.f
H. It is good practice to adopt state-of-the-art technology as part of the continual improvement process
Answer: (SHOW ANSWER)
The three options for findings that are justified in the scenario are:
*Nonconformity (NC) - The information for the acceptance of residual information security risks should be updated after the risk treatment is implemented. Clause 6.1.3.f
*Nonconformity (NC) - The IT security manager should be aware of and understand his authority and area of responsibility. Clause 7.3
*Nonconformity (NC) - The risk treatment plan No. 123 should be approved by the risk owner, the Facility Manager in this case. Clause 6.1.3.f According to ISO/IEC 27001:2022, clause 6.1.3.f, the organisation must retain documented information that includes the information for the acceptance of residual information security risks, and the approval of the risk treatment plan by the risk owner1. Therefore, option A and G are justified as nonconformities, because the organisation failed to update the information for the acceptance of residual risks, and the risk treatment plan was approved by the IT security manager, who is not the risk owner.
According to ISO/IEC 27001:2022, clause 7.3, the organisation must ensure that the persons assigned to perform the roles and responsibilities for the ISMS are competent, and are aware of the consequences of not conforming to the ISMS requirements2. Therefore, option E is justified as a nonconformity, because the IT security manager, who is responsible for the information security risk management process, was not aware of his authority and area of responsibility.
The other options are not justified as findings, because they are either irrelevant or incorrect. For example:
*Option B is irrelevant, because it is not related to the information security risk treatment plan No. 123, which is the focus of the audit.
*Option C is incorrect, because it is not an opportunity for improvement, but rather a benefit of the risk treatment plan No. 123, which is already implemented.
*Option D is incorrect, because it is not a nonconformity, but rather a requirement for the organisation to provide the resources needed for the ISMS, which is not the same as the resources needed for the risk treatment plan No. 123.
*Option F is incorrect, because it is not a nonconformity, but rather a requirement for the organisation to provide the resources needed for the continual improvement of the ISMS, which is not the same as the resources needed for the risk treatment plan No. 123.
*Option H is irrelevant, because it is not a finding, but rather a good practice, which is not the objective of the audit.
References: 1: ISO/IEC 27001:2022, 6.1.3.f; 2: ISO/IEC 27001:2022, 7.3; : ISO/IEC 27001:2022; : ISO/IEC

27001:2022

NEW QUESTION: 168
In regard to generating an audit finding, select the words that best complete the following sentence.
To complete the sentence with the best word(s), click on the blank section you want to complete so that it Is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.



Answer:



PrepCram.net
PECB

Explanation:
Audit evidence should be evaluated against the audit criteria in order to determine audit findings.
* Audit evidence is the information obtained by the auditors during the audit process that is used as a basis for forming an audit opinion or conclusion12. Audit evidence could include records, documents, statements, observations, interviews, or test results12.
* Audit criteria are the set of policies, procedures, standards, regulations, or requirements that are used as a reference against which audit evidence is compared12. Audit criteria could be derived from internal or external sources, such as ISO standards, industry best practices, or legal obligations12.
* Audit findings are the results of a process that evaluates audit evidence and compares it against audit criteria13. Audit findings can show that audit criteria are being met (conformity) or that they are not being met (nonconformity). They can also identify best practices or improvement opportunities13.
References :=
* ISO 19011:2022 Guidelines for auditing management systems
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* Components of Audit Findings - The Institute of Internal Auditors

NEW QUESTION: 169
Scenario 5
CyberShielding Systems Inc. provides security services spanning the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. CyberShielding Systems Inc. has helped various companies secure their networks for two decades through advanced products and services. Having achieved a reputation in the information and network security sector, CyberShielding Systems Inc. decided to implement a security information management system (ISMS) based on ISO/IEC 27001 and obtain a certification to better secure its internal and customer assets and gain a competitive advantage.
The certification body initiated the process by selecting the audit team for CyberShielding Systems Inc.'s ISO
/IEC 27001 certification. They provided the company with the name and background information of each audit member. However, upon review, CyberShielding Systems Inc. discovered that one of the auditors did not hold the security clearance required by them. Consequently, the company objected to the appointment of this auditor. Upon review, the certification body replaced the auditor in response to CyberShielding Systems Inc.'s objection.
As part of the audit process, CyberShielding Systems Inc.'s approach to risk and opportunity determination was assessed as a standalone activity. This involved examining the organization's methods for identifying and managing risks and opportunities. The audit team's core objectives encompassed providing assurance on the effectiveness of CyberShielding Systems Inc.'s risk and opportunity identification mechanisms and reviewing the organization's strategies for addressing these determined risks and opportunities. During this, the audit team also identified a risk due to a lack of oversight in the firewall configuration review process, where changes were implemented without proper approval, potentially exposing the company to vulnerabilities. This finding highlighted the need for stronger internal controls to prevent such issues.
The audit team accessed process descriptions and organizational charts to understand the main business processes and controls. They performed a limited analysis of the IT risks and controls because their access to the IT infrastructure and applications was limited by third-party service provider restrictions. However, the audit team stated that the risk of a significant defect occurring in CyberShielding's ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by questioning CyberShielding representatives on IT responsibilities, control effectiveness, and anti-malware measures. CyberShielding's representatives provided sufficient and appropriate evidence to address all these questions.
Despite the agreement signed before the audit, which outlined the audit scope, criteria, and objectives, the audit was primarily focused on assessing conformity with established criteria and ensuring compliance with statutory and regulatory requirements.
Question
Did the certification body have a valid reason to accept CyberShielding Systems Inc.'s objection to the appointed auditor for their ISO/IEC 27001 certification audit?
A. Yes, the certification body had a valid reason to accept CyberShielding Systems Inc.'s objection because auditors that do not hold the required security clearance should not audit the respective company.
B. No, the certification body can accept objections from auditees only if the auditor has previously displayed unprofessional conduct.
C. No, the certification body can only consider objections from auditees if there is a conflict of interest involving the auditor.
Answer: (SHOW ANSWER)
The certification body had a valid reason to accept CyberShielding Systems Inc.'s objection, making option A the correct answer. ISO/IEC 17021-1 requires certification bodies to ensure that audit teams are competent and acceptable to the auditee, particularly where access to sensitive information, systems, or facilities is involved. Security clearance requirements set by the auditee are a legitimate consideration, especially for organizations operating in highly sensitive information security environments.
In this scenario, CyberShielding Systems Inc. operates in the cybersecurity sector and handles sensitive internal and customer information. Auditors without the necessary security clearance may be unable to access required information or systems, which would compromise the effectiveness and completeness of the audit.
Accepting such an objection supports both audit quality and information protection.
Option B is incorrect because objections are not limited to cases of prior unprofessional conduct. Option C is incorrect because conflicts of interest are not the only valid grounds for objection. ISO/IEC 17021-1 allows auditees to object to auditors for justified reasons, including competence, impartiality, confidentiality, or access limitations.
Therefore, replacing the auditor due to insufficient security clearance was appropriate and consistent with certification body requirements and good auditing practice.

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by EduDump.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! EduDump.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the EduDump.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.edudump.com/exams/PECB/ISO-IEC-27001-Lead-Auditor/premium/ (**418** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)