PECB.ISO-IEC-27001-Lead-Auditor.v2026-07-14.q104

Exam Code:	ISO-IEC-27001-Lead-Auditor
Exam Name:	PECB Certified ISO/IEC 27001 Lead Auditor exam
Certification Provider:	PECB
Free Question Number:	104
Version:	v2026-07-14
# of views:	129
# of Questions views:	1040
https://www.exam-tests.com/ISO-IEC-27001-Lead-Auditor-exam/PECB.ISO-IEC-27001-Lead-Auditor.v2026-07-14.q104.html	

NEW QUESTION: 1
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: C,E (LEAVE A REPLY)
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. Reference: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 12.

NEW QUESTION: 2
A hacker gains access to a web server and reads the credit card numbers stored on that server. Which security principle is violated?
A. Availability
B. Confidentiality
C. Integrity
D. Authenticity
Answer: B (LEAVE A REPLY)
Confidentiality is one of the security principles that states that only authorized parties should have access to information assets. Confidentiality protects the secrecy and privacy of information from unauthorized disclosure or exposure. A hacker gaining access to a web server and reading the credit card numbers stored on that server violates the confidentiality principle, as he or she is not an authorized party and has access to sensitive information that belongs to others. Therefore, the correct answer is B. Reference: ISO/IEC 27000:2022, clause 3.8; Defining Security Principles - Pearson IT Certification.

NEW QUESTION: 3
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: A (LEAVE A REPLY)
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: 4
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:

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: 5
A member of staff denies sending a particular message.
Which reliability aspect of information is in danger here?
A. correctness
B. integrity
C. availability
D. confidentiality
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which two of the following are examples of audit methods that 'do' involve human interaction?
A. Performing an independent review of procedures in preparation for an audit
B. Reviewing the auditee's response to an audit finding
C. Analysing data by remotely accessing the auditee's server
D. Observing work performed by remote surveillance
E. Analysing data by remotely accessing the auditee's server
Answer: A,B (LEAVE A REPLY)
Audit methods are techniques used by auditors to obtain audit evidence. Audit methods can be classified into two categories: those that involve human interaction and those that do not2. Audit methods that involve human interaction require direct communication between the auditor and the auditee or other relevant parties, such as interviews, questionnaires, surveys, meetings, etc. Audit methods that do not involve human interaction rely on observation, inspection, measurement, testing, sampling, analysis, etc., without requiring any verbal or written exchange2. Therefore, performing an independent review of procedures in preparation for an audit and reviewing the auditee's response to an audit finding are examples of audit methods that involve human interaction, as they require reading and evaluating documents provided by the auditee or other sources. On the other hand, analysing data by remotely accessing the auditee's server and observing work performed by remote surveillance are examples of audit methods that do not involve human interaction, as they do not require any direct communication with the auditee or other parties. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 7
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. Raise a nonconformity against control A.7.7, 'clear desk and clear screen' because the drives have been left unprotected on the desktop.
C. Record a nonconformity against control A.5.13 'labelling of information' as the disk drives' status was unclear
D. Raise a nonconformity against control A.7.5, 'protecting against physical and environmental threats' because the drives have been left exposed on the desktop.
E. Record an opportunity for improvement in respect of the external provider's inventory management arrangements.
F. Ensure that the organisation's arrangements for the life cycle management of storage media have been adhered to.
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. Record the finding but note no further action is required as the pickup has now been rescheduled.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

1. Identifying the source of information
2.
3.
4.
5.
6.
7.

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.

Sampling the available data | Evaluating evidence against the audit criteria | Making audit conclusions | Verifying objective evidence | Gathering audit evidence | Recording audit findings

Answer:

In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

1. Identifying the source of information
2. Gathering audit evidence
3. Sampling the available data
4. Verifying objective evidence
5. Evaluating evidence against the audit criteria
6. Recording audit findings
7. Making audit conclusions

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.

Sampling the available data | Evaluating evidence against the audit criteria | Making audit conclusions | Verifying objective evidence | Gathering audit evidence | Recording audit findings

Explanation

A screenshot of a computer Description automatically generated

1. Identifying the source of information
2. Gathering audit evidence
3. Sampling the available data
4. Verifying objective evidence
5. Evaluating evidence against the audit criteria
6. Recording audit findings
7. Making audit conclusions

* Identifying the source of information (already given)
* Gathering audit evidence: This involves collecting information from various sources such as documents, records, interviews, and observations.

* Sampling the available data: Due to the vast amount of information available, auditors typically use sampling techniques to select representative data for closer scrutiny.
* Verifying objective evidence: This involves checking the accuracy, completeness, and reliability of the collected evidence.
* Evaluating evidence against the audit criteria: Auditors compare the collected evidence to the established criteria (e.g., standards, policies, procedures) to assess compliance and effectiveness.
* Recording audit findings: This involves documenting the results of the evaluation, including observations, conclusions, and recommendations.
* Making audit conclusions: Based on the recorded findings, auditors formulate overall conclusions about the status of the management system.
Therefore, the correct sequence is:
1. Identifying the source of information 2. Gathering audit evidence 3. Sampling the available data 4.
Verifying objective evidence 5. Evaluating evidence against the audit criteria 6. Recording audit findings 7.
Making audit conclusions

NEW QUESTION: 9
An employee caught temporarily storing an MP3 file in his workstation will not receive an IR.
A. True
B. False
Answer: B (LEAVE A REPLY)
An employee caught temporarily storing an MP3 file in his workstation will receive an IR, because this is also a violation of the organization's information security policy and acceptable use policy. An MP3 file is a type of media file that may contain copyrighted or illegal content, or may introduce malware or viruses into the organization's network. The employee should not store any unauthorized or personal files in his workstation, as this may compromise the confidentiality, integrity and availability of the organization's information assets. Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], [ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements], Example of an information security policy, Example of an acceptable use policy

NEW QUESTION: 10
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. Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified
B. Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit
C. Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised
D. Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale
E. Advise the auditee that you will arrange for the next audit to be an online audit to deal with the outstanding nonconformity
F. Note the progress made but hold the audit open until all corrective action has been cleared
G. Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity
H. Conduct an unannounced follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared
Answer: (SHOW ANSWER)
The four options for the actions you could take are A, C, F, and G. These options are consistent with the guidance and requirements of ISO 19011:2018, Clause 6.712. You could agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified (A), and document the agreement in the audit report1. You could close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised , and report the outcome to the audit client and other relevant parties1. You could note the progress made but hold the audit open until all corrective action has been cleared (F), and determine the need for another follow-up audit or other actions1. You could also advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity (G), as they are responsible for the overall management and coordination of the audit programme3. The other options are either not appropriate or not necessary for the situation. You should not recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit (B), as this may compromise the audit objectives and the audit programme1. You should not recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale (D), as this is not within your role or authority as an ISMS auditor4. You should not advise the auditee that you will arrange for the next audit to be an online audit to deal with the outstanding nonconformity (E), as this may not be feasible or effective depending on the nature and complexity of the nonconformity1. You should not conduct an unannounced follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared (H), as this may not be in accordance with the audit agreement or the audit programme1.

References: 1: ISO 19011:2018, Guidelines for auditing management systems, Clause 6.7 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 6: Closing an ISO/IEC 27001 audit \n3: ISO 19011:2018, Guidelines for auditing management systems, Clause 5.3 \n4: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 9.6

NEW QUESTION: 11
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.
A. Corrective and technical
B. Detective and managerial
C. Preventive and technical
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
Implement plan on a test basis - this comes under which section of PDCA
A. Plan
B. Do
C. Act
D. Check
Answer: B (LEAVE A REPLY)
Explanation
The PDCA cycle is a four-step method for managing and improving processes. The steps are Plan, Do, Check, and Act. In the Plan phase, the objectives and scope of the process are defined, and the resources and activities are planned. In the Do phase, the process is implemented on a test basis, and the results are recorded and analyzed1. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI
| IRCA

NEW QUESTION: 13
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:

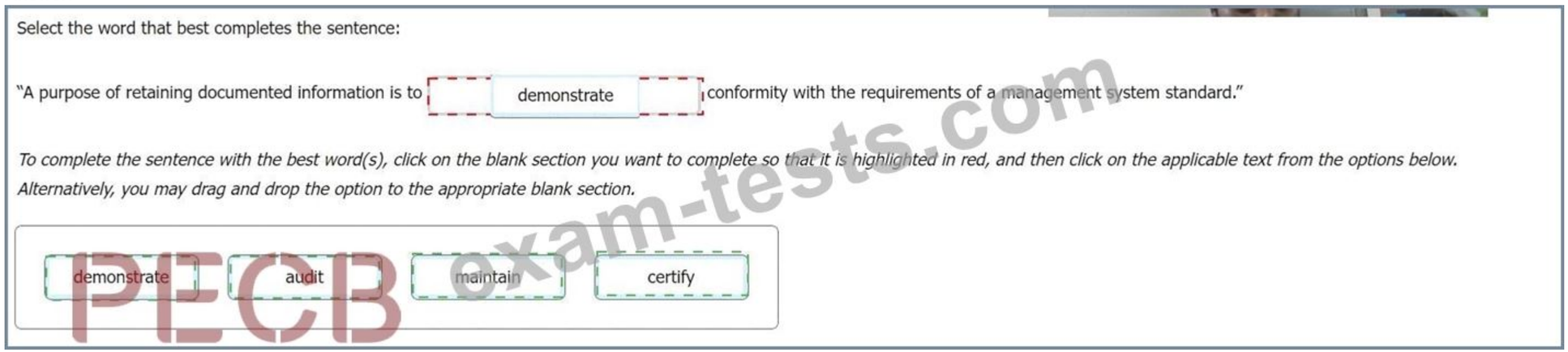
Reference:
ISO 19011:2022 Guidelines for auditing management systems
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements Components of Audit Findings - The Institute of Internal Auditors

NEW QUESTION: 14
The following are definitions of Information, except:
A. accurate and timely data
B. specific and organized data for a purpose
C. mature and measurable data
D. can lead to understanding and decrease in uncertainty
Answer: C (LEAVE A REPLY)
Explanation
The definition of information that is not correct is C: mature and measurable data. This is not a valid definition of information, as information does not have to be mature or measurable to be considered as such. Information can be any data that has meaning or value for someone or something in a certain context. Information can be subjective, qualitative, incomplete or uncertain, depending on how it is interpreted or used. Mature and measurable data are characteristics that may apply to some

types of information, but not all. The other definitions of information are correct, as they describe different aspects of information, such as accuracy and timeliness (A), specificity and organization (B), and understanding and uncertainty reduction (D). ISO/IEC
27001:2022 defines information as "any data that has meaning" (see clause 3.25). 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 Information?

NEW QUESTION: 15
Select the word that best completes the sentence:

Answer:



Explanation:

"A purpose of retaining documented information is to demonstrate conformity with the requirements of a management system standard."

The word that best completes the sentence is "demonstrate". According to ISO/IEC 27001:2022, Clause 7.5, the organization shall retain documented information as evidence of the performance of the processes and the conformity of the products and services with the requirements1. The purpose of retaining documented information is to demonstrate conformity with the requirements of the management system standard, not to maintain, audit, or certify it. References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 7.5

NEW QUESTION: 16
What is a repressive measure in case of a fire?
A. Repairing damage caused by the fire
B. Taking out a fire insurance
C. Putting out a fire after it has been detected by a fire detector
Answer: C (LEAVE A REPLY)
Explanation
A repressive measure is a measure that aims to reduce or eliminate the impact of an incident after it has occurred. Putting out a fire after it has been detected by a fire detector is an example of a repressive measure, as it reduces the damage caused by the fire. Taking out a fire insurance is not a repressive measure, but a corrective measure, as it compensates for the loss after the incident. Repairing damage caused by the fire is also not a repressive measure, but a recovery measure, as it restores the normal operation after the incident. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 28. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 29. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 30.

NEW QUESTION: 17
You are an ISMS audit team leader preparing to chair a closing meeting following a third-party surveillance audit. You are drafting a closing meeting agenda setting out the topics you wish to discuss with your auditee.
Which one of the following would be appropriate for inclusion?
A. A detailed explanation of the certification body's complaints process
B. An explanation of the audit plan and its purpose
C. A disclaimer that the result of the audit is based on the sampling of evidence
D. Names of auditees associated with nonconformities
Answer: C (LEAVE A REPLY)
This option is appropriate for inclusion in the closing meeting agenda, as it is a requirement of the ISO 19011 standard, which provides guidelines for auditing management systems, including ISMS12. The standard states that the audit team leader should advise the auditee of any situations encountered during the audit that may decrease the confidence that can be placed in the audit conclusions, such as limitations in the audit scope, access, or sampling3. The standard also states that the audit report should include a statement that the audit is based on a sample of the information available at the time of the audit, and that the audit does not provide absolute assurance of the conformity or effectiveness of the audited management system4. Therefore, the audit team leader should include a disclaimer in the closing meeting agenda to inform the auditee of the nature and limitations of the audit, and to avoid any misunderstandings or false expectations. The other options are not appropriate for inclusion in the closing meeting agenda, as they are either irrelevant, incorrect, or incomplete. For example:
*A detailed explanation of the certification body's complaints process is not relevant for the closing meeting agenda, as it is not related to the audit findings or conclusions. The certification body's complaints process should be communicated to the auditee before the audit, as part of the audit agreement or contract5.
*An explanation of the audit plan and its purpose is not correct for the closing meeting agenda, as it should have been done at the opening meeting or before the audit. The audit plan is a document that describes the scope, objectives, criteria, and methodology of the audit, as well as the audit schedule, the audit team, the audit locations, and the audit deliverables . The audit plan should be communicated and agreed with the auditee in advance, and any changes or deviations should be notified during the audit.

*Names of auditees associated with nonconformities are not complete for the closing meeting agenda, as they do not provide the details or the evidence of the nonconformities. The audit team leader should present the audit findings, which include the description, the audit criteria, and the audit evidence of each nonconformity, as well as the audit conclusions and the audit recommendation . The audit team leader should also avoid naming or blaming individuals, and focus on the processes and the system.
References: = 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, page 222: ISO 19011:2018 Guidelines for auditing management systems, clause 13: ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.94: ISO 19011:2018 Guidelines for auditing management systems, clause
7.5.25: ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, clause 9.8. : ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.1. : ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 6.2.1. : ISO 19011:
2018 Guidelines for auditing management systems, clause 6.4.2. : ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.10. : ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 6.3.3.

NEW QUESTION: 18
You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

Item	Findings	Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.	Clause 7.4 and Control A.5.24	N/A

Nonconformities (NCs)

Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.

Team Leader signed by *Audit*

Select one option of the recommendation to the audit programme manager you are going to advise to the auditee at the closing meeting.

A. Recommend certification immediately

B. Recommend that a full scope re-audit is required within 6 months

C. Recommend that an unannounced audit is carried out at a future date

D. Recommend certification after your approval of the proposed corrective action plan Recommend that the findings can be closed out at a surveillance audit in 1 year

E. Recommend that a partial audit is required within 3 months

Answer: (SHOW ANSWER)

According to ISO/IEC 17021-1:2015, which specifies the requirements for bodies providing audit and certification of management systems, clause 9.4.9 requires the certification body to make a certification decision based on the information obtained during the audit and any other relevant information1. The certification body should also consider the effectiveness of the corrective actions taken by the auditee to address any nonconformities identified during the audit1. Therefore, when making a recommendation to the audit programme manager, an ISMS auditor should consider the nature and severity of the nonconformities and the proposed corrective actions.

Based on the scenario above, the auditor should recommend certification after their approval of the proposed corrective action plan and recommend that the findings can be closed out at a surveillance audit in 1 year. The auditor should provide the following justification for their recommendation:
* Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. 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. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.
The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:
* Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.
* Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:
20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.
* Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.
* Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors.
A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.
References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 19
Auditors need to communicate effectively with auditees. Therefore, their personal behaviour is a key characteristic needed to ensure a successful audit. Below there are the characteristics and a brief related description. Match the characteristics to the descriptions.

Descriptions	Auditor's characteristics
Actively observing surroundings/activities	
Fair, truthful, sincere, honest, discreet	
Persistent and focused on objectives	
Willing to learn from situations	
Tactful in dealing with individuals	
Aware of and able to understand situations	

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.

Tenacious | Ethical | Diplomatic | Observant | Perceptive | Open to improvement

Answer:

Descriptions	Auditor's characteristics
Actively observing surroundings/activities	Observant
Fair, truthful, sincere, honest, discreet	Ethical
Persistent and focused on objectives	Tenacious
Willing to learn from situations	Open to improvement
Tactful in dealing with individuals	Diplomatic
Aware of and able to understand situations	Perceptive

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.

Tenacious | Ethical | Diplomatic | Observant | Perceptive | Open to improvement

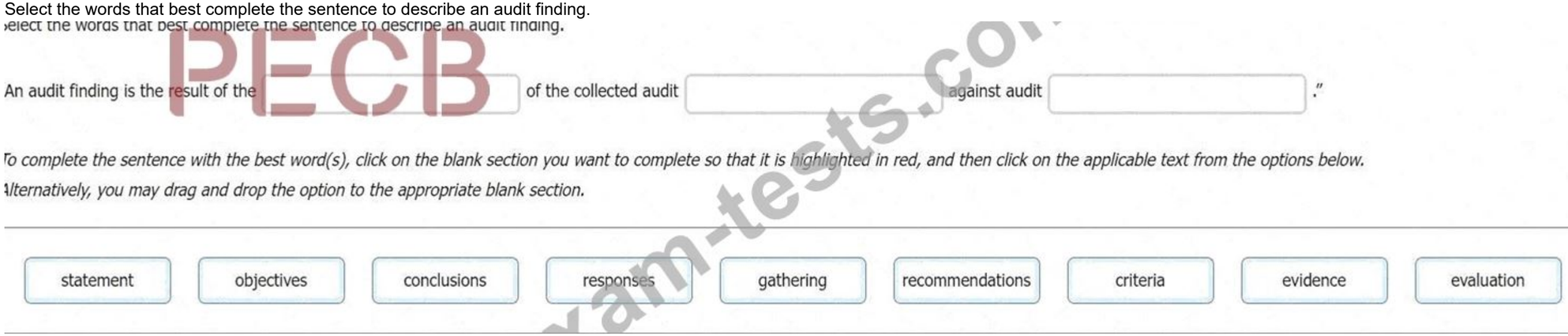
Explanation:
The possible matches of the characteristics to the descriptions are:
* Tenacious: Persistent and focused on objectives
* Ethical: Fair, truthful, sincere, honest, discreet
* Diplomatic: Tactful in dealing with individuals
* Observant: Actively observing surroundings/activities
* Perceptive: Aware of and able to understand situations
* Open to improvement: Willing to learn from situations
Actively observing surroundings/activities = Observant
Fair, truthful, sincere, honest, discreet = Ethical
Persistent and focused on objectives = Tenacious
Willing to learn from situations = Open to improvement
Tactful in dealing with individuals = Diplomatic
Aware of and able to understand situations = Perceptive
These are the auditor's characteristics and their descriptions as defined by ISO 19011:2022, Clause 7.2.21. The auditor's personal behaviour is essential for building trust and confidence with the auditee and for ensuring the credibility and effectiveness of the audit12. References: 1: ISO 19011:2022, Guidelines for auditing management systems, Clause 7.2.2 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 3: Fundamental audit concepts and principles

NEW QUESTION: 20
Question
An organization requires all employees to undergo security awareness training every six months. The training covers topics such as recognizing phishing attacks, handling sensitive data, and reporting security incidents.
After completing the training, employees must pass a short quiz to demonstrate their understanding.
What type of control does this activity represent?
A. Legal
B. Managerial
C. Administrative
Answer: C (LEAVE A REPLY)
Explanation (ISO-aligned)
* Security awareness training is an administrative (organizational) control.
* ISO/IEC 27002:2022 A.6.3 (Information security awareness, education and training) explicitly categorizes training as an administrative control.
* It governs human behavior through policy, procedures, and education, not technology or law.
Legal controls relate to regulations.
Managerial controls relate to governance decisions.
Correct classification: Administrative control.

NEW QUESTION: 21
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:
Who is primarily responsible for the preparation and content of the audit report?
A. Audit team leader
B. Audit team member
C. Certification body
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO 19011:2018 states that the audit team leader is responsible for compiling and finalizing the audit report.
* B. Incorrect:
* Team members contribute findings, but the leader ensures finalization.
* C. Incorrect:
* The certification body reviews but does not prepare the report.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.7.1 (Audit Report Preparation and Approval)

NEW QUESTION: 22
Select the words that best complete the sentence to describe an audit finding.



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: 23
What is social engineering?
A. A group planning for a social activity in the organization
B. Creating a situation wherein a third party gains confidential information from you
C. The organization planning an activity for welfare of the neighborhood
Answer: B (LEAVE A REPLY)
Explanation
Social engineering is a technique that involves creating a situation wherein a third party gains confidential information from you by manipulating your trust or exploiting your weaknesses. Social engineering can take various forms, such as phishing emails, phone calls, impersonation, or baiting. Social engineering is a common threat to information security, as it targets the human factor rather than the technical defenses. References: :
CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 26. : ISO/IEC 27001 LEAD AUDITOR
- PECB, page 13.

NEW QUESTION: 24
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: B (LEAVE A REPLY)
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: 25
During a third-party certification audit, you are presented with a list of issues by an auditee. Which four of the following constitute 'internal' issues in the context of a management system to ISO 27001:2022?
A. Higher labour costs as a result of an aging population
B. A rise in interest rates in response to high inflation
C. Poor levels of staff competence as a result of cuts in training expenditure
D. Poor morale as a result of staff holidays being reduced
E. Increased absenteeism as a result of poor management
F. A reduction in grants as a result of a change in government policy
G. A fall in productivity linked to outdated production equipment
H. Inability to source raw materials due to government sanctions
Answer: (SHOW ANSWER)
Explanation
According to ISO 27001:2022 clause 4.1, the organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system (ISMS)12 External issues are factors outside the organisation that it cannot control, but can influence or adapt to. They include political, economic, social, technological, legal, and environmental factors that may affect the organisation's information

security objectives, risks, and opportunities12 Internal issues are factors within the organisation that it can control or change. They include the organisation's structure, culture, values, policies, objectives, strategies, capabilities, resources, processes, activities, relationships, and performance that may affect the organisation's information security management system12 Therefore, the following issues are considered 'internal' in the context of a management system to ISO 27001:2022:

Poor levels of staff competence as a result of cuts in training expenditure: This is an internal issue because it relates to the organisation's capability, resource, and process of developing and maintaining the competence of its personnel involved in the ISMS. The organisation can control or change its training expenditure and its impact on staff competence12 Poor morale as a result of staff holidays being reduced: This is an internal issue because it relates to the organisation's culture, value, and relationship with its employees. The organisation can control or change its staff holiday policy and its impact on staff morale12 Increased absenteeism as a result of poor management: This is an internal issue because it relates to the organisation's performance, structure, and accountability of its management. The organisation can control or change its management practices and its impact on staff absenteeism12 A fall in productivity linked to outdated production equipment: This is an internal issue because it relates to the organisation's capability, resource, and process of ensuring the availability and suitability of its production equipment. The organisation can control or change its equipment maintenance and upgrade and its impact on productivity12 The following issues are considered 'external' in the context of a management system to ISO 27001:2022:

Higher labour costs as a result of an aging population: This is an external issue because it relates to the social and demographic factor that affects the availability and cost of labour in the market. The organisation cannot control or change the aging population, but can influence or adapt to its impact on labour costs12 A rise in interest rates in response to high inflation: This is an external issue because it relates to the economic and monetary factor that affects the cost and availability of capital in the market. The organisation cannot control or change the interest rates or inflation, but can influence or adapt to its impact on capital costs12 A reduction in grants as a result of a change in government policy: This is an external issue because it relates to the political and legal factor that affects the availability and conditions of public funding for the organisation. The organisation cannot control or change the government policy, but can influence or adapt to its impact on grants12 Inability to source raw materials due to government sanctions: This is an external issue because it relates to the political and legal factor that affects the availability and cost of raw materials in the market. The organisation cannot control or change the government sanctions, but can influence or adapt to its impact on raw materials12 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: 26

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: A,D (LEAVE A REPLY)

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: 27

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: C,E,F (LEAVE A REPLY)
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: 28
In what part of the process to grant access to a system does the user present a token?
A. Authorisation
B. Verification
C. Authentication

D. Identification
Answer: (SHOW ANSWER)
In what part of the process to grant access to a system does the user present a token? The user presents a token in the identification part of the process. Identification is the process of claiming an identity or presenting an identifier to a system. An identifier is a unique name or label that represents a person or entity. A token is a physical device or object that contains or generates an identifier, such as a smart card, a key fob, or a QR code. Identification is used to initiate the access request and associate it with an identity. Identification is followed by authentication, which verifies the identity claim, and authorization, which determines the level of access granted. ISO/IEC 27001:2022 defines identification as "recognition of an entity by an identifier in a particular context" (see clause 3.29). Reference: [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 Identification?]

NEW QUESTION: 29
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: B (LEAVE A REPLY)
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.

NEW QUESTION: 30
The data center at which you work is currently seeking ISO/IEC27001:2022 certification. In preparation for your initial certification visit a number of internal audits have been carried out by a colleague working at another data centre within your Group. They secured their 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 Certrfication Body arrives.
Which six of the following would cause you concern in respect of conformity to ISO/IEC 27001:2022 requirements?
A. The audit programme shows management reviews taking place at irregular intervals during the year

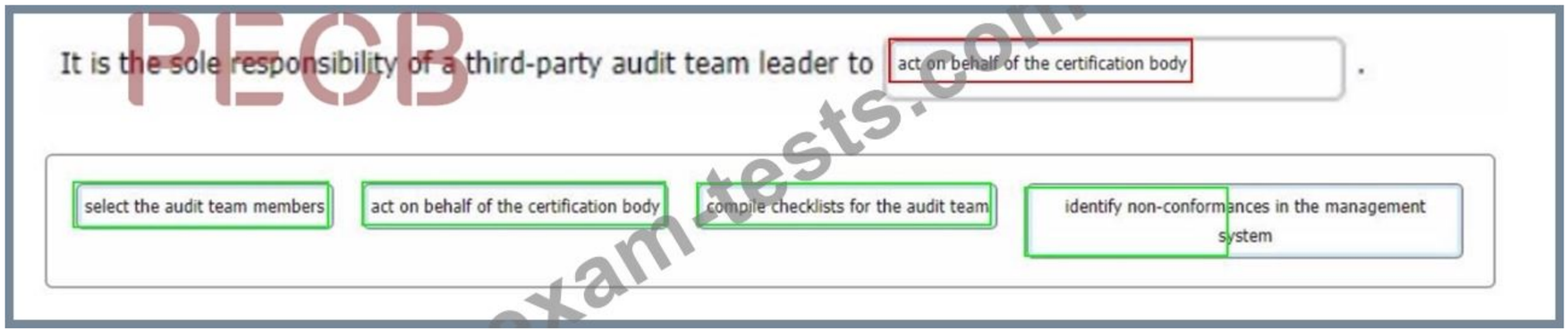
B. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet
C. The audit programme does not take into account the relative importance of information security processes
D. The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022
E. Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date
F. Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes
G. The audit programme does not reference audit methods or audit responsibilities
H. The audit programme does not take into account the results of previous audits
I. Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme
J. The audit process states the results of audits will be made available to 'relevant' managers, not top management
Answer: A,C,E,F,H,I (LEAVE A REPLY)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 9.3 requires top management to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness1. Clause 9.2 requires the organization to conduct internal audits at planned intervals to provide information on whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022, and is effectively implemented and maintained1. Therefore, when reviewing the audit process and audit findings as a final check before the external certification body arrives, an internal ISMS auditor should verify that these clauses are met in accordance with the audit criteria.
Six of the following statements would cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* The audit programme shows management reviews taking place at irregular intervals during the year:
This statement would cause concern because it implies that the organization is not conducting management reviews at planned intervals, as required by clause 9.3. This may affect the ability of top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS.
* The audit programme does not take into account the relative importance of information security processes: This statement would cause concern because it implies that the organization is not applying a risk-based approach to determine the audit frequency, methods, scope and criteria, as recommended by ISO 19011:2018, which provides guidelines for auditing management systems2. This may affect the ability of the organization to identify and address the most significant risks and opportunities for its ISMS.
* Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date: This statement would cause concern because it implies that the organization is not establishing audit criteria for each internal audit, as required by clause 9.2. Audit criteria are the set of policies, procedures or requirements used as a reference against which audit evidence is compared2.
Without audit criteria, it is not possible to determine whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022.
* Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes: This statement would cause concern because it implies that the organization is not evaluating the effectiveness of ISMS processes, as required by clause 9.1. Effectiveness is the extent to which planned activities are realized and planned results achieved2. Efficiency is the relationship between the result achieved and the resources used2. Both aspects are important for measuring and evaluating ISMS performance and improvement.
* The audit programme does not take into account the results of previous audits: This statement would cause concern because it implies that the organization is not using the results of previous audits as an input for planning and conducting subsequent audits, as recommended by ISO 19011:20182. This may affect the ability of the organization to identify and address any recurring or unresolved issues or nonconformities related to its ISMS.
* Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme: This statement would cause concern because it implies that the organization is not verifying that top management demonstrates leadership and commitment with respect to its ISMS, as required by clause 5.1. This may affect the ability of top management to ensure that the ISMS policy and objectives are established and compatible with the strategic direction of the organization; that roles, responsibilities and authorities for relevant roles are assigned and communicated; that resources needed for the ISMS are available; that communication about information security matters is established; that continual improvement of the ISMS is promoted; that other relevant management reviews are aligned with those of information security; and that support is provided to other relevant roles1.
The other statements would not cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific format or media for documenting or storing audit reports, as long as they are controlled according to clause 7.5.
* The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for auditor independence, as long as the audit is conducted objectively and impartially, in accordance with ISO 19011:20182.
* The audit programme does not reference audit methods or audit responsibilities: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for referencing audit methods or audit responsibilities in the audit programme, as long as they are defined and documented according to ISO 19011:20182.

* The audit process states the results of audits will be made available to 'relevant' managers, not top management: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for communicating the results of audits to top management, as long as they are reported to the relevant parties and used as an input for management review, according to clause 9.3.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 31
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. The audit programme does not take into account the relative importance of information security processes.
B. The audit process states the results of audits will be made available to 'relevant' managers, not top management.
C. Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date.
D. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as *. PDF documents on the organisation's intranet.
E. The audit programme shows management reviews taking place at irregular intervals during the year.
F. The audit programme does not reference audit methods or audit responsibilities.
G. The audit programme does not take into account the results of previous audits.
H. The audit programme has not been signed as 'approved by Top Management.
Answer: A,C,F,G (LEAVE A REPLY)

NEW QUESTION: 32
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:



Reference:
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: 33
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.
Based on Scenario 1, which international standard did Northstorm adopt during the second phase of expansion?
A. ISO/IEC 27701
B. ISO/IEC 27009
C. ISO/IEC 27003
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth
Northstorm adopted an international standard for Personally Identifiable Information (PII) controllers and PII processors to ensure its data handling practices were secure and compliant with global regulations. This aligns directly with ISO/IEC 27701, which extends ISO/IEC 27001 and ISO/IEC 27002 to cover Privacy Information Management Systems (PIMS), specifically addressing the protection of PII.
A . ISO/IEC 27701 - Correct Answer. This standard is designed for organizations acting as PII controllers and processors and provides guidelines on privacy management, regulatory compliance, and data protection.
B . ISO/IEC 27009 - Incorrect because this standard provides guidance on sector-specific requirements for ISMS, not privacy or PII protection.
C . ISO/IEC 27003 - Incorrect because it provides general implementation guidance for ISMS, not specific controls for PII processing.

NEW QUESTION: 34
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:
According to scenario 2, the ISMS scope was not applied to the Finance and HR Department of Knight. Is this acceptable?
A. Yes, the ISMS scope can include the whole organization or only particular departments within the organization
B. No, the ISMS scope must include all organizational units and processes
C. Yes, the ISMS must be applied only to processes and assets that may directly impact information security
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Which two of the following statements are true?
A. The benefits of implementing an ISMS primarily result from a reduction in information security risks
B. The benefit of certifying an ISMS is to obtain contracts from governmental institutions
C. The purpose of an ISMS is to apply a risk management process for preserving information security
D. The purpose of an ISMS is to demonstrate compliance with regulatory requirements
Answer: A,C (LEAVE A REPLY)
The benefits of implementing an ISMS are not limited to a reduction in information security risks, but also include improved business performance, customer satisfaction, legal compliance, and stakeholder confidence. The benefit of certifying an ISMS is not only to obtain contracts from governmental institutions, but also to demonstrate the organisation's commitment to information security to other potential customers, partners, and regulators. The purpose of an ISMS is to apply a risk management process for preserving information security, which means identifying, analysing, evaluating, treating, monitoring, and reviewing the information security risks that the organisation faces. The purpose of an ISMS is not to demonstrate compliance with regulatory requirements, but rather to ensure that the organisation meets its own information security objectives and obligations.
Reference:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements [Section 0.1] and [Section 1]

NEW QUESTION: 36
Phishing is what type of Information Security Incident?
A. Private Incidents

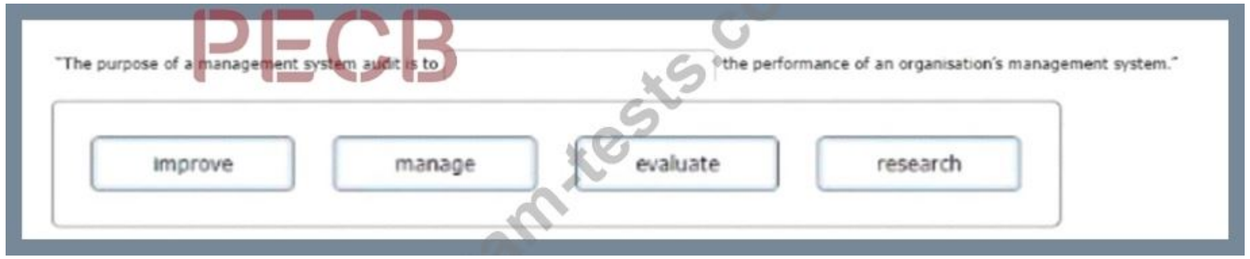
B. Cracker/Hacker Attacks
C. Technical Vulnerabilities
D. Legal Incidents
Answer: (SHOW ANSWER)
Explanation
Phishing is a type of information security incident that falls under the category of cracker/hacker attacks.
Phishing is a form of fraud that uses deceptive emails or other messages to trick recipients 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.
Phishing is a common and serious threat to information security, as it can lead to identity theft, financial loss, data breach, malware infection or other damages. 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: 37
Scenario 9
CloudFort, a small networking company, provides network security, cloud computing, and virtualization solutions. The company has recently been certified in an information security management system (ISMS) based on the ISO/IEC 27001 standard, which has resulted in a spike in its recognition, confirming the maturity of CloudFort's operation.
CloudFort continually reviewed and enhanced its security controls and the overall effectiveness and efficiency of the ISMS by conducting internal audits. Due to its size and desire for greater objectivity, the top management decided to outsource the internal audit function to ensure the internal audit is independent of the audited activities and holds an advisory role in the continual improvement of the ISMS.
After the initial certification audit, the company created a new department specializing in data storage solutions. It offered routers and switches optimized for data centers and software-based networking devices, such as network virtualization and network security appliances. Because of the new department, CloudFort initiated a risk assessment process and an internal audit. Following the internal audit results, the company confirmed the effectiveness and efficiency of the new processes and controls.
After determining that the new department fully complies with ISO/IEC 27001 requirements, top management decided to include it in the certification scope. They submitted a request to the certification body for an extension of the certification scope to ensure that the department's processes and security measures fully align with the overall ISMS.
One year after the initial certification audit, the certification body conducted another audit of CloudFort's ISMS. This audit aimed to determine CloudFort's 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 fulfills the standard requirements. Nonetheless, the new department introduced changes that significantly affected how the overall management system was governed, requiring updates to existing processes and controls.
Moreover, although CloudFort requested an extension of the certification scope, they failed to provide timely updates on the impact of the new department on the ISMS to the certification body. Thus, CloudFort's certification was suspended.
Question
CloudFort requested an extension of the certification scope to include the new department. How would you classify this situation? Refer to Scenario 9.
A. Unacceptable, because the extension should have been included in the initial certification scope and cannot be added afterward unless a major recertification process is undertaken.
B. Acceptable, many auditees can define a reduced scope for the first certification and then request for an extension during the following years.
C. Unacceptable, as expanding the scope requires a complete audit of the organization again.
Answer: B (LEAVE A REPLY)
This situation is acceptable, making option B the correct answer. ISO/IEC 17021-1 and ISO/IEC 27006 explicitly allow certified organizations to request an extension of the certification scope after initial certification. It is common and fully permissible for organizations to begin with a limited or reduced scope and later expand it as the ISMS matures, business operations grow, or new departments are created.
ISO/IEC 27001 does not require the full organization to be included in the initial certification scope. Instead, it requires the scope to be clearly defined, documented, and controlled. When CloudFort created a new department, it correctly initiated a risk assessment and internal audit, and then formally requested a scope extension from the certification body. This demonstrates alignment with ISO requirements and good ISMS governance.
Option A is incorrect because scope extensions do not require a full recertification audit unless the certification body determines that the changes are so extensive that they fundamentally alter the ISMS. Option C is also incorrect because expanding the scope does not automatically require a complete re-audit of the entire organization; the certification body typically performs a focused extension audit covering the new scope elements and their interaction with the existing ISMS.
The suspension in Scenario 9 occurred not because the scope extension request was unacceptable, but because CloudFort failed to provide timely and sufficient information to the certification body regarding the impact of the new department. The act of requesting a scope extension itself was appropriate and acceptable.

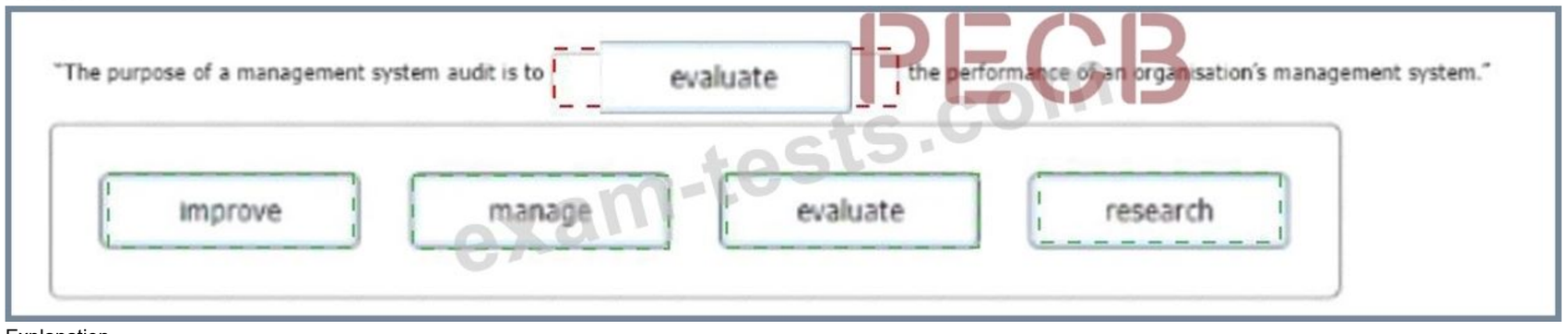
NEW QUESTION: 38
You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.
You are currently in a large room that is subdivided into several smaller rooms, each of which has a numeric 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: 39
Select a word from the following options that best completes 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.



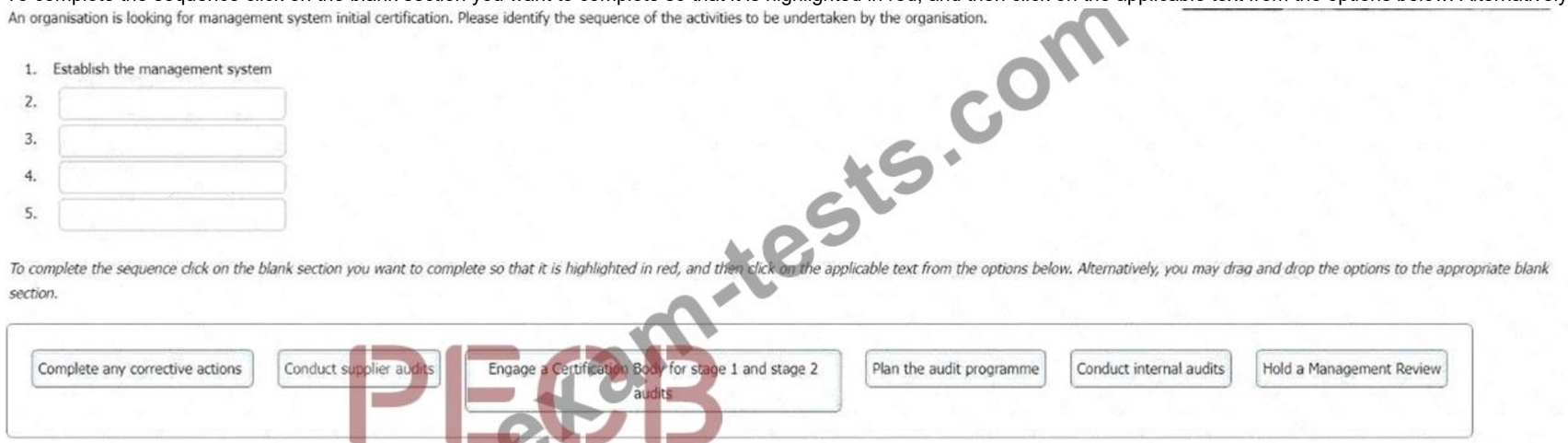
Answer:



Explanation

The purpose of a management system audit is to evaluate the performance of an organization's management system.
A management system audit is an independent and systematic analysis and evaluation of a company's overall activities and performances1. It is a valuable tool used to determine the efficiency, functions, accomplishments and achievements of the company1. A management system audit can be conducted against a range of audit criteria, including (but not limited to) requirements set of in existing ISO standards2.
According to ISO 19011:2018, which provides guidelines for auditing management systems, the purpose of an audit is to enable the auditor to provide an audit conclusion that is related to the audit objectives2. 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 system2.
Therefore, the correct answer is evaluate, as it best describes the purpose of a management system audit. The other options are not correct because they are not specific enough or do not reflect the intended outcome of an audit. For example, improve implies that the audit itself will enhance the performance of the management system, which is not necessarily true. Manage implies that the audit will control or direct the management system, which is not its role. Research implies that the audit will generate new knowledge or information about the management system, which is not its primary aim.

NEW QUESTION: 40
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.



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: 41
Which of the following does an Asset Register contain? (Choose two)
A. Asset Type
B. Asset Owner
C. Asset Modifier
D. Process ID
Answer: A,B (LEAVE A REPLY)

An asset register is a document that contains information about the assets associated with information and information processing facilities within the scope of the information security management system. An asset register should include, among other things, the asset type and the asset owner. The asset type is a category or classification of the asset, such as hardware, software, data, document, service, etc. The asset owner is a person or entity that has been assigned the responsibility for managing and protecting the asset throughout its lifecycle. The asset type and the asset owner are important information for identifying and controlling the assets, as well as for performing risk assessments and applying security controls. ISO/IEC 27001:2022 requires the organization to maintain an inventory of assets within the scope of the information security management system (see clause A.8.1.1). Reference: 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 an Asset Register?

NEW QUESTION: 42
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: 43
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 ??
A. You will ask to see the ID card of the person that is on the screen.
B. You will take photos of every person you interview.
C. You will ask those being interviewed to state their name and position beforehand.
D. You will ask for a 360-degree view of the room where the audit is being carried out.
E. You will not record any part of the audit, unless permitted.
F. You expect the auditee to have assessed all risks associated with online activities.
Answer: (SHOW ANSWER)
Explanation
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: 44
Which two of the following are examples of audit methods that 'do not' involve human interaction?
* Conducting an interview using a teleconferencing platform
A. Performing a review of auditees procedures in preparation for an audit
B. Reviewing the auditee's response to an audit finding
C. Analysing data by remotely accessing the auditee's server
D. Observing work performed by remote surveillance
E. Confirming the date and time of the audit
Answer: B,D (LEAVE A REPLY)
Audit methods are the techniques and procedures that auditors use to collect and evaluate audit evidence.
Audit methods can be classified into two categories: those that involve human interaction and those that do not. Human interaction methods are those that require direct or indirect communication with the auditee or other relevant parties, such as interviews, questionnaires, surveys, observations, or walkthroughs. Non-human interaction methods are those that do not require any communication with the auditee or other parties, such as document reviews, data analysis, or remote surveillance.
Some examples of audit methods that do not involve human interaction are:
* Performing a review of auditee's procedures in preparation for an audit: This method involves examining the auditee's documented information, such as policies, processes, records, or reports, to verify their adequacy and effectiveness in meeting the audit criteria. The auditor does not need to interact with the auditee or anyone else to perform this method.
* Analysing data by remotely accessing the auditee's server: This method involves accessing and processing the auditee's data, such as performance indicators, logs, metrics, or statistics, to verify their accuracy and reliability in meeting the audit criteria. The auditor does not need to interact with the auditee or anyone else to perform this method.
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: 45
You are an experienced ISMS auditor, currently providing support to an ISMS auditor in training who is carrying out her first initial certification audit. She asks you what she should be verifying when auditing an organisation's Information Security objectives. You ask her what she has included in her audit checklist and she provides the following replies.
Which three of these responses would you cause you concern in relation to conformity with ISO/IEC
27001:2022?
A. I am going to check how each Information Security objective has been communicated to those who need to be aware of it in order for the objective to be achieved
B. I am going to check that top management have determined the Information Security objectives for the current year. If not, I will check that this task has been programmed to be completed
C. I am going to check that the Information Security objectives are written down on paper so that everyone is clear on what needs to be achieved, how it will be achieved, and by when it will be achieved
D. I am going to check that there is a process in place to periodically revisit Information Security objectives, with a view to amending or cancelling them if circumstances necessitate this
E. I am going to check that a completion date has been set for each objective and that there are no objectives with missing 'achieve by' dates
F. I am going to check that the necessary budget, manpower and materials to achieve each objective has been determined
G. I am going to check that all the Information Security objectives are measurable. If they are not measurable the organisation will not be able to track progress against them
Answer: (SHOW ANSWER)
Explanation

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 6.2 requires an organization to establish information security objectives at relevant functions and levels1. The objectives should be consistent with the information security policy; measurable (if practicable) or capable of being evaluated; monitored; communicated; updated as appropriate1. Therefore, when auditing an organization's information security objectives, an ISMS auditor should verify these aspects in accordance with the audit criteria.
Three responses from the ISMS auditor in training that would cause concern in relation to conformity with ISO/IEC 27001:2022 are:
I am going to check that top management have determined the Information Security objectives for the current year. If not, I will check that this task has been programmed to be completed: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives at relevant functions and levels, not just at the top management level. It also implies that the auditor in training is willing to accept a delay or postponement in determining the information security objectives, which may affect the ISMS performance and effectiveness.
I am going to check that the Information Security objectives are written down on paper so that everyone is clear on what needs to be achieved, how it will be achieved, and by when it will be achieved: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives that are measurable (if practicable) or capable of being evaluated, not just written down on paper. It also implies that the auditor in training is not aware of the flexibility and suitability of different media or formats for documenting and communicating information security objectives, such as electronic or digital records, posters, newsletters, etc.
I am going to check that a completion date has been set for each objective and that there are no objectives with missing 'achieve by' dates: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives that are monitored, not just completed by a certain date. It also implies that the auditor in training is not aware of the possibility and necessity of updating information security objectives as appropriate, such as when changes occur in the internal or external context of the organization, or when new risks or opportunities arise.
The other responses from the ISMS auditor in training are acceptable and do not cause concern in relation to conformity with ISO/IEC 27001:2022. For example, checking how each Information Security objective has been communicated to those who need to be aware of it in order for the objective to be achieved is relevant to verifying the communication aspect of clause 6.2; checking that there is a process in place to periodically revisit Information Security objectives, with a view to amending or cancelling them if circumstances necessitate this is relevant to verifying the updating aspect of clause 6.2; checking that the necessary budget, manpower and materials to achieve each objective has been determined is relevant to verifying the planning aspect of clause 6.2; checking that all the Information Security objectives are measurable. If they are not measurable the organisation will not be able to track progress against them is relevant to verifying the measurability aspect of clause 6.2. References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 46
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 PEOPLE controls listed in the Statement of Applicability (SoA) and mplemented 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 protection against malware is implemented
C. Information security awareness, education and training
D. Remote working arrangements
E. The conducting of verification checks on personnel
F. The operation of the site CCTV and door control systems
G. The organisation's arrangements for information deletion
H. The organisation's business continuity arrangements
Answer: (SHOW ANSWER)
Explanation
The PEOPLE controls are related to the human aspects of information security, such as roles and responsibilities, awareness and training, screening and contracts, and remote working. The auditor in training should review the following controls:
* Confidentiality and nondisclosure agreements (A): These are contractual obligations that bind the employees and contractors of the organisation to protect the confidentiality of the information they handle, especially the data of external clients. The auditor should check if these agreements are signed, updated, and enforced by the organisation. This control is related to clause A.7.2.1 of ISO/IEC
27001:2022.
* Information security awareness, education and training : These are activities that aim to enhance the knowledge, skills, and behaviour of the employees and contractors regarding information security. The auditor should check if these activities are planned, implemented, evaluated, and improved by the organisation. This control is related to clause A.7.2.2 of ISO/IEC 27001:2022.

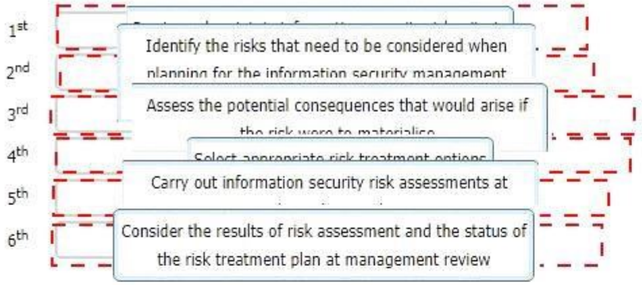
* Remote working arrangements (D): These are policies and procedures that govern the information security aspects of working from locations other than the organisation's premises, such as home or public places. The auditor should check if these arrangements are defined, approved, and monitored by the organisation. This control is related to clause A.6.2.1 of ISO/IEC 27001:2022.
* The conducting of verification checks on personnel (E): These are background checks that verify the identity, qualifications, and suitability of the employees and contractors who have access to sensitive
* information or systems. The auditor should check if these checks are conducted, documented, and reviewed by the organisation. This control is related to clause A.7.1.1 of ISO/IEC 27001:2022.
References:
* ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements
* PECB Candidate Handbook ISO/IEC 27001 Lead Auditor, 1
* ISO 27001:2022 Lead Auditor - IECB, 2
* ISO 27001:2022 certified ISMS lead auditor - Jisc, 3
* ISO/IEC 27001:2022 Lead Auditor Transition Training Course, 4
* ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy, 5

NEW QUESTION: 47
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:
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: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
C . Correct Answer: Changes to the audit scope must be approved by the auditee, the 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: 48
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?

Answer:



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

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: 49
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: 50
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 of ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organisation outsourced the mobile app development to a professional software development organisation with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified.
The IT Manager presents the software security management procedure and summarises 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 - Reference ID: 0098, details as follows:

Target of Test: ABC's healthcare mobile app, version 1	Test results	Test summary
Performance test		
Response time	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the response time.
Useability and user interface	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the user interface, size of the text, and colour.
Security test		
Access control (username and password)	PASS	Compliance with the organisation's information security policy, unique username and minimal 12 digits password (with Capital/Lower case, numbers, symbols combination)
Access control – One-time-password (OTP)	PASS	The mobile app generates an 8-digit OTP and sends it to an authorised user's mobile phone via SMS, as a second factor of identity authentication.
Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymization	Fail	Not able to perform the pseudonymization.
Final approval:		
		signed
by: *Service Manager*		

You would like to investigate other areas further to collect more audit evidence. Select three options that will not be in your audit trail.

A. Collect more evidence on how much residents' family members pay to install ABC's healthcare mobile app. (Relevant to clause 4.2)

B. Collect more evidence by downloading and testing the mobile app on your phone. (Relevant to control A.8.1)

C. Collect more evidence to determine the number of users of ABC's healthcare mobile app. (relevant to clause 4.2)

D. Collect more evidence on how the organisation performs testing of personal data handling. (Relevant to control A.5.34)

E. Collect more evidence on the organisation's business continuity policy. (Relevant to control A.5.30)

F. Collect more evidence on how the organisation manages information security in the selection of an external service provider. (Relevant to control A.5.19)

G. Collect more evidence on how the developer trains its product support personnel. (Relevant to clause 7.2)

H. Collect more evidence to verify the developer's CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certification. (Relevant to control A.5.21)

Answer: A,C,H (LEAVE A REPLY)

The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13. References: 1:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 51

There was a fire in a branch of the company Midwest Insurance. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost for good.
What is an example of the indirect damage caused by this fire?

A. Melted backup tapes

B. Burned computer systems

C. Burned documents

D. Water damage due to the fire extinguishers

Answer: D (LEAVE A REPLY)

An example of the indirect damage caused by the fire in the branch of Midwest Insurance is water damage due to the fire extinguishers. Indirect damage is the damage that occurs as a consequence of an incident, but not directly caused by it. Indirect damage can include loss of revenue, reputation, customers, market share, etc. In this case, the water damage due to the fire extinguishers is not directly caused by the fire itself, but by the actions taken to stop it. The water damage can affect other assets or information that were not burned by the fire, such as furniture, carpets, documents, etc. ISO/IEC 27001:2022 defines indirect impact as "impact resulting from consequences of an unwanted incident" (see clause 3.26).
Reference: [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 Indirect Damage?]

NEW QUESTION: 52

Select two options that describe an advantage of using a checklist.

A. Using the same checklist for every audit without review

B. Restricting interviews to nominated parties

C. Ensuring relevant audit trails are followed

D. Ensuring the audit plan is implemented

E. Reducing audit duration

F. Not varying from the checklist when necessary

Answer: (SHOW ANSWER)

Explanation
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: 53
You are performing an ISMS audit at a residential nursing home (ABC) that provides healthcare services. The next step in your audit plan is to verify the information security of 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 following:
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:

Target of Test: ABC's healthcare mobile app, version 1	Test results	Test summary
Security test		
Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymisation	Fail	Not able to perform the pseudonymisation.
Final approval:		
by: *Service Manager*		signed

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 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.
A. 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)
B. There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.

(Relevant to clause 8.1, control A.8.29)
C. There is a nonconformity (NC). The organisation and developer perform security tests that fail.
(Relevant to clause 8.1, control A.8.29)
D. 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)
Answer: D (LEAVE A REPLY)
The correct option is D. 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). The IT Manager should have approved the test results according to the software security management procedure, not the Service Manager. The Service Manager's decision to accept the failed security tests also violates the "security-by-design" and "security-by-default" principles that the organization adopted. The other options are either incorrect or irrelevant. The organization and developer did perform acceptance tests, but they failed (B, C). The Service Manager's decision to continue the service does not justify the nonconformity (A). References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 8.1 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5: Conducting an ISO/IEC 27001 audit

NEW QUESTION: 54
In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

Answer:

In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

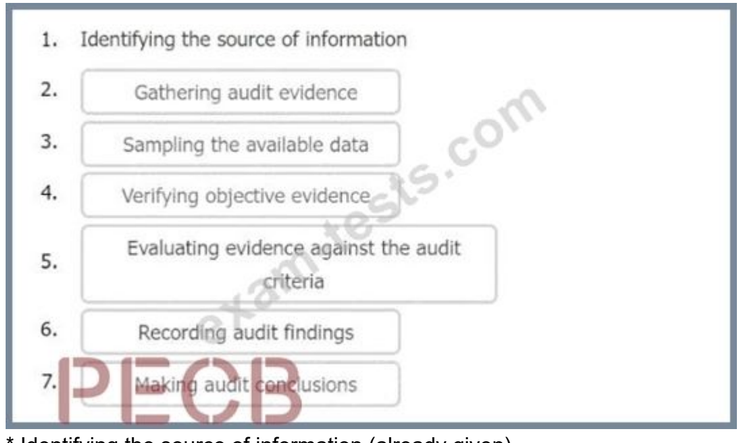
1. Identifying the source of information
2. Gathering audit evidence
3. Sampling the available data
4. Verifying objective evidence
5. Evaluating evidence against the audit criteria
6. Recording audit findings
7. Making audit conclusions

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.

Sampling the available data | Evaluating evidence against the audit criteria | Making audit conclusions | Verifying objective evidence | Gathering audit evidence | Recording audit findings

Explanation:

A screenshot of a computer Description automatically generated



* Identifying the source of information (already given)

* Gathering audit evidence: This involves collecting information from various sources such as documents, records, interviews, and observations.

* Sampling the available data: Due to the vast amount of information available, auditors typically use sampling techniques to select representative data for closer scrutiny.
* Verifying objective evidence: This involves checking the accuracy, completeness, and reliability of the collected evidence.
* Evaluating evidence against the audit criteria: Auditors compare the collected evidence to the established criteria (e.g., standards, policies, procedures) to assess compliance and effectiveness.
* Recording audit findings: This involves documenting the results of the evaluation, including observations, conclusions, and recommendations.
* Making audit conclusions: Based on the recorded findings, auditors formulate overall conclusions about the status of the management system.
Therefore, the correct sequence is:
1. Identifying the source of information 2. Gathering audit evidence 3. Sampling the available data 4.
Verifying objective evidence 5. Evaluating evidence against the audit criteria 6. Recording audit findings 7.
Making audit conclusions

NEW QUESTION: 55
You are an audit team leader who has just completed a third-party audit of a mobile telecommunication provider. You are preparing your audit report and are just about to complete a section headed 'confidentiality'.
An auditor in training on your team asks you if there are any circumstances under which the confidential report can be released to third parties.
Which four of the following responses are false?
A. Although we advise the client the report is confidential we can decide to release it to third parties if we feel this is justified. We would always tell the client afterwards
B. The report can be released to third parties but only with the explicit, prior approval of the audit client
C. There are no circumstances under which the report can be released to a third party. Confidential means confidential and releasing the document would be a breach of trust
D. The starting position is always that third parties have no automatic right to access an audit report
E. If the third party has gained a legal notice for us to disclose the report then we must do so. In all such cases we would advise the audit client and, as appropriate, the auditee
F. Any auditor employed by the auditing organisation can access the audit report
G. Our duty of confidentiality is not something that lasts forever. As a certification body, we can decide how long we wish to keep reports confidential. After this, they can be accessed by third parties making a subject access request
H. Subcontracted auditors are considered to be third parties regarding confidentiality and are therefore typically bound by confidentiality agreements
Answer: A,F,G,H (LEAVE A REPLY)
The audit report is a confidential document that contains sensitive information about the auditee's ISMS and its performance. The audit team has a duty to protect the confidentiality of the audit report and only disclose it to authorized parties, such as the audit client, the certification body, and the accreditation body. Therefore, the following responses are false:
* A: The audit team cannot decide to release the report to third parties without the consent of the audit client, as this would breach the confidentiality agreement and the audit code of conduct. The audit team should always inform the audit client before disclosing the report to any third party, and obtain their explicit, prior approval.
* F: Not every auditor employed by the auditing organization can access the audit report, as this would violate the principle of need-to-know. Only auditors who are involved in the audit process, such as the audit team leader, the audit team members, the audit programme manager, and the certification decision maker, can access the audit report. Other auditors who are not related to the audit have no legitimate reason to access the report, and should be prevented from doing so by appropriate security measures.
* G: The duty of confidentiality does not expire after a certain period of time, as this would compromise the trust and integrity of the audit process. The audit report remains confidential indefinitely, unless
* there is a legal or contractual obligation to disclose it, or the audit client agrees to release it. Third parties cannot access the audit report by making a subject access request, as this would infringe the privacy and data protection rights of the audit client and the auditee.
* H: Subcontracted auditors are not considered to be third parties regarding confidentiality, as they are part of the audit team and have a contractual relationship with the auditing organization. Subcontracted auditors are typically bound by the same confidentiality agreement and audit code of conduct as the employed auditors, and have the same rights and responsibilities to access and protect the audit report.
References: =
* ISO/IEC 27001:2022, clause 9.2, Internal audit
* ISO/IEC 27006:2015, clause 7.2.3, Confidentiality
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 22, Audit Report
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 24, Audit Code of Conduct

NEW QUESTION: 56
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:
Based on the information provided in Scenario 5, Cobt refused to provide the auditors with information on risk management. How would you, as an auditor, resolve such a situation?
A. By only accessing such information on-site or when Cobt's representatives are present
B. By refusing the audit mandate since it is within an auditor's right to do so when the confidentiality agreement is not followed
C. By reminding Cobt's representatives that the audit team leader decides the access that the audit team should have to information during the audit process
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
A . Correct Answer: When an organization refuses to share sensitive information off-site, the B . Incorrect: The auditor cannot immediately refuse the mandate. Instead, an attempt to reach an agreement should be made first.
C . Incorrect: While audit leaders define audit access, they must also respect confidentiality agreements.
Relevant Standard Reference:
ISO/IEC 27001:2022 Clause 9.2 (Internal Audit)
ISO 19011:2018 Clause 6.4.5 (Audit Information Availability and Access)

NEW QUESTION: 57
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: 58
_____ is a software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
A. Trojan
B. Operating System
C. Virus
D. Malware
Answer: (SHOW ANSWER)
Malware is a software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is a general term that covers various types of malicious software, such as viruses, worms, trojans, ransomware, spyware, adware, etc. Malware can cause serious damage to the organization's information assets and reputation, and may lead to legal or regulatory consequences. Therefore, the organization should implement appropriate controls to prevent, detect and remove malware, as specified in ISO/IEC 27001:2022 clause 12.2.1. Reference: [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 malware?

NEW QUESTION: 59
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 NO nonconformity (NC). The IT Manager demonstrates he is fully competent. (Relevant to clause 7.2)
B. 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)
C. There is a nonconformity (NC). The organisation does not control planned changes and review the consequences of unintended changes. (Relevant to clause 8.1)
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 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)
Answer: B,C (LEAVE A REPLY)
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 pseudonymization 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.
According to ISO 27001:2022 Clause 8.1, the organisation shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in Clause 6.1. The organisation shall also control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary12 In this case, the organisation has not controlled the planned change of the mobile app from version 1.0 to version 1.01, which was a minor update provided by the outsourced developer in response to frequent ransomware attacks. The IT Manager explains that the developer performed an emergency release of the updated software, and gave a verbal

guarantee that there will be no impact on any security functions. However, this is not sufficient to ensure that the change is properly assessed, tested, documented, and approved before deployment. The IT Manager should have followed the change management process and procedure, and verified that the updated software meets the security requirements and does not introduce any new vulnerabilities or risks. The IT Manager's reliance on his 20 years of information security experience and the developer's verbal guarantee is not a valid basis for skipping the re-testing of the software. Therefore, there is a nonconformity (NC) with clause 8.1.
Reference:
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: 60
What would be the reference for you to know who should have access to data/document?
A. Data Classification Label
B. Access Control List (ACL)
C. Masterlist of Project Records (MLPR)
D. Information Rights Management (IRM)
Answer: B (LEAVE A REPLY)
Explanation
The reference for you to know who should have access to data/document is the Access Control List (ACL), which is a list of users or groups who are authorized to access a specific data/document and their respective access rights (such as read, write, modify, delete, etc.). The ACL is a tool for implementing the access control policy of the organization, which is defined in accordance with ISO/IEC 27001:2022 clause 9.4.1. The ACL should be maintained and updated regularly to ensure that only authorized users can access the data/document. 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]

NEW QUESTION: 61
You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

Item	Findings	Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.	Clause 7.4 and Control A.5.24	N/A

Nonconformities (NCs)

Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.

signed by *Audit Team Leader*

Select one option of the recommendation to the audit programme manager you are going to advise to the auditee at the closing meeting.

A. Recommend certification immediately

B. Recommend that a full scope re-audit is required within 6 months

C. Recommend that an unannounced audit is carried out at a future date

D. Recommend certification after your approval of the proposed corrective action plan Recommend that the findings can be closed out at a surveillance audit in 1 year

E. Recommend that a partial audit is required within 3 months

Answer: D (LEAVE A REPLY)

According to ISO/IEC 17021-1:2015, which specifies the requirements for bodies providing audit and certification of management systems, clause 9.4.9 requires the certification body to make a certification decision based on the information obtained during the audit and any other relevant information1. The certification body should also consider the effectiveness of the corrective actions taken by the auditee to address any nonconformities identified during the audit1. Therefore, when making a recommendation to the audit programme manager, an ISMS auditor should consider the nature and severity of the nonconformities and the proposed corrective actions.

Based on the scenario above, the auditor should recommend certification after their approval of the proposed corrective action plan and recommend that the findings can be closed out at a surveillance audit in 1 year. The auditor should provide the following justification for their recommendation:

Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. 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. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:
Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.
Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.
Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.
Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.

NEW QUESTION: 62
In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

1. Identifying the source of information
2.
3.
4.
5.
6.
7.

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.

Sampling the available data | Evaluating evidence against the audit criteria | Making audit conclusions | Verifying objective evidence | Gathering audit evidence | Recording audit findings

Answer:

In the context of a management system audit, please identify the sequence of a typical process of collecting and verifying information. The first one has been done for you.

1. Identifying the source of information
2. Gathering audit evidence
3. Sampling the available data
4. Verifying objective evidence

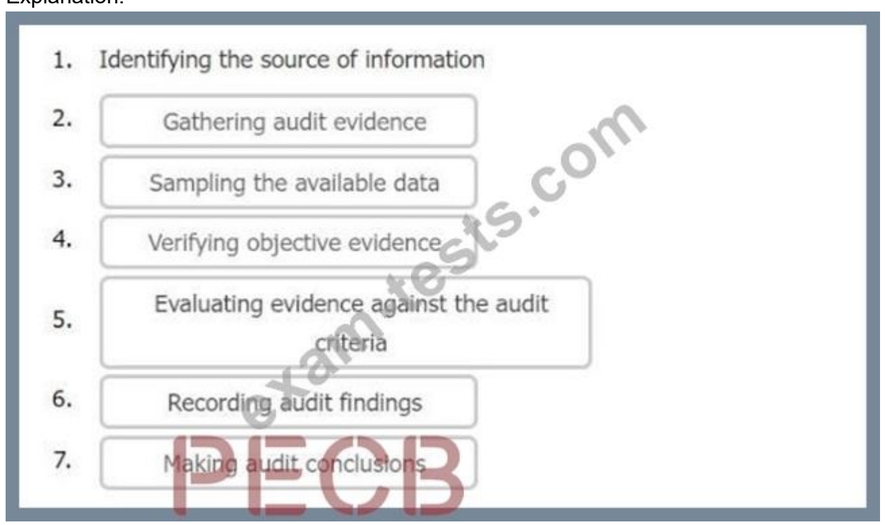
Evaluating evidence against the audit criteria

6. Recording audit findings
7. Making audit conclusions

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.

Sampling the available data | Evaluating evidence against the audit criteria | Making audit conclusions | Verifying objective evidence | Gathering audit evidence | Recording audit findings

Explanation:



* Identifying the source of information (already given)

* Gathering audit evidence: This involves collecting information from various sources such as documents, records, interviews, and observations.
* Sampling the available data: Due to the vast amount of information available, auditors typically use sampling techniques to select representative data for closer scrutiny.
* Verifying objective evidence: This involves checking the accuracy, completeness, and reliability of the collected evidence.
* Evaluating evidence against the audit criteria: Auditors compare the collected evidence to the established criteria (e.g., standards, policies, procedures) to assess compliance and effectiveness.
* Recording audit findings: This involves documenting the results of the evaluation, including observations, conclusions, and recommendations.
* Making audit conclusions: Based on the recorded findings, auditors formulate overall conclusions about the status of the management system.
Therefore, the correct sequence is:
1. Identifying the source of information 2. Gathering audit evidence 3. Sampling the available data 4.
Verifying objective evidence 5. Evaluating evidence against the audit criteria 6. Recording audit findings 7.
Making audit conclusions

NEW QUESTION: 63
Which of the following is a preventive security measure?
A. Installing logging and monitoring software
B. Shutting down the Internet connection after an attack
C. Storing sensitive information in a data save
Answer: C (LEAVE A REPLY)
A preventive security measure is a measure that aims to prevent or deter potential incidents from occurring, or to reduce their likelihood or impact. A preventive security measure can be a policy, a procedure, a device, a technique or an action that reduces the exposure to threats and vulnerabilities. Storing sensitive information in a data safe is an example of a preventive security measure, because it protects the information from unauthorized access, disclosure, modification or destruction by physical means, such as theft, fire, flood, etc. ISO/IEC 27001:2022 defines preventive control as "control that modifies risk by avoiding an unwanted incident" (see clause 3.19). Reference: [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 Preventive Security?]

NEW QUESTION: 64
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: B,D,E,F,I,J (LEAVE A REPLY)
Explanation
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: 65
Costs related to nonconformities and failures to comply with legal and contractual requirements are assessed when defining:
A. Materiality
B. Audit risks
C. Reasonable assurance
Answer: A (LEAVE A REPLY)
Materiality in the context of an audit involves assessing what level of nonconformities or failures, including those related to legal and contractual compliance, would be significant enough to affect the audit conclusions. Costs related to these issues are considered when determining materiality.

NEW QUESTION: 66
As a new member of the IT department you have noticed that confidential information has been leaked several times. This may damage the reputation of the company. You have been asked to propose an organisational measure to protect laptop computers. What is the first step in a structured approach to come up with this measure?
A. Encrypt all sensitive information
B. Formulate a policy
C. Appoint security staff
D. Set up an access control procedure
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Which one of the following statements best describes the purpose of conducting a document review?
A. To reveal whether the documented management system is nonconforming with audit criteria and to gather evidence to support the audit report
B. To decide about the conformity of the documented management system with audit standards and to gather findings to support the audit process
C. To determine the conformity of the management system, as far as documented, with audit criteria and to gather information to support the on-site audit activities
D. To detect any nonconformity of the management system, if documented, with audit criteria and to identify information to support the audit plan
Answer: C (LEAVE A REPLY)
A document review is a process of examining the documented information related to the management system before the on-site audit activities. The purpose of a document review is to: 12
* Determine the conformity of the management system, as far as documented, with audit criteria, i.e., to check whether the documents are consistent, complete, and compliant with the requirements of ISO/IEC 27001 and any other applicable standards or regulations.
* Gather information to support the on-site audit activities, i.e., to identify the scope, objectives, processes, controls, risks, and opportunities of the management system, and to plan the audit methods, techniques, and resources accordingly.
The other statements are not accurate, because:
* A document review does not reveal or decide about the conformity or nonconformity of the management system as a whole, but only of the documented information. The conformity or nonconformity of the management system is determined by the on-site audit activities, which include interviews, observations, and tests12
* A document review does not gather evidence or findings to support the audit report or process, but information to support the on-site audit activities. The evidence or findings are collected during the on-site audit activities, which are then documented and reported12
* A document review does not detect any nonconformity of the management system, if documented, but determines the conformity of the documented information. The nonconformity of the management system is detected by the on-site audit activities, which evaluate the performance and effectiveness of the management system12
* A document review does not identify information to support the audit plan, but gathers information to support the on-site audit activities. The audit plan is prepared before the document review, based on the audit scope, objectives, criteria, and program. The document review is part of the audit plan implementation12 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: 68
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: A (LEAVE A REPLY)
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: 69
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 medi a. Both documents and media are shredded in military grade devices which make it impossible to reconstruct the original.

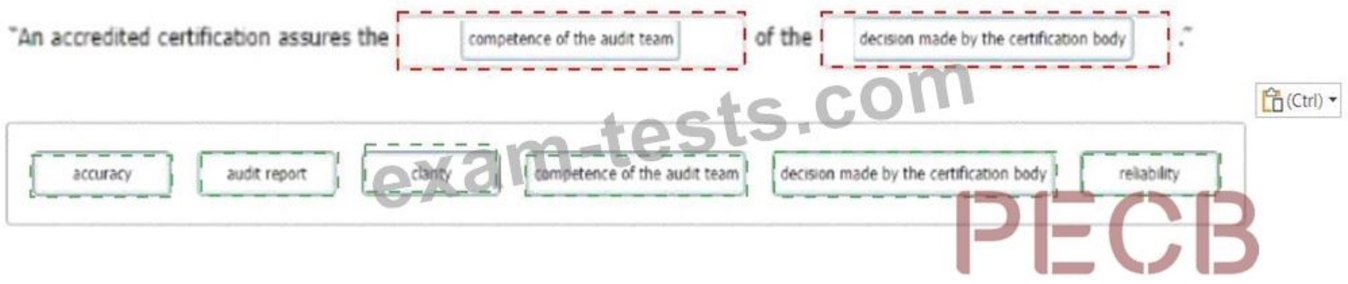
The audit has gone well and you are just about to start to write the audit report, 30 minutes before the closing meeting. At this point one of the organization's employees knocks on your door and asks if they can speak to you. They tell you that when things get busy her manager tells her to use a lower 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.
Reference:
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: 70
Select the option which best describes how Information Security Management System audits should be conducted:
A. Audit criteria should be used to assess circumstantial evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team at the audit team meeting.
B. Audit criteria should be used to assess objective evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team leader at the closing meeting.
C. Audit methods should be used to assess audit evidence in order to generate audit recommendations. Then, the audit recommendations should be created and presented to the auditee at the closing meeting.

D. Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
E. Audit objectives should be used to assess audit evidence in order to generate audit conclusions. Then, the audit findings should be created and presented to the audit client at the closing meeting.
F. Audit objectives should be used to assess objective evidence in order to generate audit conclusions. Then, the audit recommendations should be created and presented to top management at management review.
Answer: D (LEAVE A REPLY)
The option that best describes how Information Security Management System (ISMS) audits should be conducted, aligning with best practices and standards like ISO/IEC 27001:2022, is:
D . Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
This option accurately reflects the audit process, emphasizing the use of systematic audit methods to assess objective evidence, which is crucial for impartiality and accuracy in auditing. Audit findings are the results derived from evaluating the objective evidence against the audit criteri a. The conclusion, based on the audit findings, provides a comprehensive summary of the audit's outcomes, indicating whether the audited ISMS meets the established criteria. Presenting these conclusions to the auditee during the closing meeting ensures transparency and provides an opportunity for immediate clarification and discussion of the results and potential next steps.

NEW QUESTION: 71
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: 72

Question
A retail company experienced a malware infection that bypassed its existing security measures. To minimize damage, remove the malware, and restore affected systems to normal operation, what type of controls should the company implement?
A. Corrective
B. Detective
C. Preventive
Answer: (SHOW ANSWER)
The correct answer is Corrective controls, because the organization is responding to an incident that has already occurred and is taking actions to remove the malware and restore normal operations. Corrective controls are designed to limit damage, eradicate the cause of an incident, and return systems to an acceptable operational state after a security event has been detected.
In this scenario, the malware infection has already bypassed existing security measures, meaning preventive controls failed to stop the incident. The focus now is not on detection, as the infection is already known, but on remediation and recovery. Activities such as malware removal, system restoration from backups, reinstallation of compromised systems, and application of patches are classic examples of corrective controls.
ISO/IEC 27001:2022 addresses this through clause 10.2 on nonconformity and corrective action, which requires organizations to take action to control and correct incidents and deal with their consequences.
Additionally, ISO/IEC 27002:2022 includes controls related to incident response and recovery that support corrective actions after an event.
Option B is incorrect because detective controls, such as monitoring and logging, are intended to identify incidents, not resolve them. Option C is incorrect because preventive controls aim to stop incidents from occurring in the first place, such as antivirus software or access controls. Since the malware has already caused harm, corrective controls are the most appropriate response.

NEW QUESTION: 73
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: D,E (LEAVE A REPLY)
Explanation
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

NEW QUESTION: 74
Question:
An organization is evaluating the materiality of different processes within its ISMS. It is assessing the direct expenses involved with personnel, third-party services, and general fees. Which factor of materiality is the company primarily considering?
A. Cost of operations
B. Cost of the process
C. Potential cost of errors or nonconformities
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The organization is focusing on direct costs associated with running specific processes.
* "Personnel, third-party services, and general fees" refer to operational costs of specific processes, not overall business operations.
* A. Incorrect:
* Cost of operations refers to the total business expenses, not individual processes.
* C. Incorrect:
* Potential cost of errors relates to risk assessment and impact analysis, not direct expenses.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.3.2 (Audit Planning and Materiality Considerations)

NEW QUESTION: 75
Which measure is a preventive measure?
A. Installing a logging system that enables changes in a system to be recognized
B. Shutting down all internet traffic after a hacker has gained access to the company systems
C. Putting sensitive information in a safe
Answer: C (LEAVE A REPLY)
A preventive measure is a measure that aims to avoid or reduce the likelihood or impact of an unwanted incident. Putting sensitive information in a safe is an example of such a measure, as it protects the information from unauthorized access, theft, damage or loss. Installing a logging system, shutting down internet traffic or restoring data from backups are not preventive measures, but rather detective, corrective or recovery measures. They do not prevent incidents from happening, but rather help to identify, stop or recover from them. ISO/IEC 27001:2022 defines preventive action as "action to eliminate the cause of a potential nonconformity or other undesirable potential situation" (see clause 3.38). Reference: [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 Preventive Measure?

NEW QUESTION: 76
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?
A. Verification should focus on whether any action undertaken taken has been undertaken efficiently
B. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
C. Verification should focus on whether any action undertaken is complete
D. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
E. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
F. Verification should focus on whether any action undertaken has been undertaken effectively
Answer: (SHOW ANSWER)
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence.
The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12 Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12 Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 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: 77
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:
UpNet ensured independence, objectivity, and advisory activities from the internal audit. Is this action acceptable?
A. Yes, because internal audits have an advisory role
B. No, because internal audits should be independent of the audited activities
C. No, because the internal audit function was outsourced
Answer: (SHOW ANSWER)
Yes, this action is acceptable. The internal audits being outsourced ensure independence and objectivity and allow the audit function to serve its advisory role effectively, in line with ISO/IEC 27001 requirements. The independence enhances the credibility and reliability of the audit results.

NEW QUESTION: 78
Select the option which best describes how Information Security Management System audits should be conducted:
A. Audit criteria should be used to assess circumstantial evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team at the audit team meeting.
B. Audit criteria should be used to assess objective evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team leader at the closing meeting.
C. Audit methods should be used to assess audit evidence in order to generate audit recommendations. Then, the audit recommendations should be created and presented to the auditee at the closing meeting.
D. Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
E. Audit objectives should be used to assess audit evidence in order to generate audit conclusions. Then, the audit findings should be created and presented to the audit client at the closing meeting.
F. Audit objectives should be used to assess objective evidence in order to generate audit conclusions. Then, the audit recommendations should be created and presented to top management at management review.
Answer: (SHOW ANSWER)
The option that best describes how Information Security Management System (ISMS) audits should be conducted, aligning with best practices and standards like ISO/IEC 27001:2022, is:
D). Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
This option accurately reflects the audit process, emphasizing the use of systematic audit methods to assess objective evidence, which is crucial for impartiality and accuracy in auditing. Audit findings are the results derived from evaluating the objective evidence against the audit criteria. The conclusion, based on the audit findings, provides a comprehensive summary of the audit's outcomes, indicating whether the audited ISMS meets the established criteria. Presenting these conclusions to the auditee during the closing meeting ensures transparency and provides an opportunity for immediate clarification and discussion of the results and potential next steps.

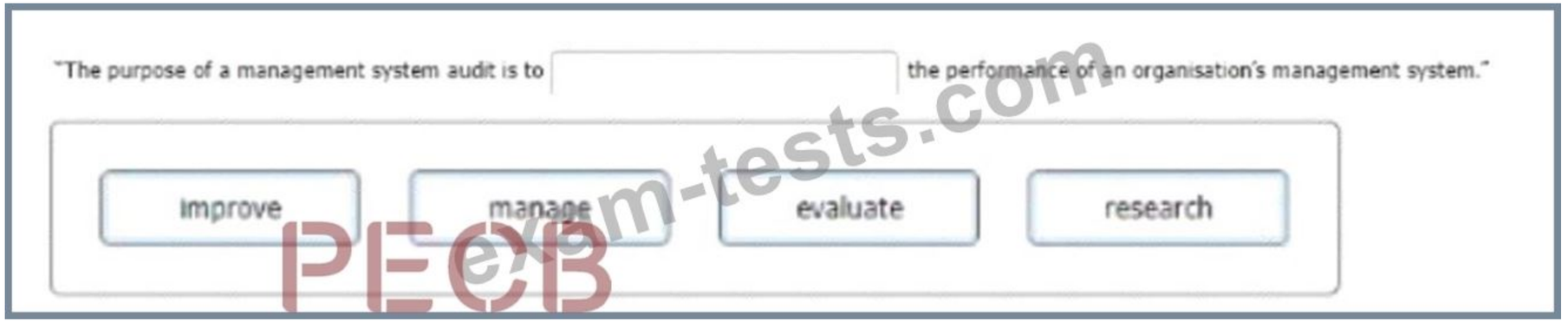
NEW QUESTION: 79
Stages of Information
A. creation, evolution, maintenance, use, disposition
B. creation, use, disposition, maintenance, evolution
C. creation, distribution, use, maintenance, disposition
D. creation, distribution, maintenance, disposition, use
Answer: (SHOW ANSWER)

The stages of information are creation, distribution, use, maintenance, and disposition. These are the phases that information goes through during its lifecycle, from the moment it is generated to the moment it is destroyed or archived. Each stage of information has different security requirements and risks, and should be managed accordingly. Creation, evolution, maintenance, use, and disposition are not the correct stages of information, as evolution is not a distinct stage, but a process that can occur in any stage. Creation, use, disposition, maintenance, and evolution are not the correct stages of information, as they are not in the right order. Creation, distribution, maintenance, disposition, and use are not the correct stages of information, as they are not in the right order. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 32. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 12.

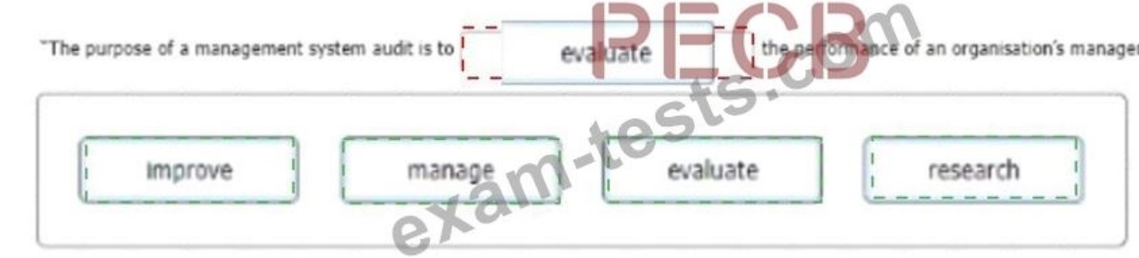
NEW QUESTION: 80
Which two of the following actions are the individual(s) managing the audit programme responsible for?
A. Determining the resources necessary for the audit programme
B. Communicating with the auditee during the audit
C. Determining the legal requirements applicable to each audit
D. Keping informed the accreditation body on the progress of the audit programme
E. Defining the objectives, scope and criteria for an individual audit
F. Defining the plan of an individual audit
Answer: A,D (LEAVE A REPLY)
Explanation
Establishing the audit programme objectives, scope and criteria
Determining the resources necessary for the audit programme, such as the audit team members, the budget, the time, the tools, etc.
Selecting and appointing the audit team leaders and auditors
Reviewing and approving the audit plans and arrangements
Ensuring the effective communication and coordination among the audit programme stakeholders, such as the auditors, the auditees, the certification bodies, the accreditation bodies, etc.
Keeping informed the accreditation body on the progress of the audit programme, especially in case of any significant changes, issues, or nonconformities Monitoring and reviewing the performance and results of the audit programme and the audit teams Evaluating the feedback and satisfaction of the auditees and other interested parties Identifying and implementing the opportunities for improvement of the audit programme The individual(s) managing the audit programme are not responsible for the following tasks, which are delegated to the audit team leaders or the auditors12:
Communicating with the auditee during the audit, such as conducting the opening and closing meetings, resolving any audit-related problems, reporting any audit findings, etc.
Determining the legal requirements applicable to each audit, such as the confidentiality, the impartiality, the consent, the liability, etc.
Defining the objectives, scope and criteria for an individual audit, which are derived from the audit programme and agreed with the auditee Defining the plan of an individual audit, which includes the audit schedule, the audit activities, the audit methods, the audit documents, etc.
References:
ISO 19011:2018 - Guidelines for auditing management systems
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-20

NEW QUESTION: 81
After a fire has occurred, what repressive measure can be taken?
A. Extinguishing the fire after the fire alarm sounds
B. Buying in a proper fire insurance policy
C. Repairing all systems after the fire
Answer: A (LEAVE A REPLY)
A repressive security measure is a measure that aims to stop or limit an ongoing incident from causing further harm, or to restore normal operations as soon as possible. A repressive security measure can be a policy, a procedure, a device, a technique or an action that responds to an incident and mitigates its consequences. Extinguishing the fire after the fire alarm sounds is an example of a repressive security measure, because it stops the fire from spreading and damaging more assets or endangering more people. ISO/IEC 27001:2022 defines repressive control as "control that modifies risk by reducing the consequences of an unwanted incident" (see clause 3.38). Reference: [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 Repressive Security?]

NEW QUESTION: 82
Select a word from the following options that best completes 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:

The purpose of a management system audit is to evaluate the performance of an organization's management system.
A management system audit is an independent and systematic analysis and evaluation of a company's overall activities and performances1. It is a valuable tool used to determine the efficiency, functions, accomplishments and achievements of the company1. A management system audit can be conducted against a range of audit criteria, including (but not limited to) requirements set of in existing ISO standards2.
According to ISO 19011:2018, which provides guidelines for auditing management systems, the purpose of an audit is to enable the auditor to provide an audit conclusion that is related to the audit objectives2. 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 system2.
Therefore, the correct answer is evaluate, as it best describes the purpose of a management system audit. The other options are not correct because they are not specific enough or do not reflect the intended outcome of an audit. For example, improve implies that the audit itself will enhance the performance of the management system, which is not necessarily true. Manage implies that the audit will control or direct the management system, which is not its role. Research implies that the audit will generate new knowledge or information about the management system, which is not its primary aim.

NEW QUESTION: 83

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?
A. 5.11 Return of assets
B. 5.13 Labelling of information
C. 5.3 Segregation of duties
D. 5.32 Intellectual property rights
E. 5.34 Privacy and protection of personal identifiable information (PII)
F. 5.6 Contact with special interest groups
G. 6.3 Information security awareness, education, and training
H. 6.4 Disciplinary process
Answer: B,E,G (LEAVE A REPLY)
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: 84
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 of ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organisation outsourced the mobile app development to a professional software development organisation with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified.
The IT Manager presents the software security management procedure and summarises 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 - Reference ID: 0098, details as follows:

Target of Test: ABC's healthcare mobile app, version 1	**Test results**	**Test summary**
Performance test		
Response time	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the response time.
Useability and user interface	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the user interface, size of the text, and colour.
Security test		
Access control (username and password)	PASS	Compliance with the organisation's information security policy, unique username and minimal 12 digits password (with Capital/Lower case, numbers, symbols combination)
Access control – One-time-password (OTP)	PASS	The mobile app generates an 8-digit OTP and sends it to an authorised user's mobile phone via SMS, as a second factor of identity authentication.
Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymization	Fail	Not able to perform the pseudonymization.
Final approval:		
signed by: *Service Manager*		

You would like to investigate other areas further to collect more audit evidence. Select three options that will not be in your audit trail.
A. Collect more evidence on how much residents' family members pay to install ABC's healthcare mobile app. (Relevant to clause 4.2)
B. Collect more evidence by downloading and testing the mobile app on your phone. (Relevant to control A.8.1)
C. Collect more evidence to determine the number of users of ABC's healthcare mobile app. (relevant to clause 4.2)
D. Collect more evidence on how the organisation performs testing of personal data handling. (Relevant to control A.5.34)

E. Collect more evidence on the organisation's business continuity policy. (Relevant to control A.5.30)
F. Collect more evidence on how the organisation manages information security in the selection of an external service provider. (Relevant to control A.5.19)
G. Collect more evidence on how the developer trains its product support personnel. (Relevant to clause 7.2)
H. Collect more evidence to verify the developer's CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO22301) and ISMS (ISO/IEC 27001) certification. (Relevant to control A.5.21)
Answer: (SHOW ANSWER)
The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13. References: 1: ISO
/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 85

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

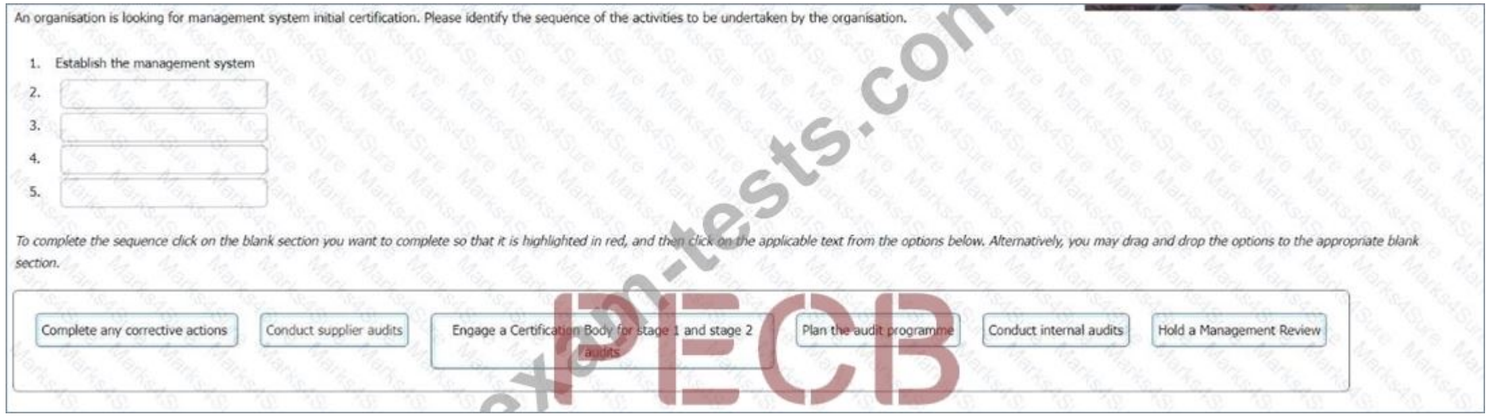
Explanation:
An audit finding is the result of the evaluation of the collected audit evidence against audit criteria.

NEW QUESTION: 86
You are an experienced ISMS audit team leader who is currently conducting a third party initial certification audit of a new client, using ISO/IEC 27001:2022 as your criteria.
It is the afternoon of the second day of a 2-day audit, and you are just about to start writing your audit report.
So far no nonconformities have been identified and you and your team have been impressed with both the site and the organisation's ISMS.
At this point, a member of your team approaches you and tells you that she has been unable to complete her assessment of leadership and commitment as she has spent too long reviewing the planning of changes.
Which one of the following actions will you take in response to this information?
A. Apologise to the client and tell them you will return at a later date to review leadership and commitment.
B. Suggest to the client that if they are prepared to upgrade your return flight to first class you will audit leadership and commitment in your own time tomorrow.
C. Advise the auditee and audit client that it is not possible to make a positive recommendation at this point.
D. Advise the auditee that the certification audit will need to be terminated and rescheduled.
E. Contact the individual managing the audit programme and seek their permission to record a positive recommendation in the audit report.
F. Contact your head office and await their further instructions of how to proceed.
G. Given there have been no nonconformities identified and the overall impression of the organisation has been a good one, record a positive recommendation for certification in the audit report.
H. Review the audit plan and client availabilities to determine whether there is any opportunity for another member of your team to pick up this task before the closing meeting.
Answer: C (LEAVE A REPLY)
Explanation
Leadership and commitment is a key requirement of ISO/IEC 27001:2022, as it establishes the top management's role and responsibility in establishing, implementing, maintaining, and continually improving the ISMS. Without assessing this aspect, the audit team cannot conclude that the ISMS is effective and conforms to the standard. Therefore, the audit team leader should advise the auditee and audit client that it is not possible to make a positive recommendation at this point, and explain the reason and the implications. The audit team leader should also consult with the certification body and the audit programme manager on the next steps, such as extending the audit duration, conducting a follow-up audit, or issuing a conditional certification, depending on the certification body's policy and the audit client's agreement. References: =
* ISO/IEC 27001:2022, clause 5, Leadership
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 22, Audit Report
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 23, Audit Conclusion and Recommendation

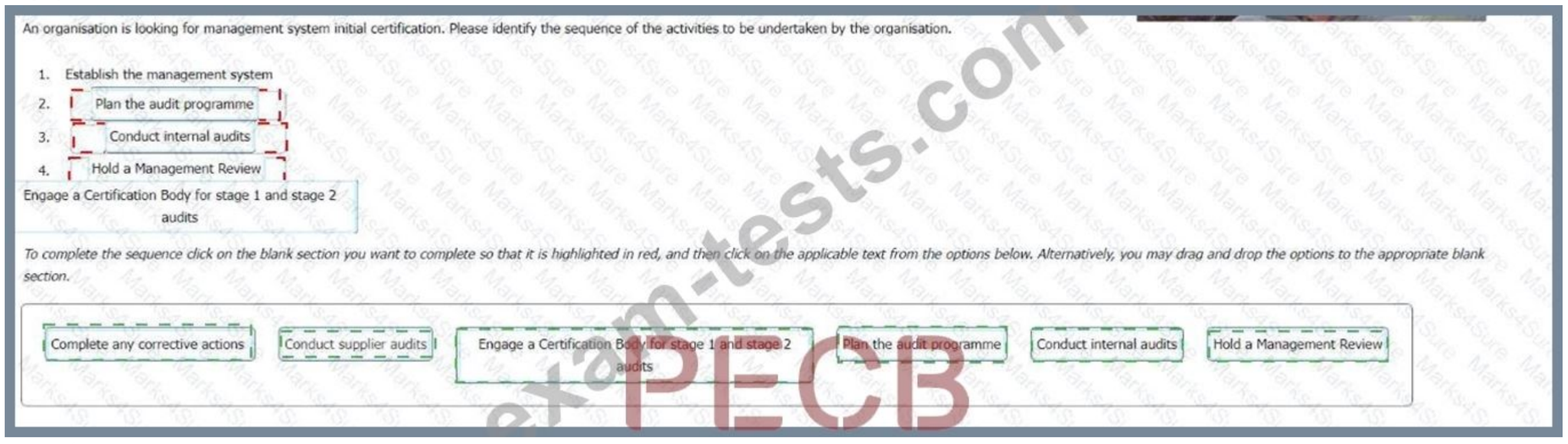
NEW QUESTION: 87

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.



Answer:



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

NEW QUESTION: 88
In acceptable use of Information Assets, which is the best practice?
A. Playing any computer games during office hours
B. Accessing phone or network transmissions, including wireless or wifi transmissions
C. Interfering with or denying service to any user other than the employee's host
D. Access to information and communication systems are provided for business purpose only
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
Which of the following is a possible event that can have a disruptive effect on the reliability of information?
A. Threat
B. Risk
C. Vulnerability
D. Dependency
Answer: A (LEAVE A REPLY)
A possible event that can have a disruptive effect on the reliability of information is a threat. A threat is anything that has the potential to harm an asset or its protection, such as a natural disaster, a human error, a malicious attack, etc. A threat can exploit a vulnerability or weakness in an asset or its protection and cause an adverse impact on the confidentiality, integrity or availability of information. ISO/IEC 27001:2022 defines threat as "potential cause of an unwanted incident, which can result in harm to a system or organization" (see clause 3.48). Reference: [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 Threat?

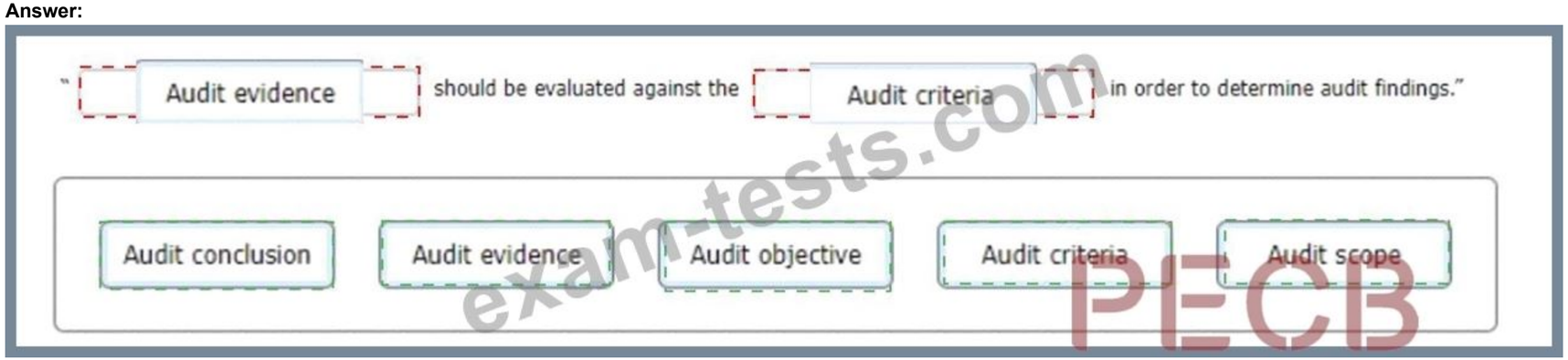
NEW QUESTION: 90
You are performing an ISMS audit at a residential nursing home that provides healthcare services.
The next step in your audit plan is to verify the information security incident management process.
The IT Security Manager presents the information security incident management procedure (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: E,G,H (LEAVE A REPLY)
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

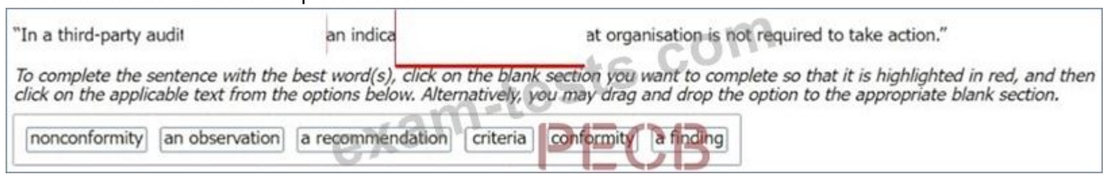
NEW QUESTION: 91
In regard to generating an audit finding, select the words that best complete the following sentence.
To complete the sentence with the best word(s), click on the blank section you want to complete so that it Is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

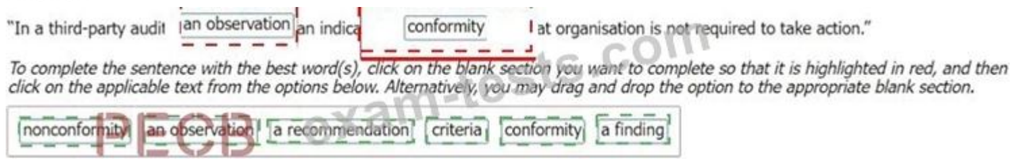


Explanation
Audit evidence should be evaluated against the audit criteria in order to determine audit findings.
* Audit evidence is the information obtained by the auditors during the audit process that is used as a basis for forming an audit opinion or conclusion12. Audit evidence could include records, 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: 92
Select the words that best complete the sentence:



Answer:



Explanation
"In a third-party audit an observation can indicate conformity at organisation is not required to take action." According to the PECB Candidate Handbook1, an observation is "a statement of fact made during an audit and substantiated by objective evidence". An observation can indicate conformity or nonconformity, but it does not require any corrective action from the audited organisation. A recommendation, on the other hand, is "a suggestion for improvement based on an observation". A recommendation may or may not be accepted by the audited organisation.
According to the Fundamentals - Third parties2, a third-party audit is "an audit conducted by an external organisation that has the legal right to audit an organisation's processes and procedures". A third-party audit can result in a finding, which is "a conclusion reached by the auditor based on the audit evidence collected". A finding can be positive or negative, depending on whether the audited organisation meets the audit criteria or not. A nonconformity is "a finding that indicates the non-fulfilment of a requirement". A nonconformity requires corrective action from the audited organisation to prevent recurrence.

NEW QUESTION: 93

Who are allowed to access highly confidential files?
A. Employees with a business need-to-know
B. Contractors with a business need-to-know
C. Employees with signed NDA have a business need-to-know
D. Non-employees designated with approved access and have signed NDA
Answer: A (LEAVE A REPLY)
Explanation
According to ISO/IEC 27001:2022, clause 8.2.1, the organization shall ensure that access to information and information processing facilities is limited to authorized users based on the access control policy and in accordance with the business requirements of access control2. Therefore, only employees with a business need-to-know are allowed to access highly confidential files, and not contractors, non-employees or employees with signed NDA. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 94
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 of ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organisation outsourced the mobile app development to a professional software development organisation with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified.
The IT Manager presents the software security management procedure and summarises 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 - Reference ID: 0098, details as follows:

Target of Test: ABC's healthcare mobile app, version 1	Test results	Test summary
Performance test		
Response time	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the response time.
Useability and user interface	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the user interface, size of the text, and colour.
Security test		
Access control (username and password)	PASS	Compliance with the organisation's information security policy, unique username and minimal 12 digits password (with Capital/Lower case, numbers, symbols combination)
Access control – One-time-password (OTP)	PASS	The mobile app generates an 8-digit OTP and sends it to an authorised user's mobile phone via SMS, as a second factor of identity authentication.

Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymization	Fail	Not able to perform the pseudonymization.
Final approval:		
by: *Service Manager*		signed

You would like to investigate other areas further to collect more audit evidence. Select three options that will not be in your audit trail.

A. Collect more evidence on how much residents' family members pay to install ABC's healthcare mobile app. (Relevant to clause 4.2)

B. Collect more evidence by downloading and testing the mobile app on your phone. (Relevant to control A.8.1)

C. Collect more evidence to determine the number of users of ABC's healthcare mobile app. (relevant to clause 4.2)

D. Collect more evidence on how the organisation performs testing of personal data handling. (Relevant to control A.5.34)

E. Collect more evidence on the organisation's business continuity policy. (Relevant to control A.5.30)

F. Collect more evidence on how the organisation manages information security in the selection of an external service provider. (Relevant to control A.5.19)

G. Collect more evidence on how the developer trains its product support personnel. (Relevant to clause 7.2)

H. Collect more evidence to verify the developer's CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certification. (Relevant to control A.5.21)

Answer: A,C,H (LEAVE A REPLY)

The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13. References: 1:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 95

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: 96
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: A (LEAVE A REPLY)
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: 97

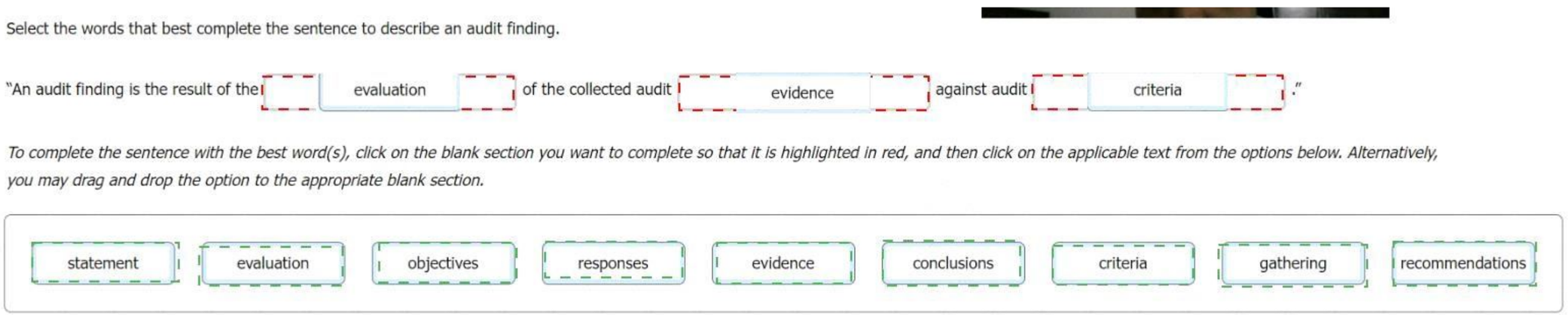
Select the words that best complete the sentence to describe an audit finding.

"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:



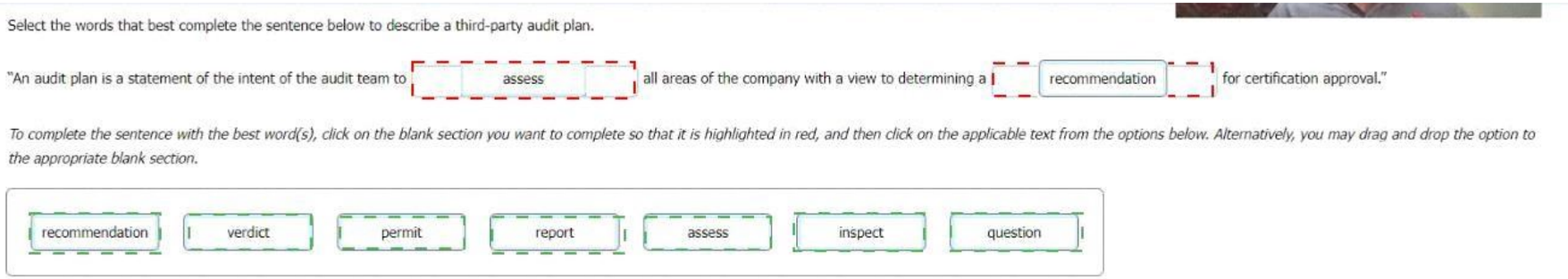
Explanation
An audit finding is the result of the evaluation of the collected audit evidence against audit criteria.

NEW QUESTION: 98
Scenario 4: SendPay is a financial company that provides its services through a network of agents and financial institutions. One of their main services is transferring money worldwide. SendPay, as a new company, seeks to offer top quality services to its clients. Since the company offers international transactions, it requires from their clients to provide personal information, such as their identity, the reason for the transactions, and other details that might be needed to complete the transaction. Therefore, SendPay has implemented security measures to protect their clients' information, including detecting, investigating, and responding to any information security threats that may emerge. Their commitment to offering secure services was also reflected during the ISMS implementation where the company invested a lot of time and resources.
Last year, SendPay unveiled their digital platform that allows money transactions through electronic devices, such as smartphones or laptops, without requiring an additional fee. Through this platform, SendPay's clients can send and receive money from anywhere and at any time. The digital platform helped SendPay to simplify the company's operations and further expand its business. At the time, SendPay was outsourcing its software operations, hence the project was completed by the software development team of the outsourced company.
The same team was also responsible for maintaining the technology infrastructure of SendPay.
Recently, the company applied for ISO/IEC 27001 certification after having an ISMS in place for almost a year. They contracted a certification body that fit their criteria. Soon after, the certification body appointed a team of four auditors to audit SendPay's ISMS.
During the audit, among others, the following situations were observed:
1.The outsourced software company had terminated the contract with SendPay without prior notice. As a result, SendPay was unable to immediately bring the services back in-house and its operations were disrupted for five days. The auditors requested from SendPay's representatives to provide evidence that they have a plan to follow in cases of contract terminations. The representatives did not provide any documentary evidence but during an interview, they told the auditors that the top management of SendPay had identified two other software development companies that could provide services immediately if similar situations happen again.
2.There was no evidence available regarding the monitoring of the activities that were outsourced to the software development company. Once again, the representatives of SendPay told the auditors that they regularly communicate with the software development company and that they are appropriately informed for any possible change that might occur.
3.There was no nonconformity found during the firewall testing. The auditors tested the firewall configuration in order to determine the level of security provided by these services. They used a packet analyzer to test the firewall policies which enabled them to check the packets sent or received in real-time.
Based on this scenario, answer the following question:
Regarding the third situation observed, auditors themselves tested the configuration of firewalls implemented in SendPay's network. How do you describe this situation? Refer to scenario 4.
A. Acceptable, technical evidence is required to validate the operation of technical processes
B. Unacceptable, the auditors should only observe the testing of system or equipment configurations and not test the system themselves
C. Unacceptable, firewall configurations should not be tested during an audit since this can have an impact systems' operation

Answer: A (LEAVE A REPLY)
It is acceptable and often necessary for auditors to test technical controls such as firewalls to validate the operation and effectiveness of these processes during an ISMS audit. This hands-on testing provides concrete, technical evidence of the security measures' performance.
References: ISO/IEC 27001:2013 Standard, Clause A.13 (Communications security), ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 99
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." Explanation: 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: 100
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: B (LEAVE A REPLY)
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: 101
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: B,D (LEAVE A REPLY)
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: 102

You are an experienced ISMS audit team leader providing instruction to an auditor in training. They are unclear in their understanding of risk processes and ask you to provide them with an example of each of the processes detailed below.

Match each of the descriptions provided to one of the following risk management processes.

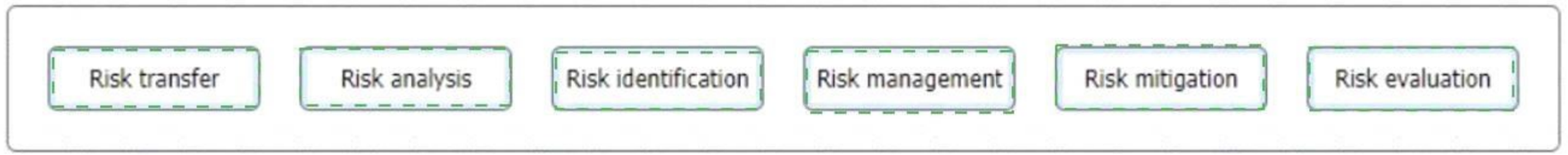
To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

A process by which the nature of the risk is determined along with its probability and impact	
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	
A process by which a risk is recognised and described	
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	

Risk transfer | Risk analysis | Risk identification | Risk management | Risk mitigation | Risk evaluation

Answer:

A process by which the nature of the risk is determined along with its probability and impact	Risk analysis
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	Risk management
A process by which a risk is recognised and described	Risk identification
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	Risk evaluation
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	Risk mitigation
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	Risk transfer



Explanation:

A process by which the nature of the risk is determined along with its probability and impact	Risk analysis
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	Risk management
A process by which a risk is recognised and described	Risk identification
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	Risk evaluation
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	Risk mitigation
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	Risk transfer

* Risk analysis is the process by which the nature of the risk is determined along with its probability and impact. Risk analysis involves estimating the likelihood and consequences of potential events or situations that could affect the organization's information security objectives or requirements12. Risk analysis could use qualitative or quantitative methods, or a combination of both12.
* Risk management is the process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices. Risk management involves establishing the context, identifying, analyzing, evaluating, treating, monitoring, and reviewing the risks that could affect the organization's information security performance or compliance12. Risk management aims to ensure that risks are identified and treated in a timely and effective manner, and that opportunities for improvement are exploited12.
* Risk identification is the process by which a risk is recognised and described. Risk identification involves identifying and documenting the sources, causes, events, scenarios, and potential impacts of risks that could affect the organization's information security objectives or requirements12. Risk identification could use various techniques, such as brainstorming, interviews, checklists, surveys, or historical data12.
* Risk evaluation is the process by which the impact and/or probability of a risk is compared against risk criteria to determine if it is tolerable. Risk evaluation involves comparing the results of risk analysis with predefined criteria that reflect the organization's risk appetite, tolerance, or acceptance12. Risk evaluation could use various methods, such as ranking, scoring, or matrix12. Risk evaluation helps to prioritize and decide on the appropriate risk treatment options12.
* Risk mitigation is the process by which the impact and/or probability of a risk is reduced by means of the application of controls. Risk mitigation involves selecting and implementing measures that are designed to prevent, reduce, transfer, or accept risks that could affect the organization's information security objectives or requirements12. Risk mitigation could include various types of controls, such as technical, organizational, legal, or physical12. Risk mitigation should be based on a cost-benefit analysis and a residual risk assessment12.
* Risk transfer is the process by which a risk is passed to a third party, for example through obtaining appropriate insurance. Risk transfer involves sharing or shifting some or all of the responsibility or liability for a risk to another party that has more capacity or capability to manage it12. Risk transfer could include various methods, such as contracts, agreements, partnerships, outsourcing, or insurance12. Risk transfer should not be used as a substitute for effective risk management within the organization12.

References :=

* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management

NEW QUESTION: 103

Who is responsible for Initial asset allocation to the user/custodian of the assets?

A. Asset Manager
B. Asset Owner
C. Asset Practitioner
D. Asset Stakeholder

Answer: (SHOW ANSWER)
Explanation
The asset owner is responsible for initial asset allocation to the user or custodian of the assets. The asset owner is a person or entity that has been assigned the responsibility for managing and protecting the asset throughout its lifecycle. The asset owner should ensure that the user or custodian of the assets has the appropriate authorization, competence and awareness to use or handle the assets securely. The asset owner should also monitor and review the use or custody of the assets and update or revoke the allocation as needed. ISO/IEC
27001:2022 requires the organization to assign owners to all assets within the scope of the information security management system (see clause A.8.1.2). 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 an Asset Owner?

NEW QUESTION: 104
Which one of the following options is the definition of an interested party?
* A third party can appeal to an organisation when it perceives itself to be affected by a decision or activity
A. A person or organisation that can affect, be affected by or perceive itself to be affected by a decision or activity
B. A group or organisation that can interfere in or perceive itself to be interfered with by a management decision
C. An individual or organisation that can control, be controlled by, or perceive itself to be controlled by a decision or activity
Answer: B (LEAVE A REPLY)
This is the definition of an interested party according to ISO 27001:2013, clause 3.16. An interested party is essentially a stakeholder, i.e., a person or organization that can influence or be influenced by the information security management system (ISMS) or its activities. Interested parties can have different needs and expectations regarding the ISMS, and these should be identified and addressed by the organization.
References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.16
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* Identifying interested parties and their expectations for an ISO 27001 ISMS
* Examples of ISO 27001 interested parties