PECB.ISO-IEC-27001-Lead-Auditor.v2024-07-04.q280

Exam Code:	ISO-IEC-27001-Lead-Auditor
Exam Name:	PECB Certified ISO/IEC 27001 Lead Auditor exam
Certification Provider:	PECB
Free Question Number:	280
Version:	v2024-07-04
# of views:	1055
# of Questions views:	2800
https://www.exam-tests.com/ISO-IEC-27001-Lead-Auditor-exam/PECB.ISO-IEC-27001-Lead-Auditor.v2024-07-04.q280.html	

NEW QUESTION: 1
You are an experienced ISMS audit team leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-Do-Check-Act cycle in respect of the operation of the information security management system.
You do this by asking him to select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below.
Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

Explanation:

* Review is the third stage of the Plan-Do-Check-Act (PDCA) cycle, which is a four-step model for implementing and improving an information security management system (ISMS) according to ISO/IEC
27001:202212. Review involves assessing and measuring the performance of the ISMS against the established policies, objectives, and criteria12.
* Assess is the verb that describes the action of reviewing the ISMS. Assess means to evaluate, analyze, or measure something in a systematic and objective manner3. Assessing the ISMS involves collecting and verifying audit evidence, identifying strengths and weaknesses, and determining the degree of conformity or nonconformity12.
* Regular is the adjective that describes the frequency or interval of reviewing the ISMS. Regular means occurring or done at fixed or uniform intervals4. Reviewing the ISMS at regular intervals means conducting internal audits and management reviews periodically, such as annually, quarterly, or monthly, depending on the needs and risks of the organization12.
* Suitability is one of the attributes that describes the quality or outcome of reviewing the ISMS. Suitability means being appropriate or fitting for a particular purpose, person, or situation5. Reviewing the ISMS for suitability means ensuring that it is aligned with the organization's strategic direction, business objectives, and information security requirements12.
References :=
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* Assess | Definition of Assess by Merriam-Webster
* Regular | Definition of Regular by Merriam-Webster
* Suitability | Definition of Suitability by Merriam-Webster

NEW QUESTION: 2
A member of staff denies sending a particular message.
Which reliability aspect of information is in danger here?
A. availability
B. correctness
C. integrity
D. confidentiality
Answer: C (LEAVE A REPLY)
The reliability aspect of information that is in danger when a member of staff denies sending a particular message is integrity. Integrity implies that information is authentic and can be verified as such. If a member of staff denies sending a message, it means that either the message was forged or the sender is lying, both of which violate the integrity of the information. Availability, correctness and confidentiality are not directly affected by this scenario. ISO/IEC 27001:2022 defines integrity as "property of accuracy and completeness" (see clause 3.24). 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 Integrity?

NEW QUESTION: 3
You are conducting an ISMS audit. The next step in your audit plan is to verify that the organisation's information security risk treatment plan has been established and implemented properly. You decide to interview the IT security manager.
You: Can you please explain how the organisation performs its information security risk assessment and treatment process?
IT Security Manager: We follow the information security risk management procedure which generates a risk treatment plan.
Narrator: You review risk treatment plan No. 123 relating to the planned installation of an electronic (invisible) fence to improve the physical security of the nursing home. You found the risk treatment plan was approved by IT Security Manager.
You: Who is responsible for physical security risks?
IT Security Manager: The Facility Manager is responsible for the physical security risk. The IT department helps them to monitor the alarm. The Facility Manager is authorized to approve the budget for risk treatment plan No. 123.
You: What residual information security risks exist after risk treatment plan No. 123 was implemented?
IT Security Manager: There is no information for the acceptance of residual information security risks as far as I know.
You prepare your audit findings. Select three options for findings that are justified in the scenario.
A. Nonconformity (NC) - The information for the acceptance of residual information security risks should be updated after the risk treatment is implemented. Clause 6.1.3.f
B. There is an opportunity for improvement (OI) to conduct security checks on the perimetre fence
C. There is an opportunity for improvement (OI) once the Electronic (invisible) fence is installed. Residents' physical security is improved
D. Nonconformity (NC) - Top management must ensure that the resources needed for the ISMS are available. Clause 5.1.c
E. Nonconformity (NC) - The IT security manager should be aware of and understand his authority and area of responsibility. Clause 7.3
F. Nonconformity (NC) - The organization should provide the resources needed for the continual improvement of the ISMS. Clause 7.1
G. Nonconformity (NC) - The risk treatment plan No. 123 should be approved by the risk owner, the Facility Manager in this case. Clause 6.1.3.f
H. It is good practice to adopt state-of-the-art technology as part of the continual improvement process
Answer: A,E,G (LEAVE A REPLY)
Explanation

The three options for findings that are justified in the scenario are:
*Nonconformity (NC) - The information for the acceptance of residual information security risks should be updated after the risk treatment is implemented. Clause 6.1.3.f
*Nonconformity (NC) - The IT security manager should be aware of and understand his authority and area of responsibility. Clause 7.3
*Nonconformity (NC) - The risk treatment plan No. 123 should be approved by the risk owner, the Facility Manager in this case. Clause 6.1.3.f According to ISO/IEC 27001:2022, clause 6.1.3.f, the organisation must retain documented information that includes the information for the acceptance of residual information security risks, and the approval of the risk treatment plan by the risk owner1. Therefore, option A and G are justified as nonconformities, because the organisation failed to update the information for the acceptance of residual risks, and the risk treatment plan was approved by the IT security manager, who is not the risk owner.
According to ISO/IEC 27001:2022, clause 7.3, the organisation must ensure that the persons assigned to perform the roles and responsibilities for the ISMS are competent, and are aware of the consequences of not conforming to the ISMS requirements2. Therefore, option E is justified as a nonconformity, because the IT security manager, who is responsible for the information security risk management process, was not aware of his authority and area of responsibility.
The other options are not justified as findings, because they are either irrelevant or incorrect. For example:
*Option B is irrelevant, because it is not related to the information security risk treatment plan No. 123, which is the focus of the audit.
*Option C is incorrect, because it is not an opportunity for improvement, but rather a benefit of the risk treatment plan No. 123, which is already implemented.
*Option D is incorrect, because it is not a nonconformity, but rather a requirement for the organisation to provide the resources needed for the ISMS, which is not the same as the resources needed for the risk treatment plan No. 123.
*Option F is incorrect, because it is not a nonconformity, but rather a requirement for the organisation to provide the resources needed for the continual improvement of the ISMS, which is not the same as the resources needed for the risk treatment plan No. 123.
*Option H is irrelevant, because it is not a finding, but rather a good practice, which is not the objective of the audit.
References: 1: ISO/IEC 27001:2022, 6.1.3.f; 2: ISO/IEC 27001:2022, 7.3; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

NEW QUESTION: 4
Changes to the information processing facilities shall be done in controlled manner.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation

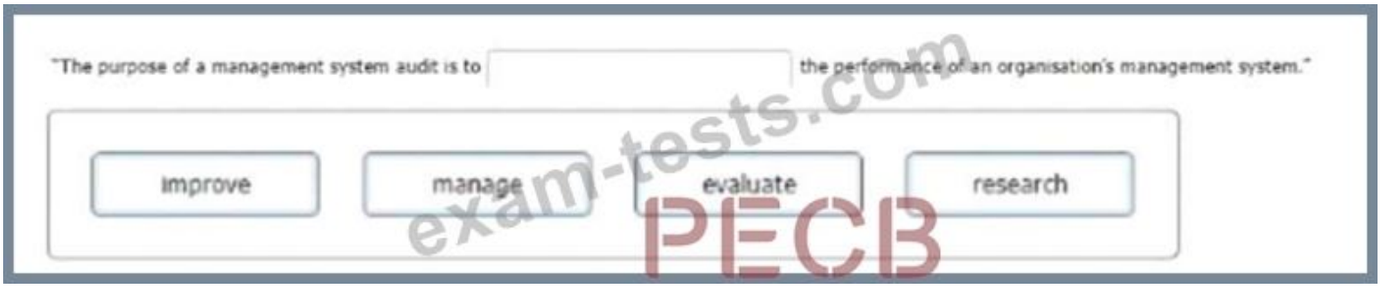
Changes to the information processing facilities shall be done in a controlled manner, according to clause
12.1.2 of ISO/IEC 27001:2022. This is to ensure that the security of information and systems is not compromised by the changes, and that the changes are authorized, documented, tested, and approved before implementation. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 63. :
ISO/IEC 27001:2022, clause 12.1.2.

NEW QUESTION: 5
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.

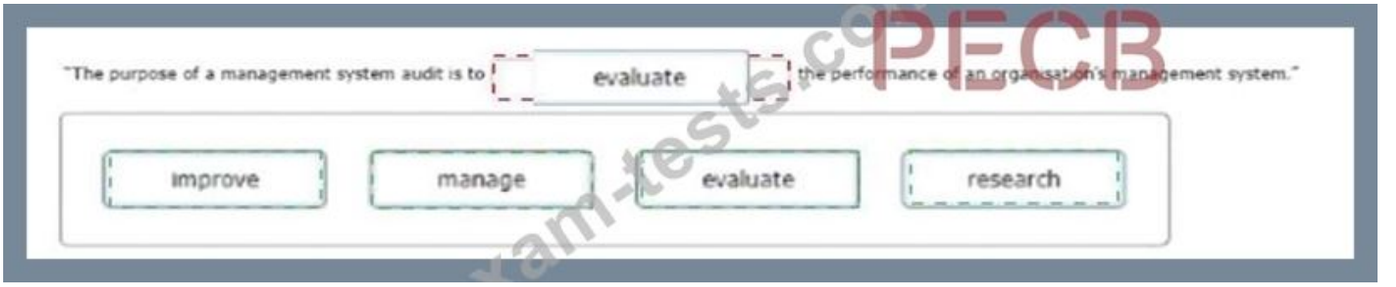
NEW QUESTION: 6
You are an experienced ISMS audit team leader providing guidance to an auditor in training. She asks you why it is important to have specific criteria relating to the grading of nonconformities. Which one of the following responses is correct?
A. Because grading criteria provide a common basis for the evaluation of nonconformities across the organization
B. Because ISO/IEC 27001:2022 requires it
C. Because the establishment and implementation of grading criteria demonstrate a high level of commitment to the corrective action process
D. Because grading criteria will ensure that all auditors score nonconformities in exactly the same way
Answer: A (LEAVE A REPLY)
Explanation
The correct response is A, because grading criteria provide a common basis for the evaluation of nonconformities across the organization. Grading criteria are the rules or standards that define the severity or impact of nonconformities, and help to determine the appropriate corrective actions and follow-up activities.

Grading criteria are important for several reasons, such as:
* They ensure consistency and objectivity in the assessment and reporting of nonconformities, and avoid subjective or arbitrary judgments.
* They facilitate the communication and understanding of nonconformities among the auditors, the auditees, and the audit clients, and enable the comparison and benchmarking of nonconformities across different processes, functions, or locations.
* They support the prioritization and allocation of resources for the resolution of nonconformities, and the monitoring and measurement of the effectiveness of the corrective actions.
* They demonstrate the commitment and accountability of the organization to the continual improvement of the ISMS, and the compliance with the ISMS requirements and expectations.
References:
* ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1
* PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2
* ISO 27001:2022 Lead Auditor - PECB3
* ISO 27001:2022 certified ISMS lead auditor - Jisc4
* ISO/IEC 27001:2022 Lead Auditor Transition Training Course5
* ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy
* ISO 19011:2022, Guidelines for auditing management systems

NEW QUESTION: 7
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: 8
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 that the Statement of Applicability (SoA) contains the necessary controls.
You review the latest SoA (version 5) document, sampling the access control to the source code (A.8.4), and want to know how the organisation secures ABC's healthcare mobile app source code received from an outsourced software developer.
The IT Security Manager explains the received source code will be checked into the SCM system to make sure of its integrity and security. Only authorised users will be able to check out the software to update it. Both check-in and check-out activities will be logged by the system automatically. The version control is managed by the system automatically.
You found a total of 10 user accounts on the SCM. All of them are from the IT department. You further check with the Human Resource manager and confirm that one of the users, Scott, resigned 9 months ago. The SCM System Administrator confirmed Scott's last check-out of the source code was found 1 month ago. He was using one of the authorised desktops from the local network in a secure area.

You check the user de-registration procedure which states "Managers have to make sure of deregistration of the user account and authorisation immediately from the relevant ICT system and/or equipment after resignation approval." There was no deregistration record for user Scott. The IT Security Manager explains that Scott is a very good software engineer, an ex-colleague, and a friend.
He still comes back to the office every month after he resigned to provide support on source code maintenance. That's why his account on SCM still exists. "We know Scott well and he passed all our background checks when he joined us. As such we didn't feel it necessary to agree any further information security requirements with him just because he is now an external provider".
You prepare the audit findings. Select the three correct options.
A. There is a nonconformity (NC). Scott should have been advised of applicable information security requirements relevant to his new relationship (external provider) with the nursing home. The IT security manager has however confirmed that this did not take place. This does not conform with control A.5.20.
B. There is a nonconformity (NC). The organisation's access control arrangements are not operating effectively as an individual who is no longer employed by the organisation is being permitted to access the nursing home's ICT systems. This does not conform with control A.5.15.
C. There is a nonconformity (NC). The IT Security manager did not make sure the user account for Scott was removed from the SCM and did not complete the user deregistration process after the resignation.
This does not conform with clause 9.1 and control A.5.15.
D. There is a nonconformity (NC). The operating procedures are not well documented. This prevented the SCM System Administrator from being able to remove a user account immediately. This does not conform with clause 9.1 and control A.5.37.
E. There is a nonconformity (NC). The organisation does not have a documented procedure setting out the use of systematic tools to provide access and version control of the source code. This does not conform with clause 9.1 and control A.8.4.
F. There is a nonconformity (NC). The organisation has failed to identify the security risks associated with leaving Scott's account open when he was only re-engaged for a short period monthly. This does not conform with clause 8.2.
G. There is a nonconformity (NC). The SCM is open-source system software. It is not secured and cannot be used for access and version control of the source code. This does not conform with clause 9.1 and control A.8.4.
H. There is a nonconformity (NC). The SCM will log the source code check-in/-out activities automatically. If something goes wrong, the team might not be able to trace it. This does not conform with clause 9.1 and control A.8.4.
Answer: B,C,F (LEAVE A REPLY)
Explanation
The correct options are:
* There is a nonconformity (NC). The organisation's access control arrangements are not operating effectively as an individual who is no longer employed by the organisation is being

permitted to access the nursing home's ICT systems. This does not conform with control A.5.15. (B): This option is correct because control A.5.15 requires the organization to implement secure log-on procedures and manage user access rights. The organization should ensure that only authorized users can access the ICT systems and that the access rights are revoked or modified when the user status changes. The fact that Scott, who resigned 9 months ago, still has an active account on the SCM and can check out the source code, indicates a failure of the access control arrangements and a nonconformity with the control A.5.15.
* There is a nonconformity (NC). The IT Security manager did not make sure the user account for Scott was removed from the SCM and did not complete the user deregistration process after the resignation. This does not conform with clause 9.1 and control A.5.15. : This option is correct because clause 9.1 requires the organization to monitor, measure, analyze, and evaluate the performance and effectiveness of the ISMS. The organization should have processes and indicators to verify that the ISMS requirements and objectives are met and that the ISMS is continually improved. The organization should also ensure that the results of the monitoring and measurement are documented and communicated. The fact that the IT Security manager did not follow the user de-registration procedure and did not document or communicate the exception for Scott, indicates a failure of the monitoring and measurement processes and a nonconformity with clause 9.1 and control A.5.15.
* There is a nonconformity (NC). The organisation has failed to identify the security risks associated with leaving Scott's account open when he was only re-engaged for a short period monthly. This does not conform with clause 8.2. (F): This option is correct because clause 8.2 requires the organization to establish and maintain an information security risk management process. The
* organization should identify the information security risks, analyze and evaluate the risks, and treat the risks according to the risk criteria and the risk treatment options. The organization should also monitor and review the risks and the risk treatment plan periodically and document the results. The fact that the organization did not identify the security risks associated with Scott's access to the SCM and the source code, such as unauthorized disclosure, modification, or deletion of the information, indicates a failure of the risk management process and a nonconformity with clause 8.2.

NEW QUESTION: 9
Why should materiality be considered during the initial contact?
A. To determine the audit duration
B. To obtain reasonable assurance that the audit can be successfully completed
C. To define processes for minimizing detection risks
Answer: B (LEAVE A REPLY)
Materiality should be considered during the initial contact to obtain reasonable assurance that the audit can be successfully completed. Determining materiality helps establish the threshold for the significance of audit findings, ensuring that the audit focuses on substantial issues that could impact the audit conclusions.

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

NEW QUESTION: 10
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 outsourced the internal audit function, as provided in scenario 9. Does it impact the internal audit process?
A. No, internal audits do not necessarily have to be independent and objective because they have an advisory role
B. No, because the internal audit process can comprise more than an audit program

C. Yes, it increases the independence and impartiality of the internal audit because auditors do not have operational roles related to the ISMS

Answer: (SHOW ANSWER)

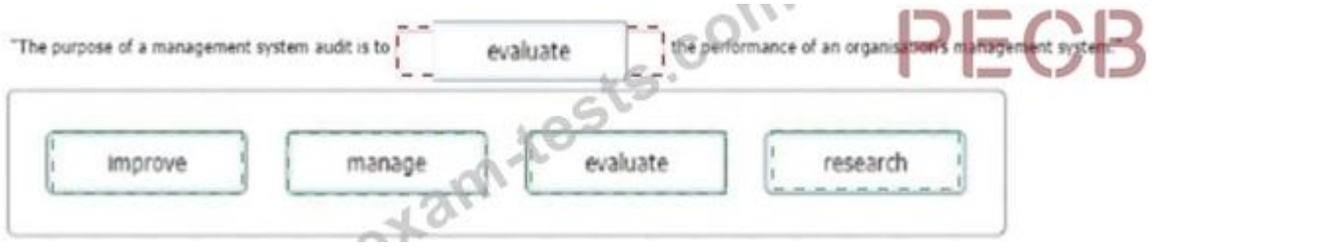
Yes, outsourcing the internal audit function can positively impact the internal audit process by increasing its independence and impartiality. This helps ensure that the internal audits are conducted without any bias or influence from the company's internal management.

NEW QUESTION: 11

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

NEW QUESTION: 13
You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre.
Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.
Select four options for the actions you could take.
A. Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared
B. Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit
C. Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity
D. Note the progress made but hold the audit open until all corrective action has been cleared
E. Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified

F. Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity
G. Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale
H. Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised
Answer: B,E,F,H (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1. The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1.
Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:
Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame. The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.
Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.
Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.

Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised by implementing effective corrective actions for most of them and agreeing on a plan for the remaining one. The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

NEW QUESTION: 14
You are an experienced ISMS audit team leader guiding an auditor in training. You are testing her understanding of follow-up audits by asking her a series of questions to which the answer is either "true* or
'false'. Which four of the following questions should the answer be true"'
A. A follow-up audit may be carried out where nonconformities are major
B. A follow-up audit may be carried out where nonconformities are minor
C. The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified
D. The outcome of a follow-up audit could lower a major nonconformity to minor status
E. The outcome of a follow-up audit could be a recommendabon to suspend the client's certification
F. The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client
G. A follow-up audit is required in all instances where nonconformities have been identified
H. A follow-up audit is required only in instances where a major nonconformity has been identified
Answer: A,B,C,F (LEAVE A REPLY)
Explanation
A follow-up audit may be carried out where nonconformities are major. This is true because a major nonconformity is a situation that raises significant doubt about the ability of the organization's management system to achieve its intended results, and therefore requires immediate corrective action. A follow-up audit is necessary to verify the effectiveness of the corrective action and the conformity of the management system12.
A follow-up audit may be carried out where nonconformities are minor. This is true because a minor nonconformity is a situation that does not affect the capability of the management system to achieve its intended results, but represents a deviation from the specified requirements. A follow-up audit may be conducted to check the implementation of the corrective action and the improvement of the management system12.
The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified. This is true because the top management is responsible for ensuring the effectiveness and continual improvement of the management system, and the audit team leader is accountable for the audit

process and the audit conclusions. The follow-up audit report should provide them with objective evidence of the status of the nonconformities and the corrective actions taken by the auditee13. The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client. This is true because the individual managing the audit programme is responsible for planning, implementing, monitoring and reviewing the audit activities, and the audit client is the organization or person requesting an audit. The follow-up audit report should inform them of the results of the follow-up audit and any changes in the certification status of the auditee13.
References :=
ISO 19011:2022 Guidelines for auditing management systems
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 15
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: C,D,E,G (LEAVE A REPLY)
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: 16
You are an experienced ISMS auditor conducting a third-party surveillance audit at an organisation which offers ICT reclamation services. ICT equipment which companies no longer require is processed by the organisation. It Is either recommissioned and reused or is securely destroyed.
You notice two servers on a bench in the corner of the room. Both have stickers on item with the server's name, IP address and admin password. You ask the ICT Manager about them, and he tells you they were part of a shipment received yesterday from a regular customer.
Which one action should you take?

A. Ask the ICT Manager to record an information security incident and initiate the information security incident management process
B. Note the audit finding and check the process for dealing with incoming shipments relating to customer IT security
C. Record what you have seen in your audit findings, but take no further action
D. Raise a nonconformity against control 5.31 Legal, staturary, regulatory and contractual requirements'
E. Raise a nonconformity against control 8.20 'network security' (networks and network devices shall be secured, managed and controlled to protect information in systems and applications)
F. Ask the auditee to remove the labels, then carry on with the audit
Answer: B (LEAVE A REPLY)
Explanation
According to ISO 27001:2022 clause 8.1.4, the organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This includes implementing appropriate contractual requirements related to information security with external providers, such as customers who send ICT equipment for reclamation12 In this case, the organisation offers ICT reclamation services, which involves processing customer ICT equipment that may contain sensitive or confidential information. The organisation should have a process in place to ensure that the customer ICT equipment is handled securely and in accordance with the customer's information security requirements. The process should include steps such as verifying the customer's identity and authorisation, checking the inventory and condition of the equipment, removing or destroying any labels or stickers that contain information about the equipment or the customer, wiping or erasing any data stored on the equipment, and documenting the actions taken and the results achieved12 The fact that the auditor noticed two servers on a bench with stickers that reveal the server's name, IP address and admin password indicates that the process for dealing with incoming shipments relating to customer IT security is not effective or not followed. This could pose a risk of unauthorised access, disclosure, or modification of the customer's information or systems. Therefore, the auditor should note the audit finding and check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:202212 The other actions are not appropriate for the following reasons:
* A. Asking the ICT Manager to record an information security incident and initiate the information security incident management process is not appropriate because this is not an information security incident that affects the organisation's own information or systems. An information security incident is defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security12 In this case, the information security event affects the customer's information or systems, not the organisation's. Therefore, the organisation should follow the process for dealing with incoming shipments relating to customer IT security, not the process for information security incident management.

* C. Recording what the auditor has seen in the audit findings, but taking no further action is not appropriate because this would not address the root cause or the impact of the issue. The auditor has a responsibility to verify the effectiveness and compliance of the organisation's information security management system, and to report any nonconformities or opportunities for improvement12 Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.
* D. Raising a nonconformity against control 5.31 Legal, statutory, regulatory and contractual requirements is not appropriate because this control is not relevant to the issue. Control 5.31 requires the organisation to identify and comply with the legal, statutory, regulatory and contractual requirements that are applicable to the information security management system12 In this case, the issue is not about the organisation's compliance with the legal, statutory, regulatory and contractual requirements, but
* about the organisation's control of the externally provided processes, products or services that are relevant to the information security management system. Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.
* E. Raising a nonconformity against control 8.20 'network security' (networks and network devices shall be secured, managed and controlled to protect information in systems and applications) is not appropriate because this control is not relevant to the issue. Control 8.20 requires the organisation to secure, manage and control its own networks and network devices to protect the information in its systems and applications12 In this case, the issue is not about the organisation's network security, but about the organisation's control of the externally provided processes, products or services that are relevant to the information security management system. Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.
* F. Asking the auditee to remove the labels, then carry on with the audit is not appropriate because this would not address the root cause or the impact of the issue. The auditor should not interfere with the auditee's operations or suggest corrective actions during the audit, as this would compromise the auditor's objectivity and impartiality12 The auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause
8.1.4 of ISO 27001:2022.
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: 17
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: C (LEAVE A REPLY)
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. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 32. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 12.

NEW QUESTION: 18
What is the standard definition of ISMS?
A. Is an information security systematic approach to achieve business objectives for implementation, establishing, reviewing,operating and maintaining organization's reputation.
B. A company wide business objectives to achieve information security awareness for establishing, implementing, operating, monitoring, reviewing, maintaining and improving
C. A project-based approach to achieve business objectives for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security
D. A systematic approach for establishing, implementing, operating,monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.
Answer: D (LEAVE A REPLY)
The standard definition of ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. This definition is given in clause 3.17 of ISO/IEC 27001:2022, and

it describes the main components and purpose of an ISMS. An ISMS is not a project-based approach, as it is an ongoing process that requires continual improvement. An ISMS is not a company wide business objective, as it is a management system that supports the organization's objectives. An ISMS is not an information security systematic approach, as it is a broader concept that encompasses the organization's context, risks, controls, and performance. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 15. :
ISO/IEC 27001:2022, clause 3.17.

NEW QUESTION: 19
Which one of the following options is the definition of the context of an organisation?
A. The control of internal and external issues that can have an effect on an organisation's desire to achieve its objectives
B. Complexity of internal and external issues that can have an effect on an organisation's approach to developing and achieving its purpose
C. A combination of internal and external issues that can have an effect on an organisation's approach to developing and achieving its objectives
D. The coordination of internal and external issues that can have a positive or negative effect on an organisation's success
Answer: C (LEAVE A REPLY)
The context of the organisation is the business environment in which the organisation operates and defines its information security management system (ISMS). It includes the internal and external factors and conditions that can influence the organisation's information security objectives, strategies, and policies. The context of the organisation helps the organisation to identify the scope, boundaries, and requirements of the ISMS, as well as the interested parties and their expectations. The context of the organisation is determined by considering both internal and external issues, such as the organisational structure, culture, values, mission, vision, objectives, strategies, resources, capabilities, processes, activities, products, services, markets, customers, competitors, suppliers, partners, regulators, laws, regulations, standards, guidelines, best practices, risks, opportunities, threats, vulnerabilities, etc. References: ISO 27001:2022 Clause 4 Context of the organization, ISO 27001 Requirement 4.1 - Understanding the Context of the Organisation, ISO 27001 context of the organization - How to define it - Advisera

NEW QUESTION: 20
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
You are an experienced audit team leader guiding an auditor in training, Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external

clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. The development and maintenance of an information asset inventory
B. Rules for transferring information within the organisation and to other organisations
C. Confidentiality and nondisclosure agreements
D. How protection against malware is implemented
E. Access to and from the loading bay
F. The conducting of verification checks on personnel
G. Remote working arrangements
H. How information security has been addressed within supplier agreements
I. How the organisation evaluates its exposure to technical vulnerabilities
J. The organisation's business continuity arrangements
K. The organisation's arrangements for information deletion
L. Information security awareness, education and training
M. How access to source code and development tools are managed
N. The operation of the site CCTV and door control systems
O. The organisation's arrangements for maintaining equipment
P. How power and data cables enter the building
Answer: D,I,M,N (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), an organization should select and implement appropriate controls to achieve its information security objectives1. The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS1. The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls2. Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:
How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems2. This control is related to control A.12.2.1 of ISO/IEC 27002:20132.
How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures2. This control is related to control A.12.6.1 of ISO/IEC 27002:20132.
How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or

systems that are developed or maintained by the organization or its external providers2. This control is related to control A.14.2.5 of ISO/IEC 27002:20132.
The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed2. This control is related to control A.11.1.4 of ISO/IEC 27002:20132.
The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance of an information asset inventory (related to control A.8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task.
Reference: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION: 21
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. Appoint security staff
B. Encrypt all sensitive information
C. Formulate a policy
D. Set up an access control procedure
Answer: C (LEAVE A REPLY)
An organisational measure is a measure that involves the establishment of policies, procedures, roles, responsibilities, and structures to manage information security within an organization. Examples of organisational measures include security policies, awareness programs, risk assessments, audits, and incident response plans. A policy is a statement of intent or direction that provides guidance for decision making and actions within an organization. A policy defines the scope, objectives, principles, and roles for information security management. Therefore, formulating a policy is the first step in a structured approach to come up with an organisational

measure to protect laptop computers. Reference: ISO/IEC 27000:2022, clause 3.47; ISO/IEC 27001:2022, clause 5.2.

NEW QUESTION: 22
You are an experienced ISMS audit team leader guiding an auditor in training. Your team has just completed a third-party surveillance audit of a mobile telecom provider. The auditor in training asks you how you intend to prepare for the Closing meeting. Which four of the following are appropriate responses?
A. I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge the findings
B. I will instruct my audit team to wait outside the auditee's offices so we can leave as quickly as possible after the closing meeting. This saves our time and the client's time too
C. It is not necessary to prepare for the closing meeting. Once you have carried out as many audits as I have you already know what needs to be discussed
D. I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented
E. I will contact head office to ensure our invoice has been paid, If not, I will cancel the closing meeting and temporarily withhold the audit report
F. I will discuss any follow-up required with my audit team
G. I will review and, as appropriate, approve my teams audit conclusions
H. I will review the audit evidence and the audit findings with the rest of the team
Answer: A,D,F,H (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.6 requires the audit team leader to conduct a closing meeting with the auditee's representatives at the end of the audit to present the audit conclusions and any findings1. The closing meeting should also provide an opportunity for the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1. Therefore, when preparing for the closing meeting, an ISMS auditor should consider the following actions:
I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to collecting and evaluating audit evidence and reaching audit conclusions. The auditor should advise the auditee that the purpose of the closing meeting is for the audit team to communicate their findings, which are based on objective evidence and professional judgement. The auditor should also explain that it is not an opportunity for the auditee to challenge these findings, as they have already been discussed and confirmed during the audit. However, the auditor should also invite the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1.
I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented: This action is appropriate because it reflects the fact that the auditor has followed a planned and agreed audit programme and schedule. The auditor should schedule a

closing meeting with the auditee's representatives at which the audit conclusions will be presented, in accordance with clause
6.6 of ISO 19011:20181. The auditor should also ensure that the closing meeting is attended by those responsible for managing or implementing the ISMS, as well as any other relevant parties1.
I will discuss any follow-up required with my audit team: This action is appropriate because it reflects the fact that the auditor has followed a risk-based approach to determining and reporting any follow-up actions required by the auditee or the certification body. The auditor should discuss any follow-up required with their audit team, such as verifying corrective actions for nonconformities or conducting a subsequent audit1. The auditor should also document any follow-up actions in the audit report1.
I will review and, as appropriate, approve my teams audit conclusions: This action is appropriate because it reflects the fact that the auditor has followed a rigorous and professional process to reaching and reporting audit conclusions. The auditor should review and, as appropriate, approve their teams audit conclusions, which are based on objective evidence and professional judgement. The auditor should also ensure that their teams audit conclusions are consistent with the audit objectives and scope, and reflect the overall performance and conformity of the ISMS1.

NEW QUESTION: 23
You are an experienced ISMS audit team leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-Do-Check-Act cycle in respect of the operation of the information security management system.
You do this by asking him to select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below.
Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

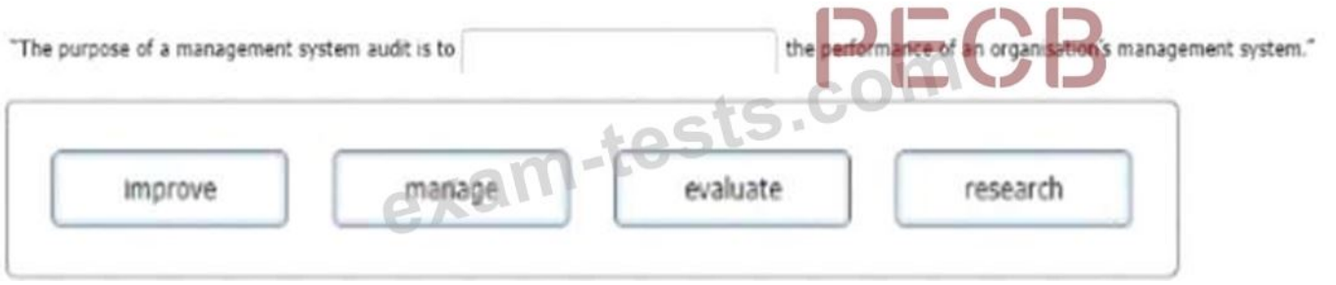
Explanation
* Review is the third stage of the Plan-Do-Check-Act (PDCA) cycle, which is a four-step model for implementing and improving an information security management system (ISMS) according to ISO/IEC
27001:202212. Review involves assessing and measuring the performance of the ISMS against the established policies, objectives, and criteria12.
* Assess is the verb that describes the action of reviewing the ISMS. Assess means to evaluate, analyze, or measure something in a systematic and objective manner3. Assessing the ISMS involves collecting and verifying audit evidence, identifying strengths and weaknesses, and determining the degree of conformity or nonconformity12.
* Regular is the adjective that describes the frequency or interval of reviewing the ISMS. Regular means occurring or done at fixed or uniform intervals4. Reviewing the ISMS at regular intervals means conducting internal audits and management reviews periodically, such as annually, quarterly, or monthly, depending on the needs and risks of the organization12.
* Suitability is one of the attributes that describes the quality or outcome of reviewing the ISMS. Suitability means being appropriate or fitting for a particular purpose, person, or situation5. Reviewing the ISMS for suitability means ensuring that it is aligned with the organization's strategic direction, business objectives, and information security requirements12.
References :=
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance
* Assess | Definition of Assess by Merriam-Webster
* Regular | Definition of Regular by Merriam-Webster
* Suitability | Definition of Suitability by Merriam-Webster

NEW QUESTION: 24
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)
Explanation
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

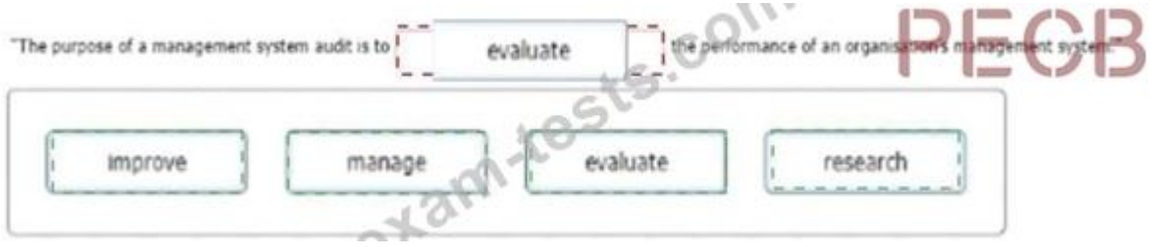
situations encountered during the audit that may decrease the confidence that can be placed in the audit conclusions, such as limitations in the audit scope, access, or sampling3. The standard also states that the audit report should include a statement that the audit is based on a sample of the information 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: 25
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.

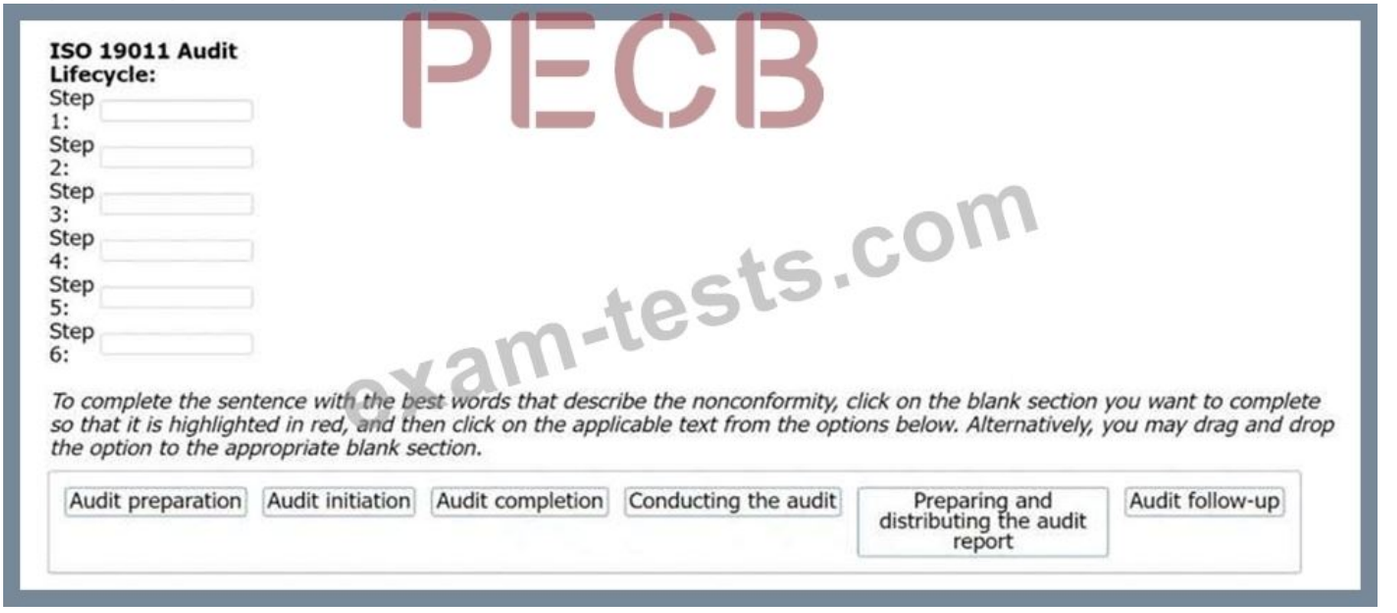
NEW QUESTION: 26
Which of the following factors does NOT contribute to the value of data for an organisation?
A. The correctness of data
B. The indispensability of data
C. The importance of data for processes
D. The content of data
Answer: D (LEAVE A REPLY)
The value of data for an organisation depends on various factors, such as the correctness, indispensability, importance, relevance, timeliness, completeness, and uniqueness of data. The content of data, however, does not contribute to its value, as it is merely the representation of data in a specific format or structure. The content of data can change depending on how it is processed, stored, or presented, but the value of data is derived from its meaning and usefulness for the organisation. Therefore, the correct answer is D. Reference: Putting a value on data - PwC UK, page 3; What is Data Value? How to Define the Value of Your Data.

NEW QUESTION: 27
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. Increase the length of the Stage 2 audit to include the extra sites
B. Obtain information about the additional sites to inform the certification body
C. Arrange to complete a remote Stage 1 audit of the two sites using a video conferencing platform
D. Inform the auditee that the request can be accepted but a full Stage 1 audit must be repeated
Answer: (SHOW ANSWER)
According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, a certification body should establish criteria for determining audit time and audit team composition based on factors such as the scope of certification, size and complexity of the organization, risks associated with its activities, etc2. Therefore, if an auditee requests to extend the audit scope to include two additional sites after completing Stage 1 of an initial certification audit, the audit team leader should obtain information about the additional sites to inform the certification body, so that they can review and approve the change in scope and adjust the audit time and audit team accordingly2. The other options are not appropriate actions for the audit team leader to take in this situation. For example, increasing the length of the Stage 2 audit to include the extra sites without informing the certification body may violate their procedures and policies; arranging to complete a remote Stage 1 audit of the two sites using a video conferencing platform may not be feasible or effective depending on the nature and location of the sites; and informing the auditee that the request can be accepted but a full Stage 1 audit must be repeated may not be necessary or reasonable if there are no significant changes in the auditee's ISMS since Stage 12. Reference: ISO/IEC 17021-1:2015 - Conformity assessment -

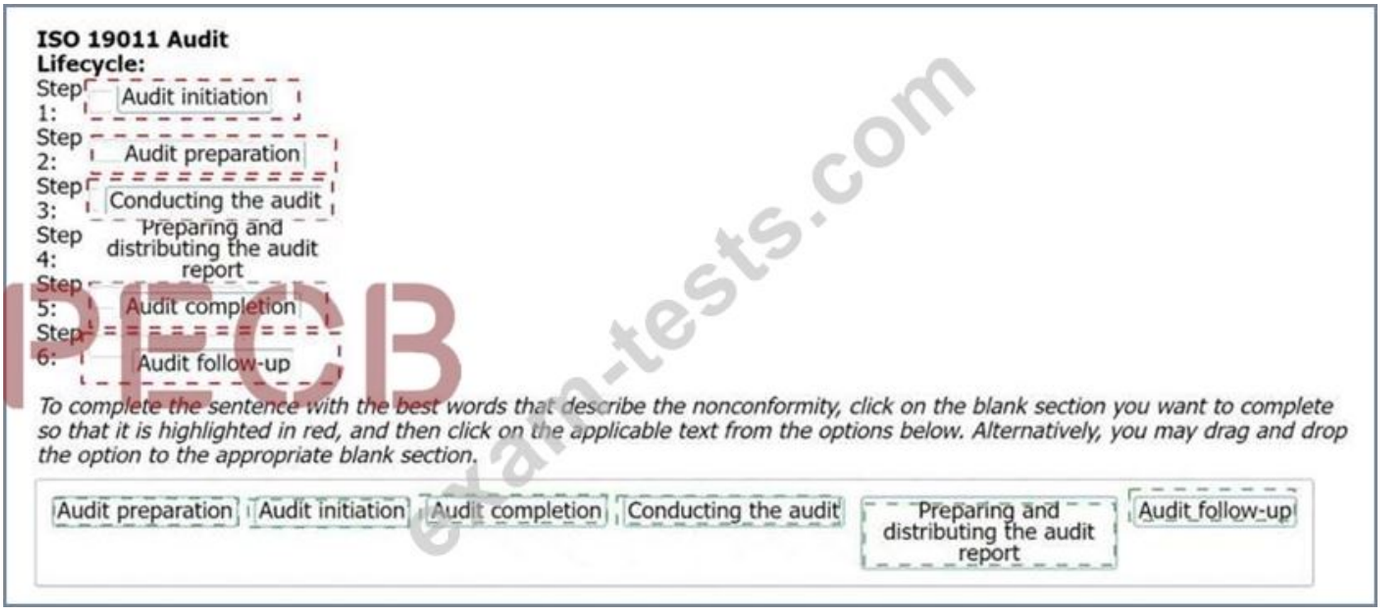
Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 28

The audit lifecycle describes the ISO 19011 process for conducting an individual audit. Drag and drop the steps of the audit lifecycle into the correct sequence.



Answer:



Explanation:

The correct sequence of the steps of the audit lifecycle according to ISO 19011:2018 is:

* Step 1: Audit initiation
* Step 2: Audit preparation
* Step 3: Conducting the audit
* Step 4: Preparing and distributing the audit report
* Step 5: Audit completion
* Step 6: Audit follow-up

This sequence reflects the logical order of the audit activities, from establishing the audit objectives, scope and criteria, to verifying the implementation and effectiveness of the corrective actions. However, ISO 19011:2018 also recognizes that some audit activities can be iterative or concurrent, depending on the nature and complexity of the audit. For example, audit preparation and conducting the audit can overlap when new information or changes occur during the audit. Similarly, audit follow-up can be integrated with audit completion when the corrective actions are verified shortly after the audit. Therefore, the audit lifecycle should be adapted to the specific context and needs of each audit.

NEW QUESTION: 29
Information Security is a matter of building and maintaining _____ .
A. Confidentiality
B. Trust
C. Protection
D. Firewalls
Answer: B (LEAVE A REPLY)
Information security is a matter of building and maintaining trust. Trust is the confidence that information and information processing facilities are protected from unauthorized or malicious actions that could compromise their confidentiality, integrity or availability. Trust is essential for establishing and maintaining relationships with customers, partners, suppliers, employees and other stakeholders who rely on the organization's information and services. Trust is also a key factor for achieving compliance with legal, regulatory and contractual obligations, as well as meeting the organization's own information security objectives and policies. ISO/IEC 27001:2022 defines information security as "preservation of confidentiality, integrity and availability of information" (see clause 3.28) and states that "the purpose of an information security management system is to provide a framework for managing activities that influence the trustworthiness of information" (see Introduction). 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 Trust?

NEW QUESTION: 30
What is the difference between a restricted and confidential document?
A. Restricted - to be shared among an authorized group
Confidential - to be shared among named individuals
B. Restricted - to be shared among named individuals
Confidential - to be shared among an authorized group
C. Restricted - to be shared among named individuals
Confidential - to be shared across the organization only
D. Restricted - to be shared among named individuals
Confidential - to be shared with friends and family
Answer: B (LEAVE A REPLY)

Explanation
The difference between a restricted and confidential document is that a restricted document is to be shared among named individuals, while a confidential document is to be shared among an authorized group.
Restricted and confidential are examples of information classification levels that indicate the sensitivity and value of information and the degree of protection required for it. Restricted documents contain information that could cause serious damage or harm to the organization or its stakeholders if disclosed to unauthorized persons. Therefore, they should only be accessed by specific individuals who have a legitimate need to know and are authorized by the information owner. Confidential documents contain information that could cause damage or harm to the organization or its stakeholders if disclosed to unauthorized persons. Therefore, they should only be accessed by a defined group of people who have a legitimate need to know and are authorized by the information owner. ISO/IEC 27001:2022 requires the organization to classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification (see clause A.8.2.1).
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 Classification?

NEW QUESTION: 31
You are an experienced ISMS audit team leader guiding an auditor in training. Your team has just completed a third-party surveillance audit of a mobile telecom provider. The auditor in training asks you how you intend to prepare for the Closing meeting. Which four of the following are appropriate responses?
A. I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these
B. I will instruct my audit team to wait outside the auditee's offices so we can leave as quickly as possible after the closing meeting. This saves our time and the client's time too
C. It is not necessary to prepare for the closing meeting. Once you have carried out as many audits as I have you already know what needs to be discussed
D. I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented
E. I will contact head office to ensure our invoice has been paid, If not, I will cancel the closing meeting and temporarily withhold the audit report
F. I will discuss any follow-up required with my audit team
G. I will review and, as appropriate, approve my teams audit conclusions
H. I will review the audit evidence and the audit findings with the rest of the team
Answer: A,D,F,H (LEAVE A REPLY)
Explanation
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.6 requires the audit team leader to conduct a closing meeting with the auditee's

representatives at the end of the audit to present the audit conclusions and any findings1. The closing meeting should also provide an opportunity for the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1. Therefore, when preparing for the closing meeting, an ISMS auditor should consider the following actions:
* I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to collecting and evaluating audit evidence and reaching audit conclusions. The auditor should advise the auditee that the purpose of the closing meeting is for the audit team to communicate their findings, which are based on objective evidence and professional judgement. The auditor should also explain that it is not an opportunity for the auditee to challenge these findings, as they have already been discussed and confirmed during the audit. However, the auditor should also invite the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1.
* I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented: This action is appropriate because it reflects the fact that the auditor has followed a planned and agreed audit programme and schedule. The auditor should schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented, in accordance with clause
6.6 of ISO 19011:20181. The auditor should also ensure that the closing meeting is attended by those responsible for managing or implementing the ISMS, as well as any other relevant parties1.
* I will discuss any follow-up required with my audit team: This action is appropriate because it reflects the fact that the auditor has followed a risk-based approach to determining and reporting any follow-up actions required by the auditee or the certification body. The auditor should discuss any follow-up required with their audit team, such as verifying corrective actions for nonconformities or conducting a subsequent audit1. The auditor should also document any follow-up actions in the audit report1.
* I will review and, as appropriate, approve my teams audit conclusions: This action is appropriate because it reflects the fact that the auditor has followed a rigorous and professional process to reaching and reporting audit conclusions. The auditor should review and, as appropriate, approve their teams audit conclusions, which are based on objective evidence and professional judgement. The auditor should also ensure that their teams audit conclusions are consistent with the audit objectives and scope, and reflect the overall performance and conformity of the ISMS1.

NEW QUESTION: 32
You are an ISMS auditor conducting a third-party surveillance audit of a telecom's provider. You are in the equipment staging room where network switches are pre-programmed before being despatched to clients. You note that recently there has been a significant increase in the number of switches failing their initial configuration test and being returned for reprogramming.
You ask the Chief Tester why and she says, 'It's a result of the recent ISMS upgrade'. Before the upgrade each technician had their own hard copy work instructions. Now, the eight members of my team have to share two laptops to access the clients' configuration instructions online. These delays put pressure on the technicians, resulting in more mistakes being made'.
Based solely on the information above, which clause of ISO to raise a nonconformity against' Select one.
A. Clause 7.5 - Documented information
B. Clause 8.1 - Operational planning and control
C. Clause 10.2 - Nonconformity and corrective action
D. Clause 7.3 - Awareness
E. Clause 7.2 - Competence
F. Clause 7.4 - Communication
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 8.1 requires an organization to plan, implement and control its processes needed to meet ISMS requirements2. This includes determining what needs to be done, how it will be done, who will do it, when it will be done, what resources are required, how performance will be evaluated, etc2. Therefore, if an ISMS auditor conducting a third-party surveillance audit of a telecom's provider notes that there has been a significant increase in the number of switches failing their initial configuration test and being returned for reprogramming due to a recent ISMS upgrade that reduced access to work instructions, this indicates a nonconformity against clause 8.1 of ISO/IEC 27001:2022. The organization has failed to plan and control its operational processes effectively to ensure information security and quality2. The other options are not correct clauses to raise a nonconformity against based solely on this information. For example, clause 7.5 deals with documented information required by ISMS or determined by an organization as necessary for its effectiveness2, but it does not specify how many copies or formats of work instructions should be available; clause 10.2 deals with nonconformity and corrective action as a response to an identified problem or incident2, but it does not address how to prevent or avoid such problems or incidents in operational processes; clause 7.3 deals with awareness of ISMS policy, objectives, roles and responsibilities among persons doing work under an organization's control2, but it does not relate to how work instructions are accessed or followed; clause 7.2 deals with competence of persons doing work under an organization's control that affects its ISMS

performance2, but it does not imply that lack of competence is caused by insufficient work instructions; clause
7.4 deals with communication about ISMS among internal and external interested parties2, but it does not cover how operational information is communicated within an organization. References: ISO/IEC 27001:2022
- Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 33
You are an experience ISMS audit team leader carrying out a third-party certification audit of an organization specialising in the secure disposal of confidential documents and removable media. Both documents and media are shredded in military grade devices which make it impossible to reconstruct the original.
The audit has gone well and you are just about to start to write the audit report, 30 minutes before the closing meeting. At this point one of the organization's employees knocks on your door and asks if they can speak to you. They tell you that when things get busy her manager tells her to use a lower grade industrial shredder instead as the organisation has more of these and they operate faster. You were not informed about the existence or use of these machines by the auditee.
Select three options for how you should respond to this information.
A. Advise the individual managing the audit programme of any recommendation by you to conduct a further auditprior to certification
B. Cancel the production of the audit report and instead review the organization's contracts with its clients to determine whether they have permitted the use of lower grade machines
C. Consider the need for a subsequent audit within 4 weeks based on the additional information that has come to light
D. Do nothing. All audits are based on a sample and the sample you took did not include a planned review of the lower grade machines
E. Extend the certification audit duration to create additional time to audit the use of the lower grade machines
F. Raise a nonconformity against 8.1 Operational Planning and Control as the organization has not been open about its processes
G. Verify with the auditee that lower grade machines are used in certain circumstances
Answer: A,C,G (LEAVE A REPLY)
According to ISO/IEC 27001:2022 clause 8.1, the organization must plan, implement and control the processes needed to meet the information security requirements, and to implement the actions determined in clause 6.1. The organization must also ensure that the outsourced processes are controlled or influenced.
According to control A.5.24, the organization must establish and maintain an information security incident management process that includes reporting information security events and weaknesses. Therefore, the use of lower grade machines for the secure disposal of confidential

documents and media could pose a significant information security risk and a potential breach of contract with the clients. The auditor should respond to this information by:
A. Advising the individual managing the audit programme of any recommendation by you to conduct a further audit prior to certification. This is in accordance with ISO/IEC 27006:2022 clause 7.4.3, which states that the audit team leader shall report to the certification body any situation that may significantly affect the audit conclusions or the certification decision, and propose any necessary changes to the audit plan.
C. Considering the need for a subsequent audit within 4 weeks based on the additional information that has come to light. This is in accordance with ISO/IEC 27006:2022 clause 7.5.2, which states that the audit team leader shall review the audit findings and any other appropriate information collected during the audit to determine the audit conclusions, and to identify any need for a subsequent audit.
G. Verifying with the auditee that lower grade machines are used in certain circumstances. This is in accordance with ISO/IEC 27006:2022 clause 7.4.2, which states that the audit team leader shall ensure that the audit is conducted in accordance with the audit plan, and that any changes to the plan are agreed upon and documented.
The other options are not appropriate responses, as they either ignore the information, exceed the scope of the audit, or prematurely raise a nonconformity without sufficient evidence. For example:
B. Cancelling the production of the audit report and instead reviewing the organization's contracts with its clients to determine whether they have permitted the use of lower grade machines. This is not a suitable response, as it would delay the audit process and the certification decision, and it would involve reviewing documents that are outside the scope of the ISMS audit. The auditor should focus on verifying the information security risk assessment and treatment process, and the information security incident management process, as they relate to the use of lower grade machines.
D. Doing nothing. All audits are based on a sample and the sample you took did not include a planned review of the lower grade machines. This is not a suitable response, as it would disregard a significant information security risk and a potential nonconformity that could affect the audit conclusions and the certification decision. The auditor should follow up on the information provided by the employee and verify its validity and impact.
E. Extending the certification audit duration to create additional time to audit the use of the lower grade machines. This is not a suitable response, as it would disrupt the audit schedule and the availability of the audit team and the auditee. The auditor should report the situation to the certification body and propose any necessary changes to the audit plan, such as conducting a subsequent audit.
F. Raising a nonconformity against 8.1 Operational Planning and Control as the organization has not been open about its processes. This is not a suitable response, as it would be based on a single source of information that has not been verified or corroborated. The auditor should collect sufficient and appropriate audit evidence to support any nonconformity, and should also consider the root cause and the severity of the nonconformity.

References:
ISO/IEC 27001:2022, clauses 8.1 and Annex A control A.5.24
ISO/IEC 27006:2022, clauses 7.4.2, 7.4.3, and 7.5.2
[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 18-19, 23-24 A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit ISO 27001 - Annex A.16: Information Security Incident Management

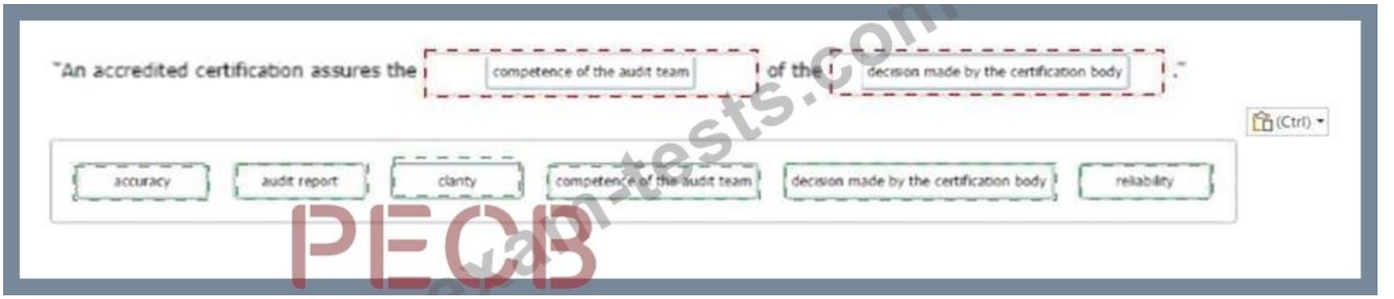
NEW QUESTION: 34
Which two of the following phrases are 'objectives' in relation to a first-party audit?
A. Apply international standards
B. Prepare the audit report for the certification body
C. Confirm the scope of the management system is accurate
D. Complete the audit on time
E. Apply Regulatory requirements
F. Update the management policy
Answer: C,F (LEAVE A REPLY)
A first-party audit is an internal audit conducted by the organization itself or by an external party on its behalf. The objectives of a first-party audit are to: 12
* Confirm the scope of the management system is accurate, i.e., it covers all the processes, activities, locations, and functions that are relevant to the information security objectives and requirements of the organization.
* Update the management policy, i.e., review and revise the policy statement, roles and responsibilities, and objectives and targets of the information security management system (ISMS) based on the audit findings and feedback.
The other phrases are not objectives of a first-party audit, but rather:
* Apply international standards: This is a requirement for the ISMS, not an objective of the audit. The ISMS must conform to the ISO/IEC 27001 standard and any other applicable standards or regulations12
* Prepare the audit report for the certification body: This is an activity of a third-party audit, not a first-party audit. A third-party audit is an external audit conducted by an independent certification body to verify the conformity and effectiveness of the ISMS and to issue a certificate of compliance12
* Complete the audit on time: This is a performance indicator, not an objective of the audit. The audit should be completed within the planned time frame and budget, but this is not the primary purpose of the audit12
* Apply regulatory requirements: This is also a requirement for the ISMS, not an objective of the audit. The ISMS must comply with the legal and contractual obligations of the organization regarding information security12 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: 35

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: 36

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 that the Statement of Applicability (SoA) contains the necessary controls.

You review the latest SoA (version 5) document, sampling the access control to the source code (A.8.4), and want to know how the organisation secures ABC's healthcare mobile app source code received from an outsourced software developer.

The IT Security Manager explains the received source code will be checked into the SCM system to make sure of its integrity and security. Only authorised users will be able to check out the

software to update it. Both check-in and check-out activities will be logged by the system automatically. The version control is managed by the system automatically.
You found a total of 10 user accounts on the SCM. All of them are from the IT department. You further check with the Human Resource manager and confirm that one of the users, Scott, resigned 9 months ago. The SCM System Administrator confirmed Scott's last check-out of the source code was found 1 month ago. He was using one of the authorised desktops from the local network in a secure area.
You check the user de-registration procedure which states "Managers have to make sure of deregistration of the user account and authorisation immediately from the relevant ICT system and/or equipment after resignation approval." There was no deregistration record for user Scott.
The IT Security Manager explains that Scott is a very good software engineer, an ex-colleague, and a friend.
He still comes back to the office every month after he resigned to provide support on source code maintenance. That's why his account on SCM still exists. "We know Scott well and he passed all our background checks when he joined us. As such we didn't feel it necessary to agree any further information security requirements with him just because he is now an external provider".
You prepare the audit findings. Select the three correct options.
A. There is a nonconformity (NC). Scott should have been advised of applicable information security requirements relevant to his new relationship (external provider) with the nursing home. The IT security manager has however confirmed that this did not take place. This does not conform with control A.5.20.
B. There is a nonconformity (NC). The organisation's access control arrangements are not operating effectively as an individual who is no longer employed by the organisation is being permitted to access the nursing home's ICT systems. This does not conform with control A.5.15.
C. There is a nonconformity (NC). The IT Security manager did not make sure the user account for Scott was removed from the SCM and did not complete the user deregistration process after the resignation.
This does not conform with clause 9.1 and control A.5.15.
D. There is a nonconformity (NC). The operating procedures are not well documented. This prevented the SCM System Administrator from being able to remove a user account immediately. This does not conform with clause 9.1 and control A.5.37.
E. There is a nonconformity (NC). The organisation does not have a documented procedure setting out the use of systematic tools to provide access and version control of the source code. This does not conform with clause 9.1 and control A.8.4.
F. There is a nonconformity (NC). The organisation has failed to identify the security risks associated with leaving Scott's account open when he was only re-engaged for a short period monthly. This does not conform with clause 8.2.
G. There is a nonconformity (NC). The SCM is open-source system software. It is not secured and cannot be used for access and version control of the source code. This does not conform with clause 9.1 and control A.8.4.

H. There is a nonconformity (NC). The SCM will log the source code check-in/-out activities automatically. If something goes wrong, the team might not be able to trace it. This does not conform with clause 9.1 and control A.8.4.

Answer: B,C,F (LEAVE A REPLY)

The correct options are:

* There is a nonconformity (NC). The organisation's access control arrangements are not operating effectively as an individual who is no longer employed by the organisation is being permitted to access the nursing home's ICT systems. This does not conform with control A.5.15. (B): This option is correct because control A.5.15 requires the organization to implement secure log-on procedures and manage user access rights. The organization should ensure that only authorized users can access the ICT systems and that the access rights are revoked or modified when the user status changes. The fact that Scott, who resigned 9 months ago, still has an active account on the SCM and can check out the source code, indicates a failure of the access control arrangements and a nonconformity with the control A.5.15.

* There is a nonconformity (NC). The IT Security manager did not make sure the user account for Scott was removed from the SCM and did not complete the user deregistration process after the resignation. This does not conform with clause 9.1 and control A.5.15. : This option is correct because clause 9.1 requires the organization to monitor, measure, analyze, and evaluate the performance and effectiveness of the ISMS. The organization should have processes and indicators to verify that the ISMS requirements and objectives are met and that the ISMS is continually improved. The organization should also ensure that the results of the monitoring and measurement are documented and communicated. The fact that the IT Security manager did not follow the user de-registration procedure and did not document or communicate the exception for Scott, indicates a failure of the monitoring and measurement processes and a nonconformity with clause 9.1 and control A.5.15.

* There is a nonconformity (NC). The organisation has failed to identify the security risks associated with leaving Scott's account open when he was only re-engaged for a short period monthly. This does not conform with clause 8.2. (F): This option is correct because clause 8.2 requires the organization to establish and maintain an information security risk management process. The organization should identify the information security risks, analyze and evaluate the risks, and treat the risks according to the risk criteria and the risk treatment options. The organization should also monitor and review the risks and the risk treatment plan periodically and document the results. The fact that the organization did not identify the security risks associated with Scott's access to the SCM and the source code, such as unauthorized disclosure, modification, or deletion of the information, indicates a failure of the risk management process and a nonconformity with clause 8.2.

NEW QUESTION: 37

You are an experienced ISMS audit team leader guiding an auditor in training. You decide to test her knowledge of follow-up audits by asking her a series of questions. Here are your questions and her answers.

Which four of your questions has she answered correctly?

A. Q: Should a follow-up audit seek to identify new nonconformities? A:YES

B. Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A:YES

C. Q: Should follow-up audits consider agreed opportunities for improvement as well as corrective action? A:No

D. Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A:YES

E. Q: Are follow-up audits required for all audits? A:No

F. Q: Should the outcome from a follow-up audit be reported to the audit team leader who carried out the audit at which the NCs were originally identified? A:YES

G. Q: Should the outcome from a follow-up audit be reported to the audit client? A:No

H. Q: Could an outcome from a follow-up audit be another follow-up audit if required? A:YES

Answer: B,D,E,H (LEAVE A REPLY)

Based on the understanding of follow-up audits, especially in the context of Information Security Management Systems (ISMS) and the guidelines provided by ISO 19011:2018, here are the four questions from your list that the auditor in training has answered correctly:

B. Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A: YES This is correct. The primary purpose of follow-up audits is to verify that nonconformities identified in previous audits have been effectively addressed and the corrective actions taken are suitable and effective.

D. Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A: YES Yes, the follow-up audit aims to verify the completion and effectiveness of corrections and corrective actions. It may also consider the implementation of opportunities for improvement identified during the initial audit.

E. Q: Are follow-up audits required for all audits? A: NO This is correct. Follow-up audits are not automatically required for all audits. They are typically conducted when nonconformities or other significant issues were identified in an earlier audit and there's a need to verify the implementation and effectiveness of the corrective actions.

H. Q: Could an outcome from a follow-up audit be another follow-up audit if required? A: YES Yes, this is a possible outcome. If the follow-up audit finds that the corrective actions have not been fully effective, or if new issues are identified, it may be necessary to conduct another follow-up audit.

The other responses provided by the auditor in training require some clarification or correction. For instance, while a follow-up audit primarily focuses on previously identified nonconformities and corrective actions, it can still identify new nonconformities if observed (A). Opportunities for improvement are generally considered in the scope of regular audits more so than in follow-up audits, which are more narrowly focused on corrective actions (C). Also, the outcomes of follow-up audits should typically be reported to both the audit team leader and the audit client (F and G), ensuring transparency and accountability.

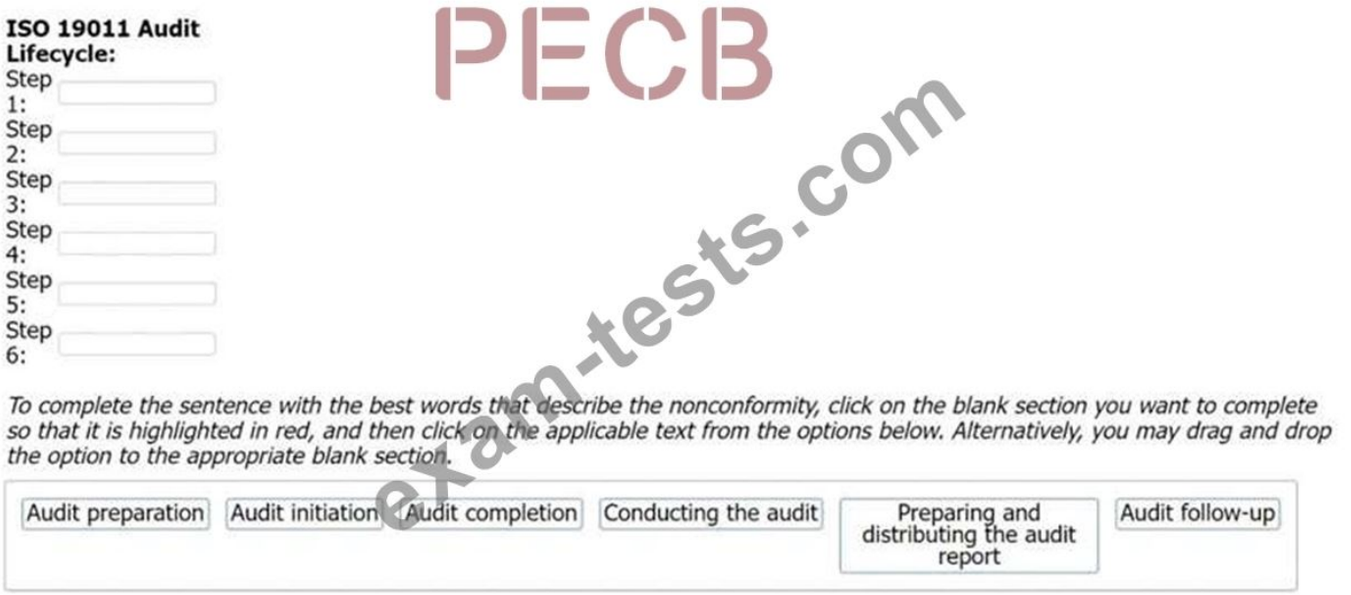
The four questions that the auditor in training has answered correctly are B, D, E, and H.

These questions and answers are consistent with the definition and purpose of a follow-up audit as specified in ISO 19011:2018, Clause 6.712. A follow-up audit is conducted to verify the completion and effectiveness of corrective actions taken as a result of a previous audit (B, D). Follow-up audits are not mandatory for all audits, but they may be required by the audit program, the audit client, or other interested parties (E). The outcome of a follow-up audit may be another follow-up audit if the corrective actions are not satisfactory or not completed within the agreed time frame (H). The other questions and answers are either incorrect or irrelevant. A follow-up audit should not seek to identify new nonconformities, as this is not its objective (A). Follow-up audits should consider agreed opportunities for improvement as well as corrective actions, as they are both outputs of a previous audit. The outcome of a follow-up audit should be reported to the audit client, as well as to other relevant parties, such as the audit team leader who carried out the previous audit (F, G). 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

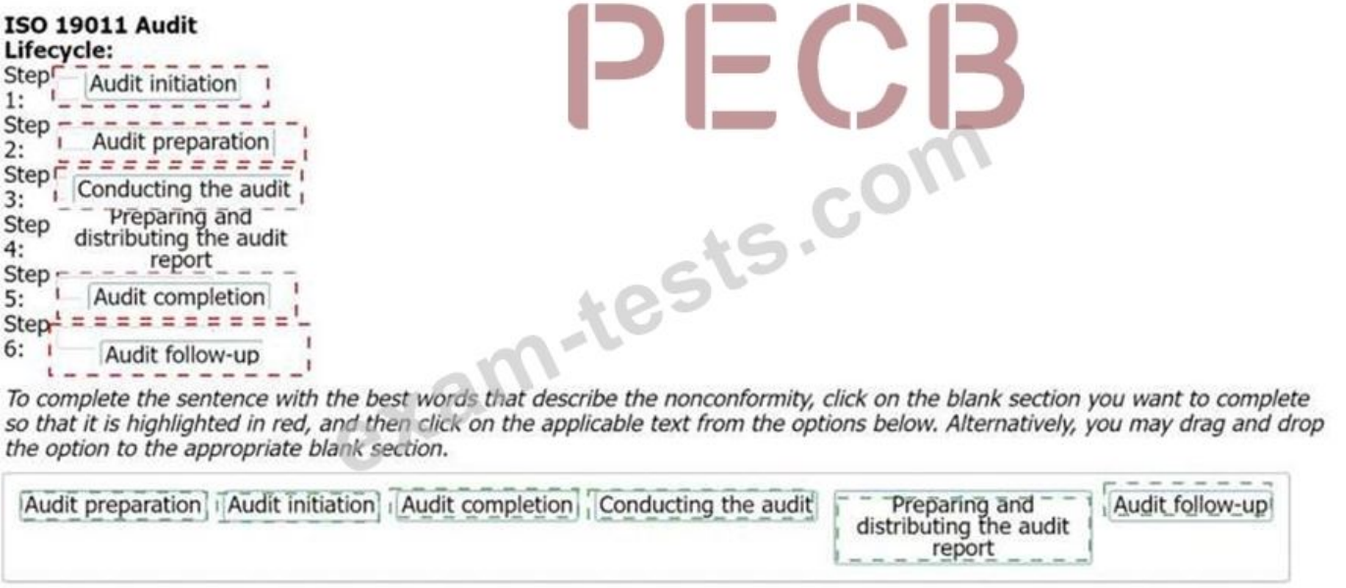
NEW QUESTION: 38
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the PHYSICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. Access to and from the loading bay
B. How power and data cables enter the building
C. Information security awareness, education, and training
D. The conducting of verification checks on personnel
E. The development and maintenance of an information asset inventory
F. The operation of the site CCTV and door control systems
G. The organisation's arrangements for maintaining equipment
H. The organisation's business continuity arrangements
Answer: A,B,F,G (LEAVE A REPLY)
The four controls from the list that are related to PHYSICAL aspects of the ISMS are:
*Access to and from the loading bay
*How power and data cables enter the building
*The operation of the site CCTV and door control systems
*The organisation's arrangements for maintaining equipment
These controls are derived from the ISO 27001 Annex A, which provides a comprehensive list of information security controls that can be applied to an ISMS1. The other controls in the list are more related to ORGANIZATIONAL, LEGAL, or HUMAN aspects of the ISMS, which are also important, but not the focus of this question.

According to the ISMS Auditing Guideline2, the auditor in training should review the PHYSICAL controls by:
*Checking the SoA to identify the applicable controls and their implementation status
*Interviewing the relevant staff and management to verify their understanding and involvement in the controls
*Observing the physical and environmental conditions to confirm the existence and effectiveness of the controls
*Examining the relevant documents and records to validate the compliance and performance of the controls I hope this helps you prepare for the exam.
References: 1: What Are ISO 27001 Controls? A Guide to Annex A | Secureframe; 2: ISMS Auditing Guideline - ISO27000

NEW QUESTION: 39
The audit lifecycle describes the ISO 19011 process for conducting an individual audit. Drag and drop the steps of the audit lifecycle into the correct sequence.



Answer:



Explanation:

The correct sequence of the steps of the audit lifecycle according to ISO 19011:2018 is:

Step 1: Audit initiation

Step 2: Audit preparation

Step 3: Conducting the audit

Step 4: Preparing and distributing the audit report

Step 5: Audit completion

Step 6: Audit follow-up

This sequence reflects the logical order of the audit activities, from establishing the audit objectives, scope and criteria, to verifying the implementation and effectiveness of the corrective actions. However, ISO 19011:2018 also recognizes that some audit activities can be iterative or concurrent, depending on the nature and complexity of the audit. For example, audit preparation and conducting the audit can overlap when new information or changes occur during the audit. Similarly, audit follow-up can be integrated with audit completion when the corrective actions are verified shortly after the audit. Therefore, the audit lifecycle should be adapted to the specific context and needs of each audit.

NEW QUESTION: 40

Information has a number of reliability aspects. Reliability is constantly being threatened.

Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.

Which of these examples is a threat to integrity?

A. a loose cable

B. accidental alteration of data

C. private use of data

D. System restart

Answer: B (LEAVE A REPLY)

A threat to integrity is anything that can compromise the accuracy, completeness or authenticity of information. Accidental alteration of data is an example of such a threat, as it can cause information to be incorrect or inconsistent. A loose cable, a system restart or a private use of data are not threats to integrity, but rather to availability or confidentiality. ISO/IEC 27001:2022 defines integrity as "property of accuracy and completeness" (see clause 3.24). 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 Integrity?

NEW QUESTION: 41

During an opening meeting of a Stage 2 audit, the Managing Director of the client organisation invites the audit team to view a new company video lasting 45 minutes. Which two of the following responses should the audit team leader make?

A. Advise the Managing Director that the audit team has to keep to the planned schedule

B. State that the audit team leader will stay behind after the opening meeting to view the video on behalf of the team

C. Invite the Managing Director to the auditors' hotel for a viewing that evening.

D. Suggest that the video could be viewed during a refreshment break

E. State that the audit team will make a decision on the viewing at a later time

F. Advise the Managing Director that the audit team agrees to his request

Answer: A,D (LEAVE A REPLY)

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

time or losing focus on the audit objectives1. Reference: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 42
Which of the following is a technical security measure?
A. Encryption
B. Security policy
C. Safe storage of backups
D. User role profiles.
Answer: A (LEAVE A REPLY)
A technical security measure is a measure that uses technology to protect information assets from unauthorized access, modification, disclosure, or destruction. Examples of technical security measures include encryption, firewalls, antivirus software, authentication systems, and access control mechanisms. Encryption is a technical security measure that transforms information into an unreadable format using a secret key or algorithm. Encryption protects the confidentiality, integrity, and availability of information by preventing unauthorized parties from accessing or altering it. Therefore, encryption is the correct answer to this question. Reference: ISO/IEC 27000:2022, clause 3.48; ISO/IEC 27002:2022, clause 10.1.

NEW QUESTION: 43
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)
Explanation
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). 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 Preventive Measure?

NEW QUESTION: 44

During an opening meeting of a Stage 2 audit, the Managing Director of the client organisation invites the audit team to view a new company video lasting 45 minutes. Which two of the following responses should the audit team leader make?

A. Advise the Managing Director that the audit team has to keep to the planned schedule

B. State that the audit team leader will stay behind after the opening meeting to view the video on behalf of the team

C. Invite the Managing Director to the auditors' hotel for a viewing that evening.

D. Suggest that the video could be viewed during a refreshment break

E. State that the audit team will make a decision on the viewing at a later time

F. Advise the Managing Director that the audit team agrees to his request

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 45

You are conducting an Information Security Management System 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 non-conformity against clause 8.1 of ISO 27001:2022.
Which one option below that best describes the non-conformity you have identified?
A. The organisation does not have an approved process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have corrected information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational methods to meet information security requirements.
B. The organisation does not have an audited process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have inaccurate information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational rules to meet information security requirements.
C. The organisation does not have an effective process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have disclosed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational controls to meet information security requirements.
D. The organisation does not have an efficient process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have detailed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational procedures to meet information security requirements.
E. The organisation does not have an efficient process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have protected information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational processes to meet information security requirements.
Answer: C (LEAVE A REPLY)
The non-conformity you have identified relates to the organization's failure to implement adequate operational controls to ensure that service and regulatory requirements for data protection are met. This situation is particularly critical given the nature of the items being shipped, which

include sensitive medical information and government documents. The fact that 15% of returned parcels have labels for different addresses, potentially exposing sensitive information to incorrect recipients, underscores the lack of effective information security practices.
The best description of the non-conformity, based on the details provided and the requirements of ISO/IEC
27001:2022, particularly clause 8.1 which deals with operational planning and control, would be:
C. The organisation does not have an effective process in place that ensures service requirements and regulatory requirements for data protection are met. Records show that 15% of returned parcels have disclosed information intended for another party to the recipient (which may include sensitive medical information or government department communications) without adequate operational controls to meet information security requirements.
This option accurately captures the essence of the non-conformity by highlighting the lack of effective operational controls to protect sensitive information, leading to potential unauthorized disclosure of information intended for another party. This is a direct violation of information security management principles, particularly those related to the protection of confidentiality and integrity of information as mandated by ISO/IEC 27001:2022.

NEW QUESTION: 46
What is an example of a human threat?
A. a lightning strike
B. fire
C. phishing
D. thunderstrom
Answer: C (LEAVE A REPLY)
Explanation
A human threat is a threat that originates from a person or a group of people who intentionally or unintentionally cause harm to an organization's information assets. Examples of human threats include hackers, insiders, terrorists, criminals, competitors, or disgruntled employees. A human threat can exploit technical, physical, or organizational vulnerabilities to compromise the confidentiality, integrity, or availability of information. Phishing is an example of a human threat that uses social engineering techniques to trick users into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Phishing attacks often involve sending fraudulent emails or messages that appear to be from legitimate sources, such as banks, government agencies, or trusted contacts. The messages may contain links to malicious websites or attachments that contain malware. Therefore, the correct answer is C. References: ISO/IEC 27000:2022, clause 3.25; What is Phishing? | How to Identify & Avoid Phishing Scams.

NEW QUESTION: 47
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.

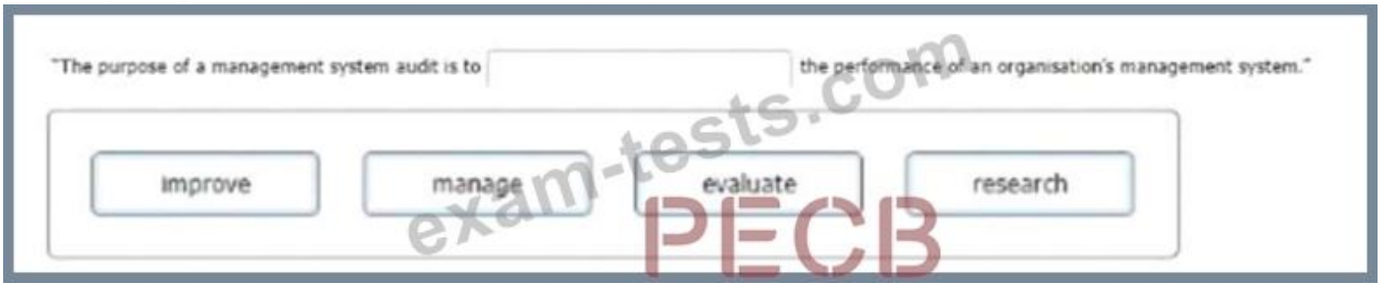
* Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related 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: 48
You are an experienced audit team leader guiding an auditor in training, Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. The development and maintenance of an information asset inventory
B. Rules for transferring information within the organisation and to other organisations
C. Confidentiality and nondisclosure agreements
D. How protection against malware is implemented
E. Access to and from the loading bay
F. The conducting of verification checks on personnel
G. Remote working arrangements
H. How information security has been addressed within supplier agreements
I. How the organisation evaluates its exposure to technical vulnerabilities
J. The organisation's business continuity arrangements
K. The organisation's arrangements for information deletion
L. Information security awareness, education and training
M. How access to source code and development tools are managed
N. The operation of the site CCTV and door control systems
O. The organisation's arrangements for maintaining equipment
P. How power and data cables enter the building
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), an organization should select and implement appropriate controls to achieve its information security objectives1. The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS1. The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls2. Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at

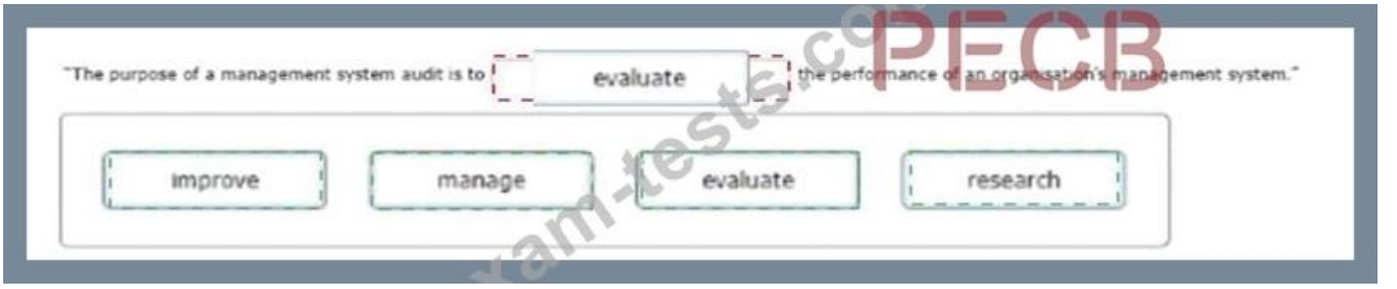
the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:
How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems2. This control is related to control A.12.2.1 of ISO/IEC 27002:20132.
How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures2. This control is related to control A.12.6.1 of ISO/IEC 27002:20132.
How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or systems that are developed or maintained by the organization or its external providers2. This control is related to control A.14.2.5 of ISO/IEC 27002:20132.
The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed2. This control is related to control A.11.1.4 of ISO/IEC 27002:20132.
The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance of an information asset inventory (related to control A.8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control
A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC
27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION: 49
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 organisation's management system."

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: 50
You are performing an ISMS audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to verify the information security of the business continuity management process.
During the audit, you learned that the organisation activated one of the business continuity plans (BCPs) to make sure the nursing service continued during the recent pandemic. You ask Service Manager to explain how the organisation manages information security during the business continuity management process.
The Service Manager presents the nursing service continuity plan for a pandemic and summarises the process as follows:
Stop the admission of any NEW residents.
70% of administration staff and 30% of medical staff will work from home.
Regular staff self-testing including submitting a negative test report 1 day BEFORE they come to the office.
Install ABC's healthcare mobile app, tracking their footprint and presenting a GREEN Health Status QR-Code for checking on the spot.
You ask the Service Manager how to prevent non-relevant family members or interested parties from accessing residents' personal data when staff work from home. The Service Manager cannot answer and suggests the n" Security Manager should help with that.
You would like to further investigate other areas to collect more audit evidence Select three options that will be in your audit trail.
A. Collect more evidence on how the organisation manages information security on mobile devices and during teleworking (Relevant to control A.6.7)
B. Collect more evidence by interviewing more staff about their feeling about working from home. (Relevant to clause 4.2)
C. Collect more evidence on what resources the organisation provides to support the staff working from home. (Relevant to clause 7.1)
D. Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home. (Relevant to clause 6)
E. Collect more evidence on how and when the Business Continuity Wan has been tested. (Relevant to control A.5.29)
F. Collect more evidence on how the organisation makes sure only staff with a negative test result can enter the organisation (Relevant to control A.7.2)
Answer: (SHOW ANSWER)
Explanation
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), control A.5.29 requires an organization to establish and maintain a business continuity management process to ensure the continued availability of information and information systems

at the required level following disruptive incidents1. The organization should identify and prioritize critical information assets and processes, assess the risks and impacts of disruptive incidents, develop and implement business continuity plans (BCPs), test and review the BCPs, and ensure that relevant parties are aware of their roles and responsibilities1. Therefore, when verifying the information security of the business continuity management process, an ISMS auditor should verify that these aspects are met in accordance with the audit criteria.

Three options that will be in the audit trail for verifying control A.5.29 are:

Collect more evidence on how the organisation manages information security on mobile devices and during teleworking (Relevant to control A.6.7): This option is relevant because it can provide evidence of how the organization has implemented appropriate controls to protect the confidentiality, integrity and availability of information and information systems when staff work from home using mobile devices, such as laptops, tablets or smartphones. This is related to control A.6.7, which requires an organization to establish a policy and procedures for teleworking and use of mobile devices1.

Collect more evidence on how and when the Business Continuity Plan has been tested (Relevant to control A.5.29): This option is relevant because it can provide evidence of how the organization has tested and reviewed the BCPs to ensure their effectiveness and suitability for different scenarios, such as a pandemic. This is related to control A.5.29, which requires an organization to test and review the BCPs at planned intervals or when significant changes occur1.

Collect more evidence on how the organisation makes sure only staff with a negative test result can enter the organisation (Relevant to control A.7.2): This option is relevant because it can provide evidence of how the organization has implemented appropriate controls to prevent or reduce the risk of infection or transmission of diseases among staff or residents, such as requiring regular staff self-testing and using a health status app. This is related to control A.7.2, which requires an organization to ensure that all employees and contractors are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational policies and procedures in this respect1.

The other options are not relevant to verifying control A.5.29, as they are not related to the control or its requirements. For example:

Collect more evidence by interviewing more staff about their feeling about working from home (Relevant to clause 4.2): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 4.2, which requires an organization to understand the needs and expectations of interested parties, but not specifically to control A.5.29.

Collect more evidence on what resources the organisation provides to support the staff working from home (Relevant to clause 7.1): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 7.1, which requires an

organization to determine and provide the resources needed for its ISMS, but not specifically to control A.5.29.
Collect more evidence on how the organisation performs a business risk assessment to evaluate how fast the existing residents can be discharged from the nursing home (Relevant to clause 6): This option is not relevant because it does not provide evidence of how the organization has established and maintained a business continuity management process or ensured the continued availability of information and information systems following disruptive incidents. It may be related to clause 6, which requires an organization to plan actions to address risks and opportunities for its ISMS, but not specifically to control A.5.29.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 51
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the PHYSICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. Access to and from the loading bay
B. How power and data cables enter the building
C. Information security awareness, education, and training
D. The conducting of verification checks on personnel
E. The development and maintenance of an information asset inventory
F. The operation of the site CCTV and door control systems
G. The organisation's arrangements for maintaining equipment
H. The organisation's business continuity arrangements
Answer: A,B,F,G (LEAVE A REPLY)
Explanation
The four controls from the list that are related to PHYSICAL aspects of the ISMS are:
*Access to and from the loading bay
*How power and data cables enter the building
*The operation of the site CCTV and door control systems
*The organisation's arrangements for maintaining equipment
These controls are derived from the ISO 27001 Annex A, which provides a comprehensive list of information security controls that can be applied to an ISMS1. The other controls in the list are more related to ORGANIZATIONAL, LEGAL, or HUMAN aspects of the ISMS, which are also important, but not the focus of this question.
According to the ISMS Auditing Guideline2, the auditor in training should review the PHYSICAL controls by:
*Checking the SoA to identify the applicable controls and their implementation status

*Interviewing the relevant staff and management to verify their understanding and involvement in the controls
*Observing the physical and environmental conditions to confirm the existence and effectiveness of the controls
*Examining the relevant documents and records to validate the compliance and performance of the controls I hope this helps you prepare for the exam.
References: 1: What Are ISO 27001 Controls? A Guide to Annex A | Secureframe; 2: ISMS Auditing Guideline - ISO27000

NEW QUESTION: 52
We can leave laptops during weekdays or weekends in locked bins.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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)
Explanation
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). 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 Threat?

NEW QUESTION: 54
Which two of the following statements are true?
A. The benefit of certifying an ISMS is to show the accreditation certificate on the website.
B. The purpose of an ISMS is to demonstrate awareness of information security issues by management.
C. The benefit of certifying an ISMS is to increase the number of customers.

D. The benefits of implementing an ISMS primarily result from a reduction in information security risks.
E. The purpose of an ISMS is to apply a risk management process for preserving information security.
F. The purpose of an ISMS is to demonstrate compliance with regulatory requirements.
Answer: (SHOW ANSWER)
The benefits of implementing an ISMS primarily result from a reduction in information security risks. E. The purpose of an ISMS is to apply a risk management process for preserving information security.
Comprehensive and Detailed Explanation: According to the ISO 27001 standard, the benefits of implementing an ISMS include the following1:
Assuring customers and other stakeholders of the confidentiality, integrity and availability of information Enhancing the ability to respond to information security incidents and minimize their impacts Improving the governance and management of information security Reducing the costs and losses associated with information security breaches Increasing the competitiveness and reputation of the organization Complying with legal, regulatory and contractual obligations The purpose of an ISMS is to provide a systematic approach to managing information security risks, based on the Plan-Do-Check-Act (PDCA) cycle1. The ISMS enables the organization to establish, implement, maintain and continually improve its information security performance, in alignment with its business objectives and the needs and expectations of interested parties1. The ISMS consists of the following elements1:
The information security policy and objectives
The scope and boundaries of the ISMS
The processes and procedures for information security risk assessment and treatment The resources and competencies for information security The roles and responsibilities for information security The performance evaluation and improvement of the ISMS The internal and external communication and awareness of the ISMS References:
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clauses 1, 4, 5, 6, 7, 8, 9 and 10 PECB Candidate Handbook ISO 27001 Lead Auditor, pages 9-11 ISO/IEC 27001:2013 Information Security Management Standards
4 Key Benefits of ISO 27001 Implementation | ISMS.online
ISO/IEC 27001:2022
An Introduction to the ISO 27001 ISMS | Secureframe

NEW QUESTION: 55
CEO sends a mail giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it. The mail should be classified as
A. Internal Mail
B. Public Mail
C. Confidential Mail

D. Restricted Mail

Answer: A (LEAVE A REPLY)

Explanation

The mail sent by the CEO giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it should be classified as internal mail. Internal mail is a type of classification that indicates that the information is intended for internal use only, and should not be disclosed to external parties without authorization. The mail sent by the CEO contains information that is relevant and important for the employees of the company, but may not be suitable for public disclosure, as it may contain sensitive or confidential information about the company's performance, goals, or plans. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 37. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 14.

NEW QUESTION: 56

In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is [b]not[/b] important for determining the value of data for an organization?

A. The content of data.

B. The degree to which missing, incomplete or incorrect data can be recovered.

C. The indispensability of data for the business processes.

D. The importance of the business processes that make use of the data.

Answer: A (LEAVE A REPLY)

Explanation

The content of data is not an important factor for determining the value of data for an organization. The content of data refers to the representation or format of data, such as text, numbers, images, audio, video, etc.

The content of data can change depending on how it is processed, stored, or presented, but the value of data is derived from its meaning and usefulness for the organization. Therefore, the content of data is not relevant for taking out a fire insurance policy, as it does not reflect the potential loss or damage that the organization would suffer if the data was destroyed by fire. The other factors, such as the degree of recoverability, the indispensability, and the importance of data for the business processes, are important for determining the value of data for an organization. These factors indicate how critical the data is for the organization's operations, performance, and competitiveness, and how difficult or costly it would be to restore or replace the data in case of a fire. Therefore, the correct answer is A. References: Putting a value on data - PwC UK, page 3; What is Data Value? How to Define the Value of Your Data.

NEW QUESTION: 57

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: 58

How are data and information related?
A. When meaning and value are assigned to data, it becomes information
B. Information consists of facts and statistics collected together for reference or analysis
C. Data is a collection of structured and unstructured information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Availability means
A. Service should be accessible at the required time and usable only by the authorized entity
B. Service should be accessible at the required time and usable by all
C. Service should not be accessible when required
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
Scenario 6: Sinvestment is an insurance company that offers home, commercial, and life insurance. The company was founded in North Carolina, but have recently expanded in other locations, including Europe and Africa.
Sinvestment is committed to complying with laws and regulations applicable to their industry and preventing any information security incident. They have implemented an ISMS based on ISO/IEC 27001 and have applied for ISO/IEC 27001 certification.
Two auditors were assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment. they started the audit activities. First, they reviewed the documentation required by the standard, including the declaration of the ISMS scope, information security policies, and internal audits reports. The review process was not easy because, although Sinvestment stated that they had a documentation procedure in place, not all documents had the same format.
Then, the audit team conducted several interviews with Sinvestment's top management to understand their role in the ISMS implementation. All activities of the stage 1 audit were performed remotely, except the review of documented information, which took place on-site, as requested by Sinvestment.
During this stage, the auditors found out that there was no documentation related to information security training and awareness program. When asked, Sinvestment's representatives stated that the company has provided information security training sessions to all employees. Stage 1 audit gave the audit team a general understanding of Sinvestment's operations and ISMS.
The stage 2 audit was conducted three weeks after stage 1 audit. The audit team observed that the marketing department (which was not included in the audit scope) had no procedures in place to control employees' access rights. Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the information security policy of the company, the issue was included in the audit report. In addition, during stage 2 audit, the audit team observed that Sinvestment did not record logs of user activities.

The procedures of the company stated that "Logs recording user activities should be retained and regularly reviewed," yet the company did not present any evidence of the implementation of such procedure.
During all audit activities, the auditors used observation, interviews, documented information review, analysis, and technical verification to collect information and evidence. All the audit findings during stages 1 and 2 were analyzed and the audit team decided to issue a positive recommendation for certification.
Based on the scenario above, answer the following question:
The audit team reviewed Sinvestment's documented information on-site, as requested by the company. Is this acceptable?
A. Yes, Sinvestment has the right to require that no document is carried off-site during the documented information review
B. No, Sinvestment cannot decide where the documentation review take place, since a confidentiality agreement was signed prior to stage 1 audit
C. No, the combination of on-site and off-site activities can impact the audit negatively
Answer: A (LEAVE A REPLY)
Yes, it is acceptable for Sinvestment to request that the review of documented information occur on-site. The company has the right to stipulate that no documents be carried off-site, especially to maintain control over sensitive information and ensure confidentiality, which aligns with the security controls expected in ISO/IEC
27001.
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

NEW QUESTION: 61
Review the following statements and determine which two are false:
A. Auditors approved for conducting onsite audits do not require additional training for virtual audits, as there are no significant differences in the skillset required
B. Conducting a technology check in advance of a virtual audit can improve the effectiveness and efficiency of the audit
C. Due to confidentiality and security concerns, screen sharing during a virtual audit is one method by which the audit team can review the auditee's documentation
D. During a virtual audit, auditees participating in interviews are strongly recommended to keep their webcam enabled
E. The number of days assigned to a third-party audit is determined by the auditee's availability
F. The selection of onsite, virtual or combination audits should take into consideration historical performance and previous audit results
Answer: (SHOW ANSWER)
* A: Auditors approved for conducting onsite audits do require additional training for virtual audits to ensure they are competent in using the technology and tools required for conducting audits remotely12.

* E: The number of days assigned to a third-party audit is not determined by the auditee's availability, but rather by factors such as the size and complexity of the organization, the scope of the audit, and the requirements of the certification body34.
References: The answers are verified based on the content and objectives of the ISMS ISO/IEC 27001 Lead Auditor course, as well as the guidelines provided in the reference materials and documents related to the course.

NEW QUESTION: 62
Which four of the following statements about audit reports are true?
A. Audit reports should be produced by the audit team leader with input from the audit team
B. Audit reports should include or refer to the audit plan
C. Audit reports should be sent to the organisation's top management first because their contents could be embarrassing
D. Audit reports should be assumed suitable for general circulation unless they are specifically marked confidential
E. Audit reports should only evidence nonconformity
F. Audit reports should be produced within an agreed timescale
G. Audit reports that are no longer required can be destroyed as part of the organisation's general waste
H. Audit reports should always be reviewed by the client, dated, and signed as 'accepted'
Answer: A,B,F,H (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the audit reports should be produced by the audit team leader with input from the audit team, as they are responsible for collecting and analysing the audit evidence1. The audit reports should also include or refer to the audit plan, as it provides the basis for the audit objectives, scope, criteria, and methodology2. Furthermore, the audit reports should be produced within an agreed timescale, as it is part of the audit programme management and ensures timely communication of the audit results3. Additionally, the audit reports should always be reviewed by the client, dated, and signed as 'accepted', as it confirms the audit completion and the formal agreement on the audit findings and conclusions4.
The other statements are false because:

Audit reports should not be sent to the organisation's top management first because their contents could be embarrassing, as this would compromise the audit impartiality and confidentiality5. Audit reports should be distributed according to the audit programme procedures and the audit plan.
Audit reports should not be assumed suitable for general circulation unless they are specifically marked confidential, as this would violate the audit confidentiality and the protection of personal information.
Audit reports should be treated as confidential documents and only shared with the authorised parties.
Audit reports should not only evidence nonconformity, as this would limit the audit scope and value.
Audit reports should also evidence conformity, improvement opportunities, good practices, and audit observations.
Audit reports that are no longer required should not be destroyed as part of the organisation's general waste, as this would pose a risk to the audit confidentiality and the information security. Audit reports should be retained, disposed, or destroyed according to the audit programme procedures and the applicable legal requirements.
References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 32, section 4.4.32: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.43: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 31, section 4.4.14: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 34, section 4.4.55: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 32, section 4.4.3. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 34, section 4.4.5.

NEW QUESTION: 63
You are an experienced ISMS audit team leader. You are providing an introduction to ISO/IEC 27001:2022 to a class of Quality Management System Auditors who are seeking to retrain to enable them to carry out information security management system audits.
You ask them which of the following characteristics of information does an information security management system seek to preserve?
Which three answers should they provide?
A. Clarity
B. Accessibility
C. Completeness
D. Importance

E. Availability
F. Confidentiality
G. Integrity
H. Efficiency
Answer: E,F,G (LEAVE A REPLY)
These three characteristics are the fundamental properties of information security, as defined by the ISO/IEC
27000 standard, which provides the overview and vocabulary of information security, cybersecurity, and privacy protection12. They are also the basis for the information security objectives and controls of the ISO/IEC 27001 standard, which specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system34. The definitions of these characteristics are as follows12:
*Availability: The property of being accessible and usable upon demand by an authorized entity.
*Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
*Integrity: The property of safeguarding the accuracy and completeness of information and processing methods.
The other characteristics listed in the question, such as clarity, accessibility, completeness, importance, and efficiency, are not directly related to information security, although they may be relevant for other aspects of information management, such as quality, usability, or performance.
References: = 1: ISO/IEC 27000:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection - Overview and vocabulary, clause 32: ISO/IEC 27000:2022 (en), Information security, cybersecurity and privacy protection - Overview and vocabulary13: ISO/IEC
27001:2022 Information technology - Security techniques - Information security management systems - Requirements, clause 6.24: ISO/IEC 27001:2022 (en), Information security, cybersecurity and privacy protection - Information security management systems - Requirements1

NEW QUESTION: 64
Which of the following is a possible event that can have a disruptive effect on the reliability of information?
A. Threat
B. Vulnerability
C. Dependency
D. Risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
Which two of the following phrases would apply to "plan" in relation to the Plan-Do-Check-Act cycle for a business process?

A. Retaining documentation
B. Retaining documentation
C. Organising changes
D. Setting objectives
E. Training staff
F. Providing ICT assets
Answer: D,E (LEAVE A REPLY)
The Plan-Do-Check-Act (PDCA) cycle is a four-step method for implementing and improving processes, products, or services. The "plan" phase involves establishing the objectives and processes necessary to deliver the desired results. This may include setting SMART goals, identifying resources, defining roles and responsibilities, conducting risk assessments, and developing plans for training, communication, and monitoring.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION: 66
You are an experienced ISMS audit team leader guiding an auditor in training. You decide to test her knowledge of follow-up audits by asking her a series of questions. Here are your questions and her answers.
Which four of your questions has she answered correctly?
A. Q: Should a follow-up audit seek to identify new nonconformities? A:YES
B. Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A:YES
C. Q: Should follow-up audits consider agreed opportunities for improvement as well as corrective action? A:No
D. Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A:YES
E. Q: Are follow-up audits required for all audits? A:No
F. Q: Should the outcome from a follow-up audit be reported to the audit team leader who carried out the audit at which the NCs were originally identified? A:YES
G. Q: Should the outcome from a follow-up audit be reported to the audit client? A:No
H. Q: Could an outcome from a follow-up audit be another follow-up audit if required? A:YES
Answer: B,D,E,H (LEAVE A REPLY)
Based on the understanding of follow-up audits, especially in the context of Information Security Management Systems (ISMS) and the guidelines provided by ISO 19011:2018, here are the four questions from your list that the auditor in training has answered correctly:
B). Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A: YES This is correct. The primary purpose of follow-up audits is to verify that nonconformities

identified in previous audits have been effectively addressed and the corrective actions taken are suitable and effective.
D). Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A: YES Yes, the follow-up audit aims to verify the completion and effectiveness of corrections and corrective actions. It may also consider the implementation of opportunities for improvement identified during the initial audit.
E). Q: Are follow-up audits required for all audits? A: NO This is correct. Follow-up audits are not automatically required for all audits. They are typically conducted when nonconformities or other significant issues were identified in an earlier audit and there's a need to verify the implementation and effectiveness of the corrective actions.
H). Q: Could an outcome from a follow-up audit be another follow-up audit if required? A: YES Yes, this is a possible outcome. If the follow-up audit finds that the corrective actions have not been fully effective, or if new issues are identified, it may be necessary to conduct another follow-up audit.
The other responses provided by the auditor in training require some clarification or correction. For instance, while a follow-up audit primarily focuses on previously identified nonconformities and corrective actions, it can still identify new nonconformities if observed (A). Opportunities for improvement are generally considered in the scope of regular audits more so than in follow-up audits, which are more narrowly focused on corrective actions (C). Also, the outcomes of follow-up audits should typically be reported to both the audit team leader and the audit client (F and G), ensuring transparency and accountability.
The four questions that the auditor in training has answered correctly are B, D, E, and H. These questions and answers are consistent with the definition and purpose of a follow-up audit as specified in ISO 19011:2018, Clause 6.712. A follow-up audit is conducted to verify the completion and effectiveness of corrective actions taken as a result of a previous audit (B, D). Follow-up audits are not mandatory for all audits, but they may be required by the audit program, the audit client, or other interested parties (E). The outcome of a follow-up audit may be another follow-up audit if the corrective actions are not satisfactory or not completed within the agreed time frame (H). The other questions and answers are either incorrect or irrelevant. A follow-up audit should not seek to identify new nonconformities, as this is not its objective (A). Follow-up audits should consider agreed opportunities for improvement as well as corrective actions, as they are both outputs of a previous audit . The outcome of a follow-up audit should be reported to the audit client, as well as to other relevant parties, such as the audit team leader who carried out the previous audit (F, G). 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

NEW QUESTION: 67
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:
Does ISO/IEC 27001 require organizations to comply with national laws and regulations?
A. Yes, but relevant legal and contractual requirements do not need to be explicitly identified
B. No, there is no clear indication in the standard as to whether the organization should comply with the national laws and regulations
C. Yes, complying with the applicable legislation is a requirement of ISO/IEC 27001
Answer: (SHOW ANSWER)
ISO/IEC 27001 requires organizations to comply with applicable legal, statutory, regulatory, and contractual requirements, including those pertaining to information security. These requirements must be identified, documented, and kept up to date as part of the organization's ISMS.
References: ISO/IEC 27001:2013 Standard, Clause 6.1.3 (Information security requirements)

NEW QUESTION: 68
What is the standard definition of ISMS?
A. A systematic approach for establishing, implementing, operating,monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

B. A company wide business objectives to achieve information security awareness for establishing, implementing, operating, monitoring, reviewing, maintaining and improving
C. A project-based approach to achieve business objectives for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security
D. Is an information security systematic approach to achieve business objectives for implementation, establishing, reviewing,operating and maintaining organization's reputation.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
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: C,D (LEAVE A REPLY)
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: 70
Select the words that best complete the sentence:

Answer:

Explanation:
A third-party audit is an independent assessment of an organisation's management system by an external auditor, who is not affiliated with the organisation or its customers. The auditor verifies that the management system meets the requirements of a specific standard, such as ISO 27001, and evaluates its effectiveness and performance. The auditor also identifies any strengths, weaknesses, opportunities, or risks of the management system, and provides recommendations for improvement. The purpose of a third-party audit is to provide an objective and impartial evaluation of the organisation's management system, and to inform a certification decision by a certification body. A certification body is an organisation that grants a certificate of conformity to the organisation, after reviewing the audit report and evidence, and confirming that the management system meets the certification criteria. A certification decision is the outcome of the certification process, which can be positive (granting, maintaining, renewing, or expanding the scope of certification) or negative (suspending, withdrawing, or reducing the scope of certification). References:
* PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25

* ISO 19011:2018 - Guidelines for auditing management systems
* The ISO 27001 audit process | ISMS.online

NEW QUESTION: 71
You are an experienced ISMS audit team leader guiding an auditor in training. You decide to test her knowledge of follow-up audits by asking her a series of questions. Here are your questions and her answers.
Which four of your questions has she answered correctly?
A. Q: Should a follow-up audit seek to identify new nonconformities? A:YES
B. Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A:YES
C. Q: Should follow-up audits consider agreed opportunities for improvement as well as corrective action?
A:No
D. Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A:YES
E. Q: Are follow-up audits required for all audits? A:No
F. Q: Should the outcome from a follow-up audit be reported to the audit team leader who carried out the audit at which the NCs were originally identified? A:YES
G. Q: Should the outcome from a follow-up audit be reported to the audit client? A:No
H. Q: Could an outcome from a follow-up audit be another follow-up audit if required? A:YES
Answer: A,B,D,H (LEAVE A REPLY)
Explanation
The four questions that she answered correctly are:
Q: Should a follow-up audit seek to identify new nonconformities? A: YES Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A: YES Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A: YES Q: Could an outcome from a follow-up audit be another follow-up A follow-up audit is an audit that is conducted after a previous audit to verify the implementation and effectiveness of the corrective actions and/or opportunities for improvement that were agreed upon as a result of the previous audit12. Therefore, a follow-up audit should seek to identify new nonconformities that may have arisen since the previous audit, as well as to ensure that the existing nonconformities have been effectively addressed.
A follow-up audit should also consider the agreed opportunities for improvement as well as the corrective actions, because both are intended to enhance the performance and conformity of the ISMS12. However, the follow-up audit should not treat the opportunities for improvement as mandatory requirements, but rather as suggestions that may or may not have been implemented by the auditee3.

The purpose of a follow-up audit is to verify the completion and effectiveness of the corrections, corrective actions, and opportunities for improvement that were agreed upon as a result of the previous audit12. A correction is the action taken to eliminate a detected nonconformity, while a corrective action is the action taken to eliminate the cause of a nonconformity and to prevent its recurrence4. An opportunity for improvement is a potential improvement that is identified during an audit, but is not a nonconformity3.
An outcome from a follow-up audit could be another follow-up audit if required, depending on the nature and severity of the nonconformities and the effectiveness of the corrective actions12. For example, if the follow-up audit reveals that the nonconformities have not been adequately addressed, or that new nonconformities have emerged, then another follow-up audit may be necessary to ensure that the ISMS is compliant and effective.
References:
1: PECB Candidate Handbook - ISO 27001 Lead Auditor, page 25 2: ISO 19011:2018 - Guidelines for auditing management systems, clause 6.7 3: ISO 27007:2017 - Guidelines for information security management systems auditing, clause 7.5.3 4: ISO 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, clause 3.9 and 3.10

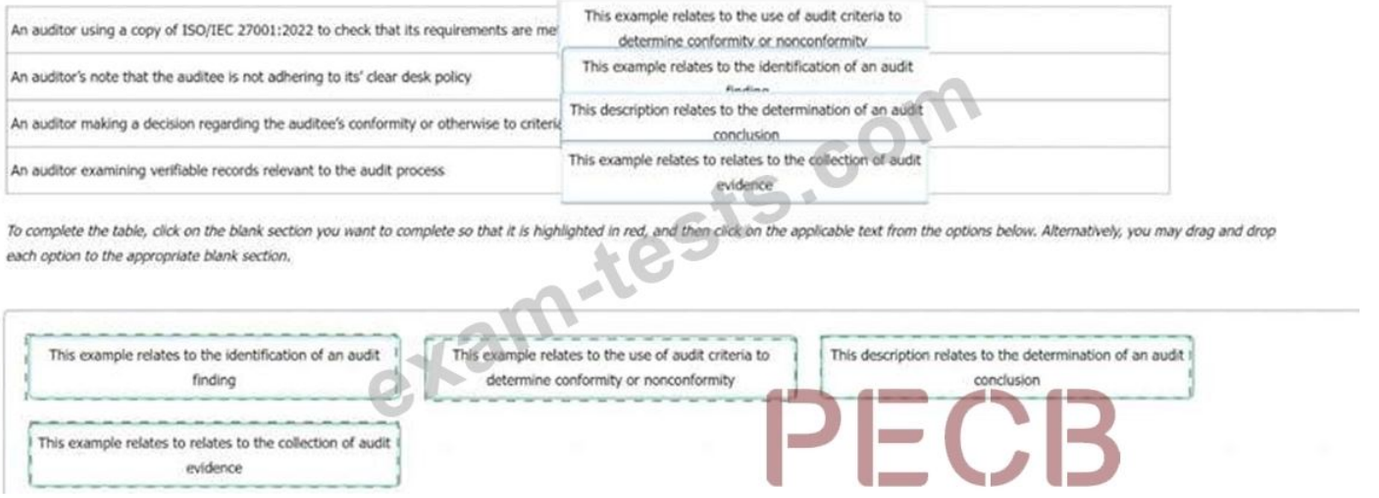
NEW QUESTION: 72
You are performing an ISO 27001 ISMS surveillance audit at a residential nursing home, ABC Healthcare Services. ABC uses a healthcare mobile app designed and maintained by a supplier, WeCare, to monitor residents' well-being. During the audit, you learn that 90% of the residents' family members regularly receive medical device advertisements from WeCare, by email and SMS once a week. The service agreement between ABC and WeCare prohibits the supplier from using residents' personal data. ABC has received many complaints from residents and their family members.
The Service Manager says that the complaints were investigated as an information security incident which found that they were justified.
Corrective actions have been planned and implemented according to the nonconformity and corrective action management procedure.
You write a nonconformity "ABC failed to comply with information security control A.5.34 (Privacy and protection of PII) relating to the personal data of residents' and their family members. A supplier, WeCare, used residents' personal information to send advertisements to family members." Select three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity.
A. ABC asks an ISMS consultant to test the ABC Healthcare mobile app for protection against cyber-crime.
B. ABC cancels the service agreement with WeCare.
C. ABC confirms that information security control A.5.34 is contained in the Statement of Applicability (SoA).
D. ABC discontinues the use of the ABC Healthcare mobile app.

E. ABC introduces background checks on information security performance for all suppliers.
F. ABC periodically monitors compliance with all applicable legislation and contractual requirements involving third parties.
G. ABC takes legal action against WeCare for breach of contract.
H. ABC trains all staff on the importance of maintaining information security protocols.
Answer: B,E,F (LEAVE A REPLY)
The three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity are:
B. ABC cancels the service agreement with WeCare.
E. ABC introduces background checks on information security performance for all suppliers.
F. ABC periodically monitors compliance with all applicable legislation and contractual requirements involving third parties.
B. This option is a possible correction and corrective action that ABC could take to address the nonconformity. A correction is the action taken to eliminate a detected nonconformity, while a corrective action is the action taken to eliminate the cause of a nonconformity and to prevent its recurrence1. By cancelling the service agreement with WeCare, ABC could stop the unauthorized use of residents' personal data and protect their privacy and rights. This could also prevent further complaints and legal issues from the residents and their family members. However, this option may also have some drawbacks, such as the loss of a service provider, the need to find an alternative solution, and the potential impact on the residents' well-being.
E. This option is a possible corrective action that ABC could take to address the nonconformity. By introducing background checks on information security performance for all suppliers, ABC could ensure that they select and work with reliable and trustworthy partners who respect the confidentiality, integrity, and availability of the information they handle. This could also help ABC to comply with information security control A.15.1.1 (Information security policy for supplier relationships), which requires the organisation to agree and document information security requirements for mitigating the risks associated with supplier access to the organisation's assets2.
F. This option is a possible corrective action that ABC could take to address the nonconformity. By periodically monitoring compliance with all applicable legislation and contractual requirements involving third parties, ABC could verify that the suppliers are fulfilling their obligations and responsibilities regarding information security. This could also help ABC to comply with information security control A.18.1.1 (Identification of applicable legislation and contractual requirements), which requires the organisation to identify, document, and keep up to date the relevant legislative, regulatory, contractual, and other requirements to which the organisation is subject3.
References:
1: ISO 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, clause 3.9 and 3.10 2: ISO/IEC 27001:2022 - Information technology

- Security techniques - Information security management systems - Requirements, Annex A, control
A.15.1.1 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, Annex A, control A.18.1.1

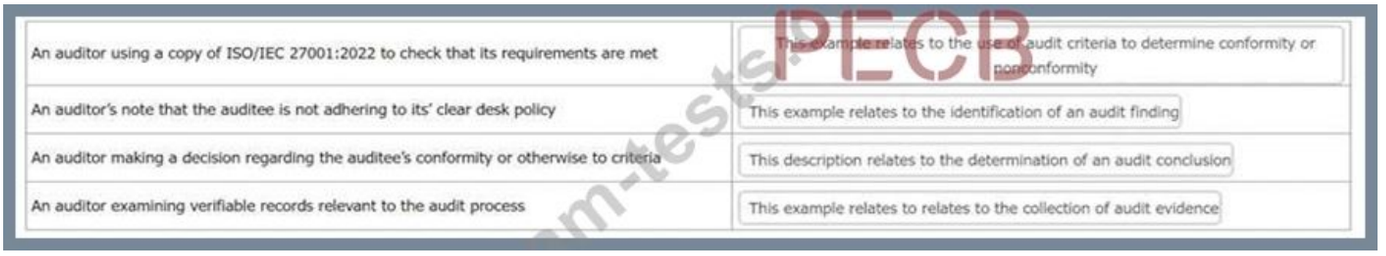
NEW QUESTION: 73
You are an experienced ISMS audit team leader, assisting an auditor in training to write their first audit report.
You want to check the auditor in training's understanding of terminology relating to the contents of an audit report and chose to do this by presenting the following examples.
For each example, you ask the auditor in training what the correct term is that describes the activity Match the activity to the description.

Answer:



Explanation:
1. An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met:
Termed: Reviewing audit criteria.
Justification: The auditor is comparing the auditee's information security management system (ISMS) against the established criteria outlined in the ISO/IEC 27001:2022 standard. This activity falls under the use of audit criteria to determine conformity or nonconformity.
2. An auditor's note that the auditee is not adhering to its clear desk policy:

Termed: Identifying an audit finding.
Justification: The auditor has observed a deviation from the auditee's established policy on clear desks. This observation is documented as a potential nonconformity, which requires further investigation and evaluation.
3. An auditor making a decision regarding the auditee's conformity or otherwise to criteria:
Termed: Determining an audit conclusion.
Justification: Based on the collected audit evidence and evaluation against the established criteria, the auditor forms an opinion about the overall compliance of the auditee's ISMS. This opinion is the audit conclusion and is a key element of the audit report.
4. An auditor examining verifiable records relevant to the audit process:
Termed: Collecting audit evidence.
Justification: The auditor is gathering objective and verifiable information to support their findings and conclusions. This information comes from various sources, including documents, records, interviews, and observations.



NEW QUESTION: 74
Below is Purpose of "Integrity", which is one of the Basic Components of Information Security
A. the property that information is not made available or disclosed to unauthorized individuals
B. the property of safeguarding the accuracy and completeness of assets.
C. the property that information is not made available or disclosed to unauthorized individuals
D. the property of being accessible and usable upon demand by an authorized entity.
Answer: B (LEAVE A REPLY)
Integrity is one of the basic components of information security, along with confidentiality and availability. Integrity means that information is safeguarded from unauthorized or accidental changes that could affect its accuracy and completeness. Integrity ensures that information is reliable and trustworthy3. Reference: ISO/IEC 27001:2022 Lead Auditor Training Course - BSI

NEW QUESTION: 75
There is a network printer in the hallway of the company where you work. Many employees don't pick up their printouts immediately and leave them on the printer.
What are the consequences of this to the reliability of the information?
A. The integrity of the information is no longer guaranteed.
B. The availability of the information is no longer guaranteed.
C. The confidentiality of the information is no longer guaranteed.
D. The Security of the information is no longer guaranteed.
Answer: C (LEAVE A REPLY)

Explanation
Confidentiality is one of the Confidentiality, Integrity, Availability (CIA) principles of information security 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. Often, people do not pick up their prints from a shared printer. This can affect the confidentiality of information, as anyone who passes by the printer can see or take the printed documents that may contain confidential or personal information. This can lead to information leakage, identity theft, fraud, or other malicious activities. Therefore, the correct answer is C.
References: ISO/IEC 27000:2022, clause 3.8; How & Where to Print Sensitive Documents on a Shared Printer.

NEW QUESTION: 76
You are an experienced ISMS audit team leader conducting a third-party surveillance audit of an internet services provider. You are reviewing the organization's risk assessment processes for conformity with ISO/IEC 27001:2022.
Which three of the following audit findings would prompt you to raise a nonconformity report?
A. Both systems contain additional information security risks which are not associated with preserving the confidentiality, integrity and accessibility of information
B. The organisation is treating information security risks in the order in which they are identified
C. The organisation's information security risk assessment process suggests each risk is allocated a risk owner
D. The organisation has not used RAG (Red, Amber, Green) to classify its' information security risks.
Instead, it has used a smiling emoji, a neutral face emoji and a sad face emoji
E. The organisation's risk assessment criteria have not been reviewed and approved by top management
F. The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
G. The organisation has assessed the probability of all of its information security risks as either 0%, 25%,
50%, 75% or 100%
H. There is a different system in place for assessing operational information security risks and for assessing strategic information security risks
Answer: B,E,F (LEAVE A REPLY)
The three audit findings that would prompt you to raise a nonconformity report are:
*The organisation is treating information security risks in the order in which they are identified
*The organisation's risk assessment criteria have not been reviewed and approved by top management
*The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk According to ISO/IEC 27001:2022, clause 6.1.2, the organisation must establish and maintain an information security risk management process that is

consistent with the organisation's context and aligned with its overall risk management approach1. This process must include the following steps:
*Establishing the risk assessment criteria, which must be approved by top management and reflect the organisation's risk appetite and objectives2
*Identifying the information security risks, which must consider the assets, threats, vulnerabilities, impacts, and likelihoods3
*Analysing the information security risks, which must determine the levels of risk and compare them with the risk criteria4
*Evaluating the information security risks, which must prioritise the risks and decide whether they need treatment or not5 Therefore, the audit findings B, E, and F indicate that the organisation is not following the required steps of the information security risk management process, and thus are nonconformities with the standard.
The other audit findings are not necessarily nonconformities, as they may be acceptable depending on the organisation's context and justification. For example:
*Audit finding A may be acceptable if the organisation has identified and treated the additional information security risks that are relevant to its scope and objectives, and has documented the rationale for doing so6
*Audit finding C may be acceptable if the organisation has assigned clear roles and responsibilities for the information security risk management process, and has ensured that the risk owners have the authority and competence to manage the risks7
*Audit finding D may be acceptable if the organisation has defined and communicated the meaning and implications of the emoji-based risk classification, and has ensured that it is consistent with the risk criteria and the risk treatment process8
*Audit finding G may be acceptable if the organisation has justified the use of discrete values for the probability of the information security risks, and has ensured that they are realistic and consistent with the risk criteria and the risk analysis method9
*Audit finding H may be acceptable if the organisation has established and maintained different systems for assessing operational and strategic information security risks, and has ensured that they are integrated and aligned with the overall risk management approach and the ISMS objectives10 References: 1: ISO/IEC 27001:2022, 6.1.2; 2: ISO/IEC 27001:2022, 6.1.2 a); 3: ISO/IEC 27001:2022, 6.1.2 b); 4: ISO/IEC 27001:2022, 6.1.2 c); 5: ISO/IEC 27001:2022, 6.1.2 d); 6: ISO/IEC 27001:2022, A.0.2; 7:
ISO/IEC 27001:2022, 5.3; 8: ISO/IEC 27001:2022, 6.1.2 a) 2); 9: ISO/IEC 27001:2022, 6.1.2 c) 2); 10:
ISO/IEC 27001:2022, 6.1.2 a) 1); : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; :
ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC
27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

NEW QUESTION: 77
You are an experienced ISMS audit team leader. During the conducting of a third-party surveillance audit, you decide to test your auditee's knowledge of ISO/IEC 27001's risk management requirements.
You ask her a series of questions to which the answer is either 'that is true' or 'that is false'. Which four of the following should she answer 'that is true'?
A. The results of risk assessments must be maintained
B. Risk identification is used to determine the severity of an information security risk
C. ISO/IEC 27001 provides an outline approach for the management of risk
D. The organisation must produce a risk treatment plan for every business risk identified
E. The organisation must operate a risk treatment process to eliminate it's information security risks
F. The initial phase in an organisation's risk management process should be information security risk assessment
G. Risks assessments should be undertaken at monthly intervals
H. Risk assessments should be undertaken following significant changes
Answer: A,C,D,H (LEAVE A REPLY)
The following four statements are true according to ISO/IEC 27001's risk management requirements: 12
* The results of risk assessments must be maintained. This is true because clause 8.2.3 of ISO/IEC
27001:2022 requires the organisation to retain documented information of the information security risk assessment process and the results12
* ISO/IEC 27001 provides an outline approach for the management of risk. This is true because clause
6.1.2 of ISO/IEC 27001:2022 specifies the general steps for the information security risk management process, which include establishing the risk criteria, assessing the risks, treating the risks, and monitoring and reviewing the risks12
* The organisation must produce a risk treatment plan for every business risk identified. This is true because clause 6.1.3 of ISO/IEC 27001:2022 requires the organisation to produce a risk treatment plan that defines the actions to be taken to address the unacceptable risks, the responsibilities, the expected dates, and the resources required12

* Risk assessments should be undertaken following significant changes. This is true because clause 8.2.4 of ISO/IEC 27001:2022 requires the organisation to review and update the risk assessment at planned intervals or when significant changes occur12 The following four statements are false according to ISO/IEC 27001's risk management requirements:
* Risk identification is used to determine the severity of an information security risk. This is false because risk identification is used to identify the assets, threats, vulnerabilities, and existing controls that are relevant to the information security risk management process. The severity of an information security risk is determined by the risk analysis, which evaluates the likelihood and impact of the risk scenarios12
* The organisation must operate a risk treatment process to eliminate its information security risks. This is false because the organisation can choose from four options to treat its information security risks: avoid, transfer, mitigate, or accept. The organisation does not have to eliminate all its information security risks, but only those that are unacceptable according to its risk criteria12
* The initial phase in an organisation's risk management process should be information security risk assessment. This is false because the initial phase in an organisation's risk management process should be establishing the risk management framework, which includes defining the risk management policy,
* objectives, scope, roles, responsibilities, and criteria. The information security risk assessment is the second phase in the risk management process12
* Risks assessments should be undertaken at monthly intervals. This is false because there is no fixed frequency for conducting risk assessments in ISO/IEC 27001. The organisation should determine the appropriate intervals for reviewing and updating the risk assessment based on its risk appetite, risk profile, and operational context12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 78
Which two of the following phrases are 'objectives' in relation to a first-party audit?
A. Apply international standards
B. Prepare the audit report for the certification body
C. Confirm the scope of the management system is accurate
D. Complete the audit on time
E. Apply Regulatory requirements
F. Update the management policy
Answer: C,F (LEAVE A REPLY)
A first-party audit is an internal audit conducted by the organization itself or by an external party on its behalf. The objectives of a first-party audit are to: 12
* Confirm the scope of the management system is accurate, i.e., it covers all the processes, activities, locations, and functions that are relevant to the information security objectives and requirements of the organization.

* Update the management policy, i.e., review and revise the policy statement, roles and responsibilities, and objectives and targets of the information security management system (ISMS) based on the audit findings and feedback.
The other phrases are not objectives of a first-party audit, but rather:
* Apply international standards: This is a requirement for the ISMS, not an objective of the audit. The ISMS must conform to the ISO/IEC 27001 standard and any other applicable standards or regulations12
* Prepare the audit report for the certification body: This is an activity of a third-party audit, not a first-party audit. A third-party audit is an external audit conducted by an independent certification body to verify the conformity and effectiveness of the ISMS and to issue a certificate of compliance12
* Complete the audit on time: This is a performance indicator, not an objective of the audit. The audit
* should be completed within the planned time frame and budget, but this is not the primary purpose of the audit12
* Apply regulatory requirements: This is also a requirement for the ISMS, not an objective of the audit. The ISMS must comply with the legal and contractual obligations of the organization regarding information security12 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: 79
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)
Explanation
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: 80
Scenario 9: UpNet, a networking company, has been certified against ISO/IEC 27001. It provides network security, virtualization, cloud computing, network hardware, network management software, and networking technologies.
The company's recognition has increased drastically since gaining ISO/IEC 27001 certification. The certification confirmed the maturity of UpNefs operations and its compliance with a widely recognized and accepted standard.
But not everything ended after the certification. UpNet continually reviewed and enhanced its security controls and the overall effectiveness and efficiency of the ISMS by conducting internal audits. The top management was not willing to employ a full-time team of internal auditors, so they decided to outsource the internal audit function. This form of internal audits ensured independence, objectivity, and that they had an advisory role about the continual improvement of the ISMS.
Not long after the initial certification audit, the company created a new department specialized in data and storage products. They offered routers and switches optimized for data centers and software-based networking devices, such as network virtualization and network security appliances. This caused changes to the operations of the other departments already covered in the ISMS certification scope.

Therefore. UpNet initiated a risk assessment process and an internal audit. Following the internal audit result, the company confirmed the effectiveness and efficiency of the existing and new processes and controls.
The top management decided to include the new department in the certification scope since it complies with ISO/IEC 27001 requirements. UpNet announced that it is ISO/IEC 27001 certified and the certification scope encompasses the whole company.
One year after the initial certification audit, the certification body conducted another audit of UpNefs ISMS.
This audit aimed to determine the UpNefs ISMS fulfillment of specified ISO/IEC 27001 requirements and ensure that the ISMS is being continually improved. The audit team confirmed that the certified ISMS continues to fulfill the requirements of the standard. Nonetheless, the new department caused a significant impact on governing the management system. Moreover, the certification body was not informed about any changes. Thus, the UpNefs certification was suspended.
Based on the scenario above, answer the following question:
Based on scenario 9, why was UpNefs certification suspended?
A. Because UpNet used and applied the certification out of its scope
B. Because UpNet outsourced the internal audit function
C. Because UpNefs ISMS does not fulfill the requirements of the standard
Answer: (SHOW ANSWER)
UpNet's certification was suspended because the certification body was not informed about the significant changes caused by the new department, impacting the governance of the management system. ISO/IEC 27001 requires organizations to inform the certification body of any changes that significantly impact the ISMS.

NEW QUESTION: 81
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

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

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: 82
Information Security is a matter of building and maintaining _____ .
A. Confidentiality
B. Trust

C. Protection
D. Firewalls
Answer: B (LEAVE A REPLY)
Explanation
Information security is a matter of building and maintaining trust. Trust is the confidence that information and information processing facilities are protected from unauthorized or malicious actions that could compromise their confidentiality, integrity or availability. Trust is essential for establishing and maintaining relationships with customers, partners, suppliers, employees and other stakeholders who rely on the organization's information and services. Trust is also a key factor for achieving compliance with legal, regulatory and contractual obligations, as well as meeting the organization's own information security objectives and policies.
ISO/IEC 27001:2022 defines information security as "preservation of confidentiality, integrity and availability of information" (see clause 3.28) and states that "the purpose of an information security management system is to provide a framework for managing activities that influence the trustworthiness of information" (see Introduction). 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 Trust?

NEW QUESTION: 83
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 and explains that the process is based on ISO/IEC 27035-1:2016.
You review the document and notice a statement "any information security weakness, event, and incident should be reported to the Point of Contact (PoC) within 1 hour after identification". When interviewing staff, you found that there were differences in the understanding of the meaning of "weakness, event, and incident".
You sample incident report records from the event tracking system for the last 6 months with summarized results in the following table.

Type of report	Description	Resolution/Recovery Actions	Resolution/ Recovery Time
Information security weakness, report ID: 056	The human resources manager's mobile phone was hacked by ransomware, asking for $1000 to unlock (decrypt) the data	IT department suggests the person shall pay the ransom to unlock the phone. No further action is needed.	24 hours
Information security weakness, report ID: 078	The medical staff's company mobile phone (with patient data) was hacked by ransomware, asking for $5000 to unlock (decrypt) the data	IT department suggests the company shall pay the ransom to unlock the company phone. No further action is needed.	24 hours
Information security event, report ID: 090	The cloud server does not respond and healthcare monitoring stops for 8 hours.	IT department reboots the cloud server remotely. No further action is needed.	24 hours
Information security incident, report ID: 012	The cloud server does not respond and healthcare monitoring stops for 48 hours.	IT department reboots thencloud server remotely. No further action is needed.	24 hours

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

A. Collect more evidence on how and when the Human Resources manager pays the ransom fee to unlock personal mobile data, i.e., credit card, and bank transfer. (Relevant to control A.5.26)

B. Collect more evidence on what the service requirements of healthcare monitoring are. (Relevant to clause 4.2)

C. Collect more evidence on how the organization determined no further action was needed after the incident. (Relevant to control A.5.26)

D. Collect more evidence on how the organisation determined the incident recovery time. (Relevant to control A.5.27)

E. Collect more evidence on the incident recovery procedures. (Relevant to control A.5.26)

F. Collect more evidence by interviewing more staff about their understanding of the reporting process.
(Relevant to control A.6.8)

G. Collect more evidence on how and when the company pays the ransom fee to unlock the company's mobile phone and data, i.e., credit card, and bank transfer. (Relevant to control A.5.26)

Answer: B,G (LEAVE A REPLY)

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 4.2 requires an organization to determine the needs and expectations of interested parties that are relevant to its ISMS1. This includes identifying the legal, regulatory, contractual and other requirements that apply to its information security activities1. Therefore,

collecting more evidence on what the service requirements of healthcare monitoring are may not be relevant to verifying the information security incident management process, as it is not directly related to the audit objective or criteria. This option will not be in the audit trail.

NEW QUESTION: 84
Which one of the following options best describes the main purpose of a Stage 1 third-party audit?
A. To introduce the audit team to the client
B. To learn about the organisation's procurement
C. To determine redness for a stage 2 audit
D. To check for legal compliance by the organisation
E. To prepare an independent audit report
F. To get to know the organisation's customers
Answer: C (LEAVE A REPLY)
The main purpose of a Stage 1 third-party audit is to determine readiness for a Stage 2 audit. A Stage 1 audit is a preliminary assessment that evaluates the organization's ISMS documentation, scope, context, and objectives, and identifies any major gaps or nonconformities that need to be addressed before the Stage 2 audit. A Stage 1 audit does not introduce the audit team to the client, as this is done during the audit planning phase. A Stage 1 audit does not check for legal compliance by the organization, as this is done during the Stage 2 audit. A Stage 1 audit does not prepare an independent audit report, as this is done after the Stage 2 audit. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 70. : ISO/IEC 27001 LEAD AUDITOR - PECB, page 23.

NEW QUESTION: 85
Which is not a requirement of HR prior to hiring?
A. Undergo background verification
B. Applicant must complete pre-employment documentation requirements
C. Must undergo Awareness training on information security.
D. Must successfully pass Background Investigation
Answer: (SHOW ANSWER)
Explanation
According to ISO/IEC 27001:2022, clause 7.2.2, the organization shall ensure that all persons who have access to information are aware of the information security policy and their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance2. Therefore, awareness training on information security is a requirement for all persons, not just new hires. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 86

An employee caught with offense of abusing the internet, such as P2P file sharing or video/audio streaming, will not receive a warning for committing such act but will directly receive an IR.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.
Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.
To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:
*How are responsibilities for IT and IT controls defined and assigned?
*How does Data Grid Inc. assess whether the controls have achieved the desired results?
*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?
*Are firewall-related controls implemented?
Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.
The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.
Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.

Based on this scenario, answer the following question:
Data Grid Inc. is responsible for all the actions below, EXCEPT:
A. Specifying the audit criteria
B. Appointing the audit team
C. Defining the audit scope
Answer: B (LEAVE A REPLY)
In the context of ISO/IEC 27001 audits, the audit team is appointed by the certification body, not by the organization being audited. Data Grid Inc. is responsible for specifying the audit criteria and defining the audit scope, but not for appointing the audit team.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 88
You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.
The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.
Select three options that relate to ISO/IEC 27001:2022's requirements regarding external providers.
A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
E. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
F. I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest
Answer: A,B,E (LEAVE A REPLY)
* A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO

27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12

* B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO
27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the
* information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12
* E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12
* F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO
27001:2022:

* C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12

* D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12
* G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12
* H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The
* organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

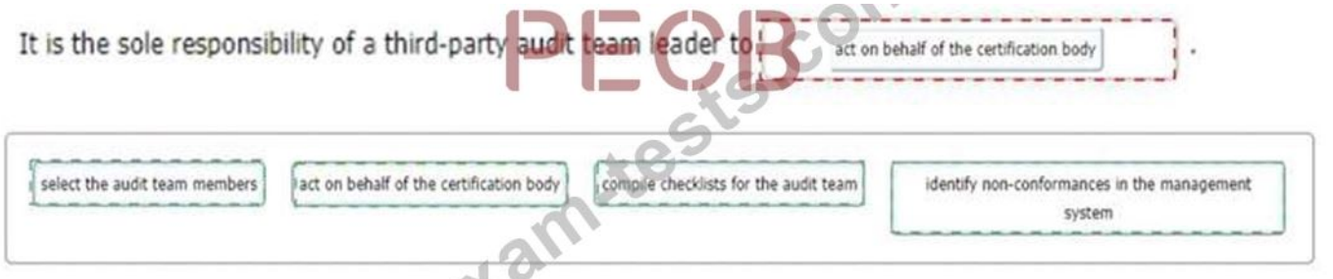
NEW QUESTION: 89
What is the relationship between data and information?
A. Data is structured information.
B. Information is the meaning and value assigned to a collection of data.
Answer: B (LEAVE A REPLY)
The relationship between data and information is that information is the meaning and value assigned to a collection of data. Data is a set of facts, figures, symbols or characters that can be processed by a computer or other means. Data by itself has no inherent meaning or context. Information is data that has been processed, organized, interpreted or presented in a way that makes it useful or meaningful for a specific purpose or audience. Information can be used to convey knowledge, support decision making or communicate messages. ISO/IEC 27001:2022 defines data as "representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or by automatic means" (see clause 3.12) and information as "meaningful data" (see clause 3.25). 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 Data and Information?

NEW QUESTION: 90
After conducting an external audit, the auditor decided that the internal auditor would follow-up on the implementation of corrective actions until the next surveillance audit. Is this acceptable?
A. No, only the external auditor should follow up on the implementation of corrective actions after the completion of the audit
B. Yes, the internal auditor may verify the implementation of corrective actions if it cannot be done by the external auditor
C. Yes, the internal auditor may follow-up on the implementation of corrective actions until a verification from the external auditor during the surveillance audit
Answer: C (LEAVE A REPLY)
Yes, it is acceptable for the internal auditor to follow-up on the implementation of corrective actions until verified by the external auditor during the next surveillance audit. This practice supports continuous improvement and ensures that corrective actions are effectively implemented and maintained over time.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, Clause 9.2 (Internal audit)

NEW QUESTION: 91
Select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:



Explanation

It is the sole responsibility of a third-party audit team leader to act on behalf of the certification body .

* A third-party audit team leader is a person who leads an audit team that conducts audits on behalf of an external organization, such as a certification body, that provides certification or accreditation services to other organizations12.
* One of the main responsibilities of a third-party audit team leader is to act on behalf of the certification body, which means to represent its interests, policies, and procedures during the audit process12.
* Acting on behalf of the certification body involves communicating with the audit client and the auditee, planning and conducting the audit, reporting and evaluating the audit results, and making recommendations for certification or accreditation decisions12.
* Acting on behalf of the certification body also requires maintaining professional integrity, impartiality, confidentiality, and competence throughout the audit process12.

References :=

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

NEW QUESTION: 92

The following are the guidelines to protect your password, except:

A. Don't use the same password for various company system security access

B. Do not share passwords with anyone

C. For easy recall, use the same password for company and personal accounts

D. Change a temporary password on first log-on

Answer: (SHOW ANSWER)

The following are guidelines to protect your password, except for easy recall use the same password for company and personal accounts; do not share passwords with anyone. Using the same password for company and personal accounts is not a guideline to protect your password, as it increases the risk of compromising your password if one of your accounts is hacked or breached. You should use different and unique passwords for each account, and change them regularly. Sharing passwords with anyone is not a guideline to protect your password, as it

reduces the security and accountability of your password. You should keep your password confidential and never disclose it to anyone, even if they claim to be authorized or trustworthy. Don't use the same password for various company system security access is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if one of the systems is compromised or breached. You should use different and complex passwords for each system, and follow the password policies and standards of the organization. Change a temporary password on first log-on is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if the temporary password is intercepted or leaked. You should change the temporary password to a personal and secure password as soon as possible, and avoid using default or predictable passwords. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 43. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

NEW QUESTION: 93
Objectives, criteria, and scope are critical features of a third-party ISMS audit. Which two issues are audit objectives?
A. Evaluate customer processes and functions
B. Assess conformity with ISO/IEC 27001 requirements
C. Fulfil the audit plan
D. Confirm sites operating the ISMS
E. Determine the scope of the ISMS
F. Review organisation efficiency
Answer: (SHOW ANSWER)
Explanation
Audit objectives are the specific purposes or goals that the customer or the certification body wants to achieve through the audit. They define what the audit intends to accomplish and provide the basis for planning and conducting the audit. Audit objectives may vary depending on the type, scope, and criteria of the audit, but they should be clear, measurable, and achievable.
Some examples of audit objectives for a third-party ISMS audit are:
* Assess conformity with ISO/IEC 27001 requirements: This objective means that the audit aims to verify that the organisation's ISMS meets the requirements of the ISO/IEC 27001 standard, which specifies the best practices for establishing, implementing, maintaining, and improving an information security management system. The audit will evaluate the organisation's ISMS documentation, processes, controls, and performance against the standard's clauses and annex A controls.
* Confirm sites operating the ISMS: This objective means that the audit aims to confirm that the organisation's ISMS covers all the relevant sites or locations where the organisation operates or provides its services. The audit will verify that the scope of the ISMS is accurate and consistent with the organisation's context, objectives, and risks.
The other phrases are not audit objectives, but rather:

* Evaluate customer processes and functions: This is not an audit objective, but rather a possible audit criterion or a requirement that the organisation's processes and functions should meet. The audit criterion is the reference against which the audit evidence is compared to determine conformity or nonconformity. The audit criterion may include ISO/IEC 27001 requirements, customer requirements, or other applicable standards or regulations.
* Fulfil the audit plan: This is not an audit objective, but rather a task or an activity that the auditor performs during the audit. The audit plan is a document that describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. The auditor should follow and fulfil the audit plan to ensure that the audit is conducted effectively and efficiently.
* Determine the scope of the ISMS: This is not an audit objective, but rather a prerequisite or an input for conducting the audit. The scope of the ISMS is the extent and boundaries of the information security management system within the organisation. It defines what processes, activities, locations, assets, and
* stakeholders are included or excluded from the ISMS. The scope of the ISMS should be determined by the organisation before applying for certification or undergoing an audit.
* Review organisation efficiency: This is not an audit objective, but rather a possible outcome or a result of conducting an audit. The organisation efficiency is a measure of how well the organisation uses its resources to achieve its goals and objectives. The audit may help review and improve the organisation efficiency by identifying strengths, weaknesses, opportunities, and threats in its information security management system.
References:
* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB
* ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION: 94
An employee caught temporarily storing an MP3 file in his workstation will not receive an IR.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
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)
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 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: 96
Which of the following is an information security management system standard published by the International Organization for Standardization?

A. ISO9008
B. ISO27001
C. ISO5501
D. ISO22301
Answer: B (LEAVE A REPLY)
ISO/IEC 27001:2022 is an information security management system standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The standard is intended to be applicable to all organizations, regardless of type, size or nature. ISO/IEC 27001:2022 is part of the ISO/IEC 27000 family of standards, which provide a comprehensive framework for information security management. 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, ISO/IEC 27000 family - Information security management systems

NEW QUESTION: 97
You are an experienced ISMS audit team leader, talking to an Auditor in training who has been assigned to your audit team. You want to ensure that they understand the importance of the Check stage of the Plan-Do-Check-Act cycle in respect of the operation of the information security management system.
You do this by asking him to select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below.
Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

Explanation:

Review is the third stage of the Plan-Do-Check-Act (PDCA) cycle, which is a four-step model for implementing and improving an information security management system (ISMS) according to ISO/IEC

27001:202212. Review involves assessing and measuring the performance of the ISMS against the established policies, objectives, and criteria12.

Assess is the verb that describes the action of reviewing the ISMS. Assess means to evaluate, analyze, or measure something in a systematic and objective manner3. Assessing the ISMS involves collecting and verifying audit evidence, identifying strengths and weaknesses, and determining the degree of conformity or nonconformity12.

Regular is the adjective that describes the frequency or interval of reviewing the ISMS. Regular means occurring or done at fixed or uniform intervals4. Reviewing the ISMS at regular intervals means conducting internal audits and management reviews periodically, such as annually, quarterly, or monthly, depending on the needs and risks of the organization12.

Suitability is one of the attributes that describes the quality or outcome of reviewing the ISMS. Suitability means being appropriate or fitting for a particular purpose, person, or situation5. Reviewing the ISMS for suitability means ensuring that it is aligned with the organization's strategic direction, business objectives, and information security requirements12.

References :=

ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance Assess | Definition of Assess by Merriam-Webster Regular | Definition of Regular by Merriam-Webster Suitability | Definition of Suitability by Merriam-Webster

NEW QUESTION: 98

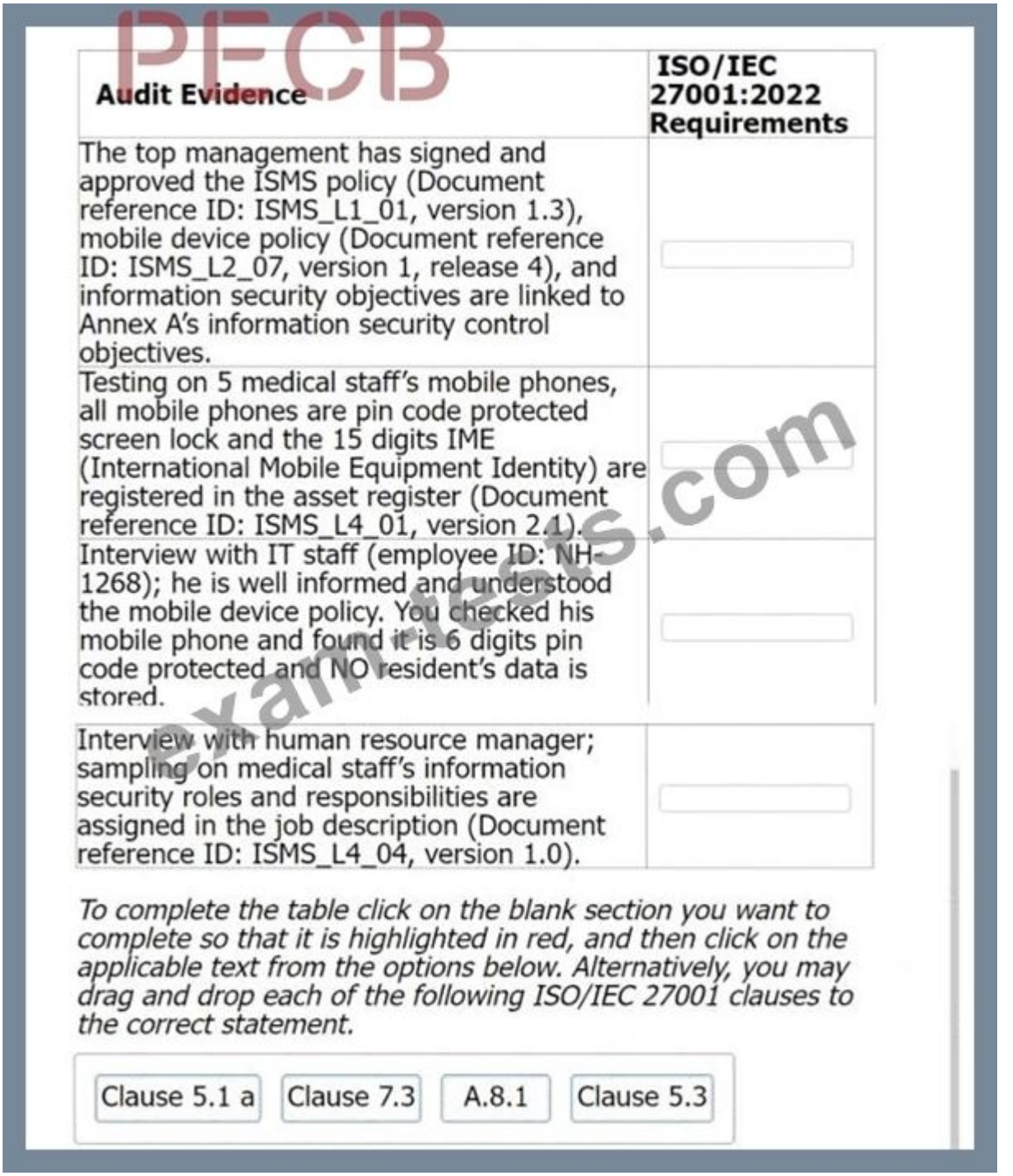
You are performing an ISMS audit at a European-based residential

nursing home called ABC that provides healthcare services. You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.

The next step in your audit plan is to verify that the information security policy and objectives have been established by top management.

During the audit, you found the following audit evidence.

Match the audit evidence to the corresponding requirement in ISO/IEC 27001:2022.



Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	

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 of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a | Clause 7.3 | A.8.1 | Clause 5.3

Answer:

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	Clause 5.1 a
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	A.8.1
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	Clause 7.3
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	Clause 5.3

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 of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a | Clause 7.3 | A.8.1 | Clause 5.3

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	Clause 5.1 a
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	A.8.1
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	Clause 7.3
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	Clause 5.3

NEW QUESTION: 99

You are an experienced audit team leader guiding an auditor in training.

Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.

Select four controls from the following that would you expect the auditor in training to review.

You are an experienced audit team leader guiding an auditor in training, Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.

Select four controls from the following that would you expect the auditor in training to review.

A. The development and maintenance of an information asset inventory

B. Rules for transferring information within the organisation and to other organisations

C. Confidentiality and nondisclosure agreements

D. How protection against malware is implemented

E. Access to and from the loading bay

F. The conducting of verification checks on personnel

G. Remote working arrangements

H. How information security has been addressed within supplier agreements

I. How the organisation evaluates its exposure to technical vulnerabilities

J. The organisation's business continuity arrangements

K. The organisation's arrangements for information deletion

L. Information security awareness, education and training

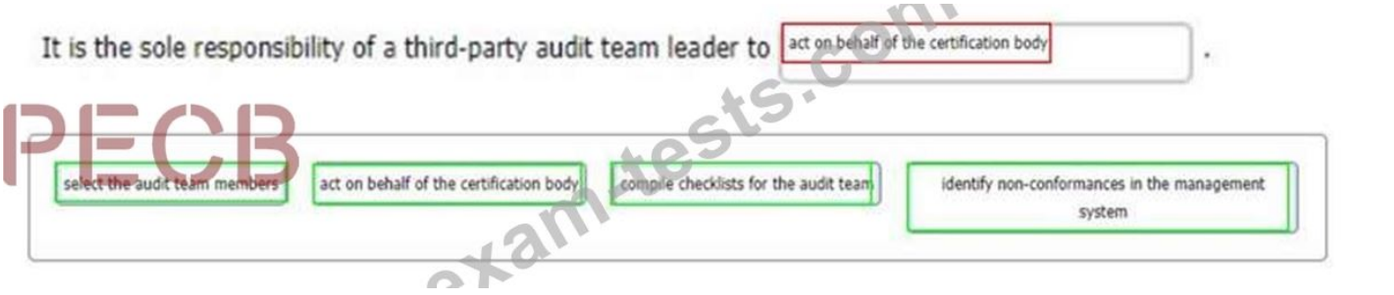
M. How access to source code and development tools are managed

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

control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC
27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION: 100
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:



NEW QUESTION: 101
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: 102
In the event of an Information security incident, system users' roles and responsibilities are to be observed, except:
A. Report suspected or known incidents upon discovery through the Servicedesk
B. Preserve evidence if necessary
C. Cooperate with investigative personnel during investigation if needed
D. Make the information security incident details known to all employees
Answer: D (LEAVE A REPLY)
The role and responsibility that system users should not observe in the event of an information security incident is D: make the information security incident details known to all employees. This is not a proper role or responsibility for system users, as it could cause unnecessary panic, confusion or speculation among employees who are not involved in the incident response process. It could also compromise the confidentiality and integrity of the incident information, which could be sensitive or confidential in nature. Making the information security incident details known to all employees could also violate the information security policies and procedures of the organization, which may require a certain level of discretion and confidentiality when dealing with incidents. The other roles and responsibilities are correct, as they describe what system users should do in the event of an information security incident, such as reporting the incident to the Servicedesk (A), preserving evidence if necessary (B), and cooperating with investigative personnel if needed
. These roles and responsibilities help to ensure a quick, effective and orderly response to information security incidents. ISO/IEC 27001:2022 requires the organization to implement procedures for reporting and managing information security incidents (see clause A.16.1). 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 Security Incident Management?

NEW QUESTION: 103

Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.

Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.

To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:

*How are responsibilities for IT and IT controls defined and assigned?

*How does Data Grid Inc. assess whether the controls have achieved the desired results?

*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?

*Are firewall-related controls implemented?

Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.

The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.

Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.

Based on this scenario, answer the following question:

Based on scenario 5, the audit team assessed the ISMS as a whole, rather than assessing the effectiveness and conformity of each process. Is this acceptable?

A. Yes, due to time constraints for the audit completion, the audit team must obtain absolute assurance by assessing the ISMS as a whole

B. No, the audit team should obtain assurance that the ISMS conforms to the standard requirements by assessing each process

C. Yes, if the audit team has obtained a reasonable assurance that helps them evaluate the ISMS conformity

Answer: (SHOW ANSWER)

Yes, assessing the ISMS as a whole can be acceptable if the audit team obtains reasonable assurance that the system conforms to the standard requirements. The approach taken by the audit team must still ensure that all significant aspects of the ISMS are evaluated adequately, and if this is achieved through a holistic assessment, it is considered sufficient.

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

NEW QUESTION: 104

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: 105
The following options are key actions involved in a first-party audit. Order the stages to show the sequence in which the actions should take place.

Answer:

Explanation

The correct order of the stages is:

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Audit preparation: This stage involves defining the audit objectives, scope, criteria, and plan. The auditor also prepares the audit checklist, which is a list of questions or topics that will be covered during the audit. The audit checklist helps the auditor to ensure that all relevant aspects of the ISMS are addressed and that the audit evidence is collected in a systematic and consistent manner12.

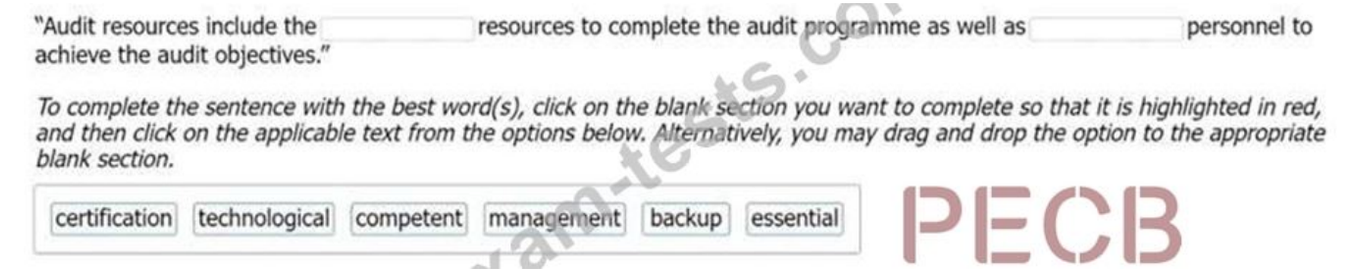
Audit execution: This stage involves conducting the audit activities, such as opening meeting, interviews, observations, document review, and closing meeting. The auditor gathers objective evidence, which is any information that supports the audit findings and conclusions. Objective evidence can be qualitative or quantitative, and can be obtained from various sources, such as records, statements, physical objects, or observations123.

Audit reporting: This stage involves reviewing the audit evidence, evaluating the audit findings, and documenting the audit results. The auditor reviews the audit evidence to determine whether it is sufficient, reliable, and relevant to support the audit findings. The auditor evaluates the audit findings to determine the degree of conformity or nonconformity of the ISMS with the audit criteria. The auditor documents the audit results in an audit report, which is a formal record of the audit process and outcomes. The audit report typically includes the following elements123:

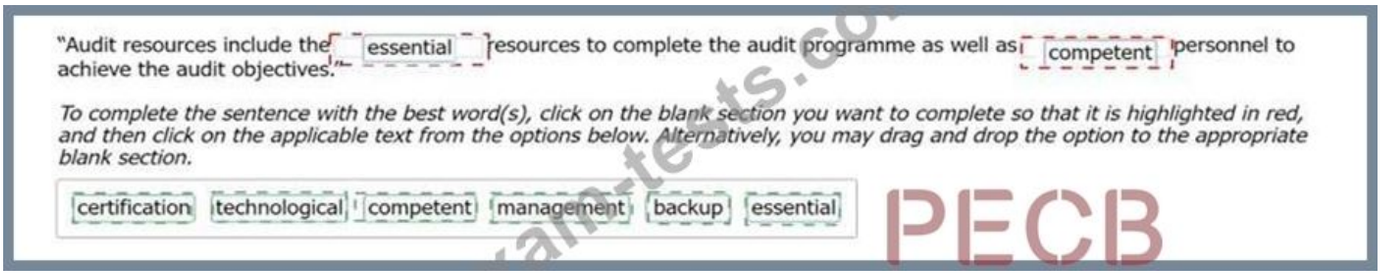
An introduction clarifying the scope, objectives, timing and extent of the work performed An executive summary indicating the key findings, a brief analysis and a conclusion The intended report recipients and, where appropriate, guidelines on classification and circulation Detailed findings and analysis Recommendations for improvement, where applicable A statement of conformity or nonconformity with the audit criteria Any limitations or exclusions of the audit scope or evidence Any deviations from the audit plan or procedures Any unresolved issues or disagreements between the auditor and the auditee A list of references, abbreviations, and definitions used in the report A list of appendices, such as audit plan, audit checklist, audit evidence, audit team members, etc.
Audit follow-up: This stage involves verifying the implementation and effectiveness of the corrective actions taken by the auditee to address the audit findings. The auditor monitors the progress and completion of the corrective actions, and evaluates their impact on the ISMS performance and conformity. The auditor may conduct a follow-up audit to verify the corrective actions on-site, or may rely on other methods, such as document review, remote interviews, or self-assessment by the auditee.
The auditor documents the follow-up results and updates the audit report accordingly123.
References:
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
ISO 19011:2018 - Guidelines for auditing management systems
The ISO 27001 audit process | ISMS.online

NEW QUESTION: 106
Which of the following does an Asset Register contain? (Choose two)
A. Asset Type
B. Asset Modifier
C. Asset Owner
D. Process ID
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 107
Select the words that best complete the sentence below to describe audit resources:



Answer:



Explanation:

According to ISO 19011:2018, clause 5.3, the person responsible for managing the audit programme should determine the resources necessary for the audit programme, such as the audit team members, the budget, the time, the tools, etc. The audit resources should be sufficient and appropriate to ensure the quality and effectiveness of the audit programme and the audit results. The audit resources include the following elements12:

* Essential resources: These are the resources that are required to conduct the audit programme and the individual audits, such as the audit documents, the audit methods, the audit tools, the audit schedule, the audit budget, etc. The essential resources should be identified and allocated based on the audit objectives, scope, and criteria, and the availability and cooperation of the auditee. The essential resources should also be reviewed and updated as necessary to reflect any changes or deviations in the audit programme or the individual audits.
* Competent personnel: These are the audit team members who have the appropriate knowledge, skills, and experience to conduct the audit effectively and efficiently, and to provide credible and reliable audit results and recommendations. The competent personnel should include the audit team leader, the auditors, and any technical experts or observers who support the audit team. The competent personnel should be selected and appointed based on the audit objectives, scope, and criteria, and the specific competence requirements for the audit programme and the individual audits. The competent personnel
* should also be independent and impartial, and avoid any conflicts of interest or self-interest that may affect the audit results or the audit decisions.

References:

* ISO 19011:2018 - Guidelines for auditing management systems, clause 5.3
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19

NEW QUESTION: 108

Which is the glue that ties the triad together

A. Process

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

NEW QUESTION: 109
Scenario 8: EsBank provides banking and financial solutions to the Estonian banking sector since September
2010. The company has a network of 30 branches with over 100 ATMs across the country. Operating in a highly regulated industry, EsBank must comply with many laws and regulations regarding the security and privacy of data. They need to manage information security across their operations by implementing technical and nontechnical controls. EsBank decided to implement an ISMS based on ISO/IEC
27001 because it provided better security, more risk control, and compliance with key requirements of laws and regulations.
Nine months after the successful implementation of the ISMS, EsBank decided to pursue certification of their ISMS by an independent certification body against ISO/IEC 27001 .The certification audit included all of EsBank's systems, processes, and technologies.
The stage 1 and stage 2 audits were conducted jointly and several nonconformities were detected. The first nonconformity was related to EsBank's labeling of information. The company had an information classification scheme but there was no information labeling procedure. As a result, documents requiring the same level of protection would be labeled differently (sometimes as confidential, other times sensitive).
Considering that all the documents were also stored electronically, the nonconformity also impacted media handling. The audit team used sampling and concluded that 50 of 200 removable media stored sensitive information mistakenly classified as confidential. According to the information classification scheme, confidential information is allowed to be stored in removable media, whereas storing sensitive information is strictly prohibited. This marked the other nonconformity.
They drafted the nonconformity report and discussed the audit conclusions with EsBank's representatives, who agreed to submit an action plan for the detected nonconformities within two months.
EsBank accepted the audit team leader's proposed solution. They resolved the nonconformities by drafting a procedure for information labeling based on the classification scheme for both physical and electronic formats.
The removable media procedure was also updated based on this procedure.

Two weeks after the audit completion, EsBank submitted a general action plan. There, they addressed the detected nonconformities and the corrective actions taken, but did not include any details on systems, controls, or operations impacted. The audit team evaluated the action plan and concluded that it would resolve the nonconformities. Yet, EsBank received an unfavorable recommendation for certification.

Based on the scenario above, answer the following question:

Which option justifies the unfavorable recommendation for certification? Refer to scenario 8.

A. The major nonconformity related to storing sensitive information in removable media

B. The minor nonconformity related to the lack of information labeling procedure

C. The unrealistic date of the submitted action plan (two weeks)

Answer: A (LEAVE A REPLY)

The major nonconformity related to storing sensitive information in removable media justifies the unfavorable recommendation for certification. This issue directly contradicts the information classification scheme's stipulations, indicating a significant oversight in enforcing the ISMS policies.

NEW QUESTION: 110

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

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

Answer:

Explanation

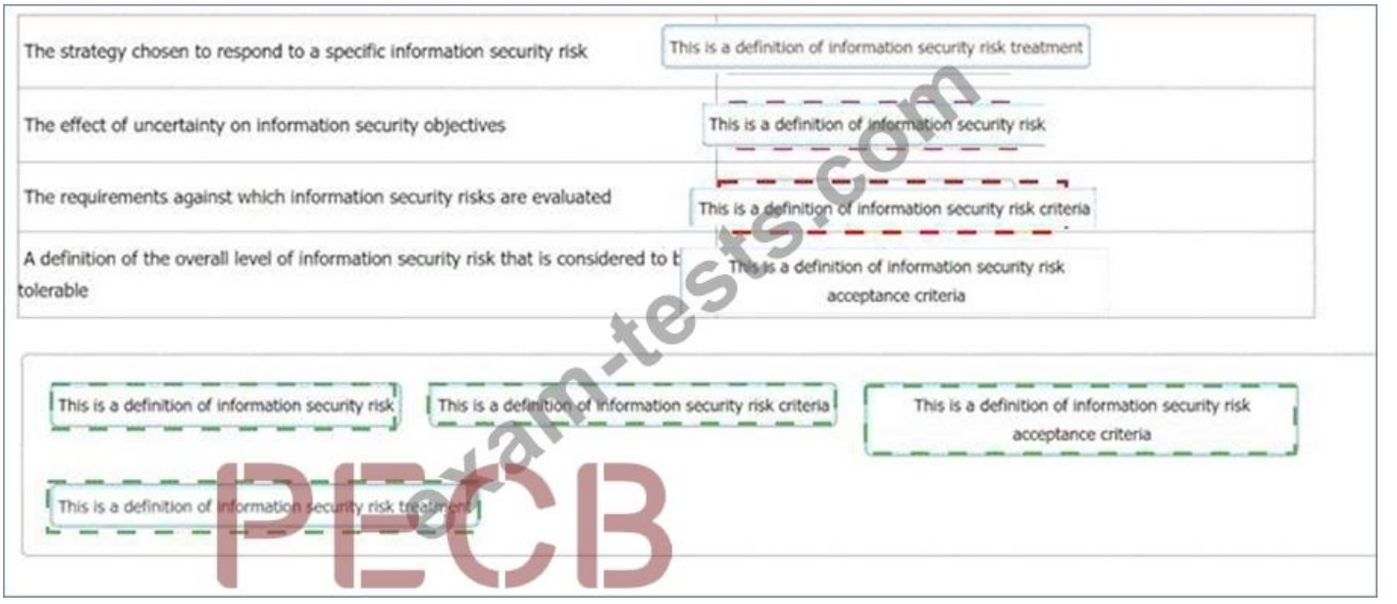
Step 1 = Incident logging Step 2 = Incident categorisation Step 3 = Incident prioritisation Step 4 = Incident assignment Step 5 = Task creation and management Step 6 = SLA management and escalation Step 7 = Incident resolution Step 8 = Incident closure The order of the stages in the information security incident management process should follow a logical sequence that ensures a quick, effective, and orderly response to the incidents, events, and weaknesses. The order should also be consistent with the best practices and guidance provided by ISO/IEC 27001:2022 and ISO/IEC 27035:2022. Therefore, the following order is suggested:
Step 1 = Incident logging: This step involves recording the details of the potential incident, event, or weakness, such as the date, time, source, description, impact, and reporter. This step is important to provide a traceable record of the incident and to facilitate the subsequent analysis and response. This step is related to control A.16.1.1 of ISO/IEC 27001:2022, which requires the organization to establish responsibilities and procedures for the management of information security incidents, events, and weaknesses. This step is also related to clause 6.2 of ISO/IEC 27035:2022, which provides guidance on how to log the incidents, events, and weaknesses.
Step 2 = Incident categorisation: This step involves determining the type and nature of the incident, event, or weakness, such as whether it is a hardware issue, network issue, or software issue. This step is important to classify the incident and to assign it to the appropriate resolver or team. This step is related to control A.16.1.2 of ISO/IEC 27001:2022, which requires the organization to report information security events and weaknesses as quickly as possible through appropriate management channels. This step is also related to clause 6.3 of ISO/IEC 27035:2022, which provides guidance on how to categorize the incidents, events, and weaknesses.
Step 3 = Incident prioritisation: This step involves assessing the severity and urgency of the incident, event, or weakness, and classifying it as critical, high, medium, or low. This step is important to prioritize the incident and to allocate the necessary resources and time for the response. This step is related to control A.16.1.3 of ISO/IEC 27001:2022, which requires the organization to assess and prioritize information security events and weaknesses in accordance with the defined criteria. This step is also related to clause 6.4 of ISO/IEC 27035:2022, which provides guidance on how to prioritize the incidents, events, and weaknesses.
Step 4 = Incident assignment: This step involves passing the incident, event, or weakness to the individual or team who is best suited to resolve it, based on their skills, knowledge, and availability.
This step is important to ensure that the incident is handled by the right person or team and to avoid delays or confusion. This step is related to control A.16.1.4 of ISO/IEC 27001:2022, which requires the organization to respond to information security events and weaknesses in a timely manner, according to the agreed procedures. This step is also related to clause 6.5 of ISO/IEC 27035:2022, which provides guidance on how to assign the incidents, events, and weaknesses.
Step 5 = Task creation and management: This step involves identifying and coordinating the work needed to resolve the incident, event, or weakness, such as performing root cause analysis, testing solutions, implementing changes, and documenting actions. This step is important to ensure that the incident is resolved effectively and efficiently, and that the actions are tracked and

controlled. This step is related to control A.16.1.5 of ISO/IEC 27001:2022, which requires the organization to apply lessons learned from information security events and weaknesses to take corrective and preventive actions. This step is also related to clause 6.6 of ISO/IEC 27035:2022, which provides guidance on how to create and manage the tasks for the incidents, events, and weaknesses.
Step 6 = SLA management and escalation: This step involves ensuring that any service level agreements (SLAs) are adhered to while the resolution is being implemented, and that the incident is escalated to a higher level of authority or support if a breach looks likely or occurs. This step is important to ensure that the incident is resolved within the agreed time frame and quality, and that any deviations or issues are communicated and addressed. This step is related to control A.16.1.6 of ISO/IEC 27001:2022, which requires the organization to communicate information security events and weaknesses to the relevant internal and external parties, as appropriate. This step is also related to clause 6.7 of ISO/IEC
27035:2022, which provides guidance on how to manage the SLAs and escalations for the incidents, events, and weaknesses.
Step 7 = Incident resolution: This step involves applying a temporary workaround or a permanent solution to resolve the incident, event, or weakness, and restoring the normal operation of the information and information processing facilities. This step is important to ensure that the incident is resolved completely and satisfactorily, and that the information security is restored to the desired level.
This step is related to control A.16.1.7 of ISO/IEC 27001:2022, which requires the organization to identify the cause of information security events and weaknesses, and to take actions to prevent their recurrence or occurrence. This step is also related to clause 6.8 of ISO/IEC 27035:2022, which provides guidance on how to resolve the incidents, events, and weaknesses.
Step 8 = Incident closure: This step involves closing the incident, event, or weakness, after verifying that it has been resolved satisfactorily, and that all the actions have been completed and documented.
This step is important to ensure that the incident is formally closed and that no further actions are required. This step is related to control A.16.1.8 of ISO/IEC 27001:2022, which requires the organization to collect evidence and document the information security events and weaknesses, and the actions taken. This step is also related to clause 6.9 of ISO/IEC 27035:2022, which provides guidance on how to close the incidents, events, and weaknesses.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6 ISO/IEC 27035:2022, Information technology - Security techniques - Information security incident management

NEW QUESTION: 111

You have just completed a scheduled information security audit of your organisation when the IT Manager approaches you and asks for your assistance in the revision of the company's risk management process.
He is attempting to update the current documentation to make it easier for other managers to understand, however, it is clear from your discussion he is confusing several key terms.
You ask him to match each of the descriptions with the appropriate risk term. What should the correct answers be?

Answer:



Explanation:
The correct answers for matching each of the descriptions with the appropriate risk term are:
* The strategy chosen to respond to a specific information security risk: This is a definition of information
* security risk treatment. According to ISO/IEC 27000:2022, information security risk treatment is "the process of selecting and implementing measures to modify the information security risk" Section 3.33.

* The effect of uncertainty on information security objectives: This is a definition of information security risk. According to ISO/IEC 27000:2022, information security risk is "the effect of uncertainty on information security objectives" Section 3.32.
* The requirements against which information security risks are evaluated: This is a definition of information security risk criteria. According to ISO/IEC 27000:2022, information security risk criteria are "the terms of reference by which the significance of information security risks is assessed" Section
3.31.
* A definition of the overall level of information security risk that is considered to be tolerable: This is a definition of information security risk acceptance criteria. According to ISO/IEC 27000:2022, information security risk acceptance criteria are "the level of information security risk that is acceptable" Section 3.30.

NEW QUESTION: 112
A hacker gains access to a webserver and can view a file on the server containing credit card numbers.
Which of the Confidentiality, Integrity, Availability (CIA) principles of the credit card file are violated?
A. Availability
B. Confidentiality
C. Integrity
D. Compliance
Answer: B (LEAVE A REPLY)
Confidentiality is one of the Confidentiality, Integrity, Availability (CIA) principles of information security 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 viewing a file containing credit card numbers 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: 113
You have a hard copy of a customer design document that you want to dispose off. What would you do
A. Give it to the office boy to reuse it for other purposes
B. Shred it using a shredder
C. Throw it in any dustbin
D. Be environment friendly and reuse it for writing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
During a follow-up audit, you notice that a nonconformity identified for completion before the follow-up audit is still outstanding.
Which four of the following actions should you take?
A. Report the failure to address the corrective action for the outstanding nonconformity to the organisation's top management
B. Immediately raise an nonconformity as the date for completion has been exceeded
C. If the delay is justified agree on a revised date for clearing the nonconformity with the auditee/audit client
D. Contact the individuals) managing the audit programme to seek their advice as to how to proceed
E. Decide whether the delay in addressing the nonconformity is justified
F. Cancel the follow-up audit and return when an assurance has been received that the nonconformity has been cleared
G. Note the nonconformity is still outstanding and follow audit trails to determine why
H. If the delay is unjustified advise the auditee /audit client and agree on remedial action
Answer: (SHOW ANSWER)
Explanation
According to the ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, the following actions should be taken when a nonconformity identified for completion before the follow-up audit is still outstanding:
* A. Report the failure to address the corrective action for the outstanding nonconformity to the organisation's top management. This is part of the auditor's responsibility to communicate the audit results and ensure that the audit objectives are met12.
* C. If the delay is justified agree on a revised date for clearing the nonconformity with the auditee/audit client. This is part of the auditor's responsibility to verify the effectiveness of the corrective actions taken by the auditee and to close the nonconformity when the evidence is satisfactory12.
* E. Decide whether the delay in addressing the nonconformity is justified. This is part of the auditor's responsibility to evaluate the evidence presented by the auditee and to use professional judgement and objectivity to determine the validity of the reasons for the delay12.
* G. Note the nonconformity is still outstanding and follow audit trails to determine why. This is part of the auditor's responsibility to collect and verify audit evidence and to identify the root causes of the nonconformity12.
References:
* 1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, CQI and IRCA Certified Training, 1
* 2: ISO/IEC 27001 Lead Auditor Training Course, PECB, 2

NEW QUESTION: 115

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

B. Yes, only if EsBank has previously verified the effectiveness of the action plan and informed the audit team that the action plan allows the correction of nonconformities
C. No, the auditee should verify if the action plan allows the correction of nonconformities and elimination of the root causes
Answer: A (LEAVE A REPLY)
Yes, the audit team must evaluate the action plan and verify if it is appropriate for correcting the detected nonconformities. This is part of the auditor's responsibilities to ensure that the proposed actions adequately address the issues identified during the audit.

NEW QUESTION: 116
A decent visitor is roaming around without visitor's ID. As an employee you should do the following, except:
A. Say "hi" and offer coffee
B. Call the receptionist and inform about the visitor
C. Greet and ask him what is his business
D. Escort him to his destination
Answer: A (LEAVE A REPLY)
Explanation
As an employee, you should do the following when you see a visitor roaming around without visitor's ID, except saying "hi" and offering coffee. Saying "hi" and offering coffee is not an appropriate action, as it may imply that you are welcoming or endorsing the visitor without verifying their identity or purpose. This may also give the visitor an opportunity to gain your trust or exploit your kindness. Calling the receptionist and informing about the visitor is an appropriate action, as it alerts the responsible staff to handle the situation and ensure that the visitor is authorized and registered. Greeting and asking him what is his business is an appropriate action, as it shows your concern and curiosity about the visitor's presence and intention. Escorting him to his destination is an appropriate action, as it prevents the visitor from wandering around unattended and accessing unauthorized areas or information. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 42. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

NEW QUESTION: 117
During an audit, the audit team leader reached timely conclusions based on logical reasoning and analysis.
What professional behaviour was displayed by the audit team leader?
A. Decisive
B. Open minded
C. Ethical
D. Perceptive
Answer: (SHOW ANSWER)

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, one of the professional behaviours expected from an audit team leader is to be decisive, which means to "reach timely conclusions based on logical reasoning and analysis" (page 8). Being open minded, ethical, and perceptive are also desirable qualities for an audit team leader, but they do not match the description given in the question.
References: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 8.

NEW QUESTION: 118
You are an audit team leader conducting a third-party surveillance audit of a telecom services provider. You have assigned responsibility for auditing the organisation's information security objectives to a junior member of your audit team. Before they begin their assessment, you ask them the following question to check their understanding of the requirements of ISO/IEC 27001:2022.
Which four of the following criteria must Information security objectives fulfil?
A. They must be communicated appropriately
B. They must be available as documented information
C. They must always be measured
D. They must always be monitored
E. They must be reviewed annually
F. They must be clear and unambiguous
G. They must be consistent with the IS Policy
H. They must be achievable
Answer: A,B,G,H (LEAVE A REPLY)
According to ISO/IEC 27001:2022, clause 6.2, information security objectives are the specific results that an organisation intends to achieve with its information security management system (ISMS). The standard specifies that information security objectives must fulfil the following criteria:
* They must be communicated appropriately (A): The organisation must ensure that the relevant internal and external parties are informed about the information security objectives and their roles and responsibilities in achieving them. This can help to create awareness, commitment, and accountability for information security. This criterion is related to clause 6.2.2 of ISO/IEC 27001:2022.
* They must be available as documented information (B): The organisation must maintain and retain documented information on the information security objectives, including their scope, level, indicators, and time frame. This can help to provide evidence, traceability, and consistency for information security. This criterion is related to clause 6.2.1 of ISO/IEC 27001:2022.
* They must be consistent with the IS Policy (G): The organisation must ensure that the information security objectives are aligned with the information security policy, which is the top-level statement of the organisation's intentions and direction for information security. This can help to support the strategic objectives and the context of the organisation. This criterion is related to clause 5.2 of ISO/IEC
27001:2022.

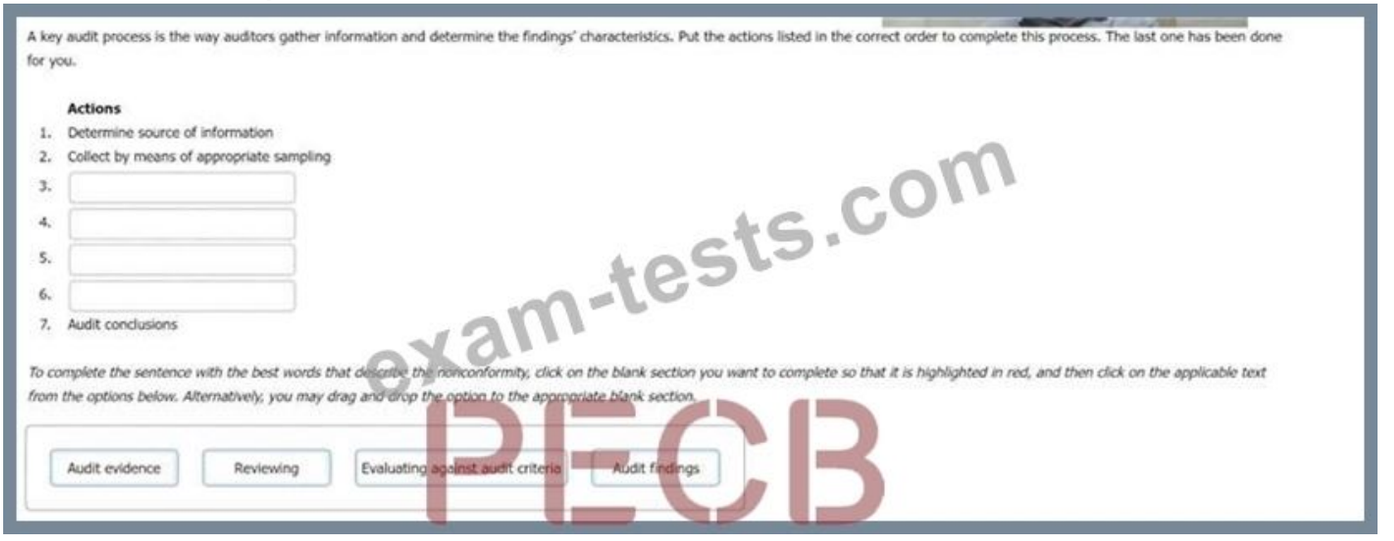
* They must be achievable (H): The organisation must ensure that the information security objectives are realistic and attainable, considering the available resources, capabilities, and constraints. This can help to avoid setting unrealistic or unfeasible expectations and to monitor and measure the progress and performance of information security. This criterion is related to clause 6.2.1 of ISO/IEC 27001:2022.

References:

* ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1
* PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2
* ISO 27001:2022 Lead Auditor - PECB3
* ISO 27001:2022 certified ISMS lead auditor - Jisc4
* ISO/IEC 27001:2022 Lead Auditor Transition Training Course5
* ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6

NEW QUESTION: 119

A key audit process is the way auditors gather information and determine the findings' characteristics. Put the actions listed in the correct order to complete this process. The last one has been done for you.



Answer:

Explanation:
Determine source of information
Collect by means of appropriate sampling
Reviewing
Audit evidence
Evaluating against audit criteria
Audit findings
Audit conclusions
The reviewing step involves checking the accuracy, completeness, and relevance of the collected information.
The audit evidence step involves documenting the information in a verifiable and traceable manner. The evaluating against audit criteria step involves comparing the audit evidence with the requirements of the ISO
27001 standard and the organization's own policies and objectives. The audit findings step involves identifying any nonconformities, weaknesses, or opportunities for improvement in the ISMS. The audit conclusions step involves summarizing the audit results and providing recommendations for corrective actions or enhancements.

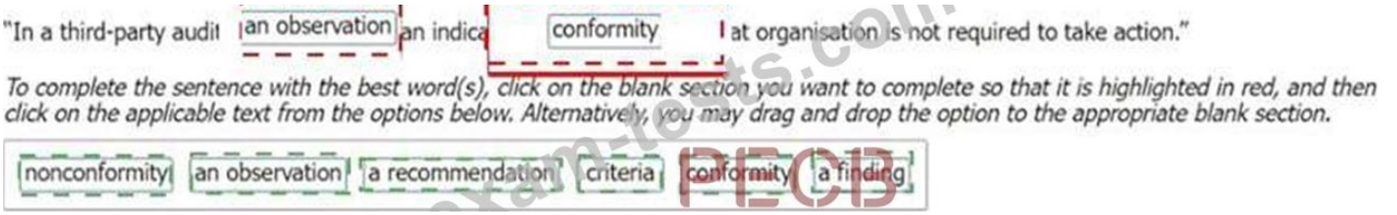
NEW QUESTION: 120
Who are allowed to access highly confidential files?
A. Employees with a business need-to-know
B. Contractors with a business need-to-know
C. Employees with signed NDA have a business need-to-know
D. Non-employees designated with approved access and have signed NDA
Answer: A (LEAVE A REPLY)
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. Reference: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 121

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: 122

You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including misaddressed labels and, in 15% of cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).
You: Are items checked before being dispatched?
SM: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.
You: What action is taken when items are returned?
SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.
You raise a nonconformity against ISO 27001:2022 based on the lack of control of the labelling process.
At the closing meeting, the Shipping Manager issues an apology to you that his comments may have been misunderstood. He says that he did not realise that there is a background IT process that automatically checks that the right label goes onto the right parcel otherwise the parcel is ejected at labelling. He asks that you withdraw your nonconformity.
Select three options of the correct responses that you as the audit team leader would make to the request of the Shipping Manager.
A. Advise the Shipping Manager that his request will be included in the audit report
B. Advise management that the new information provided will be discussed when the auditors have more time
C. Inform the Shipping Manager that the nonconformity is minor and should be quickly corrected
D. Ask the audit team members to state what they think should happen
E. Inform him of your understanding and withdraw the nonconformity
F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed
G. Advise the Shipping Manager that the nonconformity must stand since the evidence obtained for it was dear
H. Indicate that the nonconformity is evidence of a deeper system failure that needs to be rectified
Answer: A,B,F (LEAVE A REPLY)
* A. Advise the Shipping Manager that his request will be included in the audit report. This is true because the audit report should document all the relevant information and evidence related to the audit, including any requests or objections raised by the auditee. The audit report should also provide the rationale for the audit conclusions and recommendations12.
* B. Advise management that the new information provided will be discussed when the auditors have more time. This is true because the auditors should not make hasty decisions based on incomplete or unverified information. The auditors should review and evaluate the new

information in a systematic and objective manner, and determine whether it affects the audit findings, nonconformities, or conclusions12.
* F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed. This is true because the auditors should acknowledge and appreciate the cooperation and transparency of the auditee, but also maintain their professional integrity and independence. The auditors should not withdraw a nonconformity unless they are satisfied that it was raised in error or that it has been effectively corrected and verified12.
References :=
* ISO 19011:2022 Guidelines for auditing management systems
* ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 123
Scenario 5: Data Grid Inc. is a well-known company that delivers security services across the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. For two decades, Data Grid Inc. has helped various companies secure their networks through advanced products and services. Having achieved reputation in the information and network security field, Data Grid Inc. decided to obtain the ISO/IEC 27001 certification to better secure its internal and customer assets and gain competitive advantage.
Data Grid Inc. appointed the audit team, who agreed on the terms of the audit mandate. In addition, Data Grid Inc. defined the audit scope, specified the audit criteria, and proposed to close the audit within five days. The audit team rejected Data Grid Inc.'s proposal to conduct the audit within five days, since the company has a large number of employees and complex processes. Data Grid Inc. insisted that they have planned to complete the audit within five days, so both parties agreed upon conducting the audit within the defined duration. The audit team followed a risk-based auditing approach.
To gain an overview of the main business processes and controls, the audit team accessed process descriptions and organizational charts. They were unable to perform a deeper analysis of the IT risks and controls because their access to the IT infrastructure and applications was restricted. However, the audit team stated that the risk that a significant defect could occur to Data Grid Inc.'s ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by asking the representatives of Data Grid Inc. the following questions:
*How are responsibilities for IT and IT controls defined and assigned?
*How does Data Grid Inc. assess whether the controls have achieved the desired results?
*What controls does Data Grid Inc. have in place to protect the operating environment and data from malicious software?
*Are firewall-related controls implemented?
Data Grid Inc.'s representatives provided sufficient and appropriate evidence to address all these questions.

The audit team leader drafted the audit conclusions and reported them to Data Grid Inc.'s top management.
Though Data Grid Inc. was recommended for certification by the auditors, misunderstandings were raised between Data Grid Inc. and the certification body in regards to audit objectives. Data Grid Inc. stated that even though the audit objectives included the identification of areas for potential improvement, the audit team did not provide such information.
Based on this scenario, answer the following question:
Based on scenario 5, the audit team disagreed with the proposed audit duration by Data Grid Inc. for the ISMS audit. How do you describe such a situation?
A. Acceptable, auditors have the right to object, even refuse the audit mandate, if they deem that the audit duration is not sufficient
B. Unacceptable, the audit duration is defined by the auditee and cannot be changed by the auditors
C. Unacceptable, once the audit mandate is accepted, the audit duration cannot be changed
Answer: (SHOW ANSWER)
Auditors have the authority to object or even refuse an audit mandate if they believe that the audit duration proposed by the auditee is not sufficient to thoroughly assess the ISMS. It is crucial for the audit to be comprehensive enough to cover all necessary aspects of the system, ensuring its effectiveness and compliance.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 124
You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre.
Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.
Select four options for the actions you could take.
A. Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared
B. Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit
C. Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity
D. Note the progress made but hold the audit open until all corrective action has been cleared
E. Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified
F. Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity
G. Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale

H. Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised

Answer: B,E,F,H (LEAVE A REPLY)

Explanation

According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1. The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1.

Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:

* Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame. The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.
* Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.
* Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.
* Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised

by implementing effective corrective actions for most of them and agreeing on a plan for the remaining one. The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

NEW QUESTION: 125
Which one of the following conclusions in the audit report is not required by the certification body when deciding to grant certification?
A. The corrections taken by the organisation related to major nonconformities have been accepted.
B. The organisation fully complies with all legal and other requirements applicable to the Information Security Management System.
C. The plans to address corrective actions related to minor nonconformities have been accepted
D. The scope of certification has been fulfilled
Answer: B (LEAVE A REPLY)
The conclusion in the audit report that is not required by the certification body when deciding to grant certification is that the organisation fully complies with all legal and other requirements applicable to the ISMS. This is because the certification body does not have the authority or the responsibility to verify the legal compliance of the organisation, as this is outside the scope of ISO/IEC 27001:2022. The certification body only evaluates the conformity of the organisation's ISMS with the requirements of the standard, which include the establishment of a process to identify and evaluate the legal and other requirements that are relevant to the ISMS. The organisation is responsible for ensuring its own legal compliance and for providing evidence of such compliance to the certification body if requested. References: = ISO/IEC 27001:2022, clause 6.1.3; ISO/IEC 27006:2022, clause 9.2.2.4; PECB Candidate Handbook ISO 27001 Lead Auditor, page 29.

NEW QUESTION: 126
The following are the guidelines to protect your password, except:
A. Don't use the same password for various company system security access
B. Do not share passwords with anyone
C. For easy recall, use the same password for company and personal accounts
D. Change a temporary password on first log-on
Answer: (SHOW ANSWER)
Explanation
The following are guidelines to protect your password, except for easy recall use the same password for company and personal accounts; do not share passwords with anyone. Using the same password for company and personal accounts is not a guideline to protect your password, as it increases the risk of compromising your password if one of your accounts is hacked or breached. You should use different and unique passwords for each account, and change them regularly. Sharing passwords with anyone is not a guideline to protect your password, as it reduces the security and accountability of your password. You should keep your password

confidential and never disclose it to anyone, even if they claim to be authorized or trustworthy. Don't use the same password for various company system security access is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if one of the systems is compromised or breached.
You should use different and complex passwords for each system, and follow the password policies and standards of the organization. Change a temporary password on first log-on is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if the temporary password is intercepted or leaked. You should change the temporary password to a personal and secure password as soon as possible, and avoid using default or predictable passwords. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 43. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

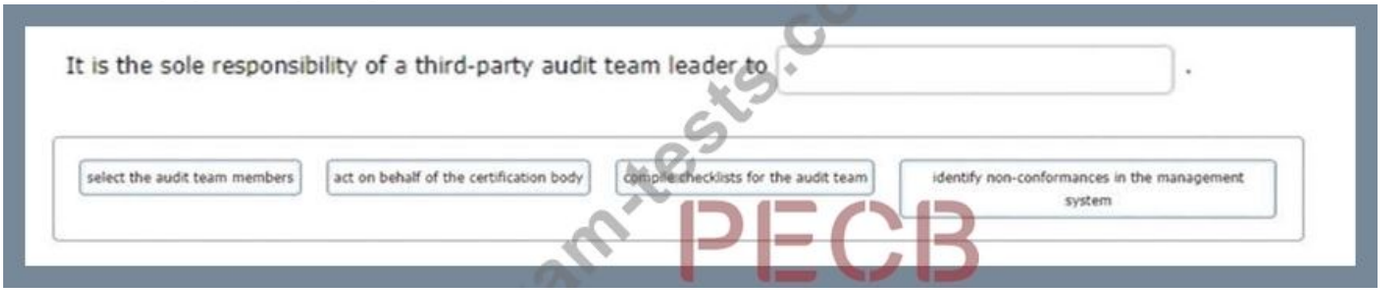
NEW QUESTION: 127
Select the words that best complete the sentence to describe an audit finding.

Answer:

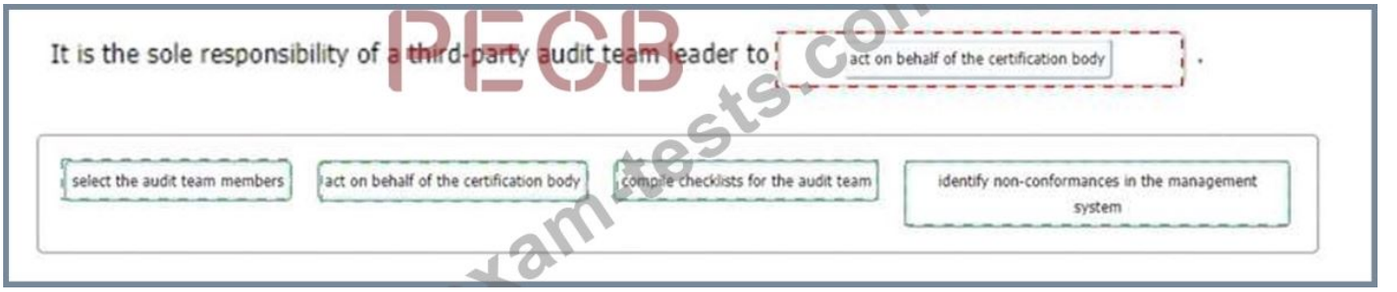
Explanation:
"An audit finding is the result of the evaluation of the collected audit evidence against audit criteria." The words that best complete the sentence to describe an audit finding are evaluation and evidence. According to ISO 19011:2022, an audit finding is the result of the evaluation of 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: 128
Select the words that best complete the sentence:

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



Answer:



Explanation

It is the sole responsibility of a third-party audit team leader to **act on behalf of the certification body** .

* A third-party audit team leader is a person who leads an audit team that conducts audits on behalf of an external organization, such as a certification body, that provides certification or accreditation services to other organizations12.
* One of the main responsibilities of a third-party audit team leader is to act on behalf of the certification body, which means to represent its interests, policies, and procedures during the audit process12.
* Acting on behalf of the certification body involves communicating with the audit client and the auditee, planning and conducting the audit, reporting and evaluating the audit results, and making recommendations for certification or accreditation decisions12.
* Acting on behalf of the certification body also requires maintaining professional integrity, impartiality, confidentiality, and competence throughout the audit process12.

References :=

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

NEW QUESTION: 129

You see a blue color sticker on certain physical assets. What does this signify?

A. The asset is very high critical and its failure affects the entire organization
B. The asset with blue stickers should be kept air conditioned at all times
C. The asset is high critical and its failure will affect a group/s/project's work in the organization
D. The asset is critical and the impact is restricted to an employee only

Answer: C (LEAVE A REPLY)

Explanation

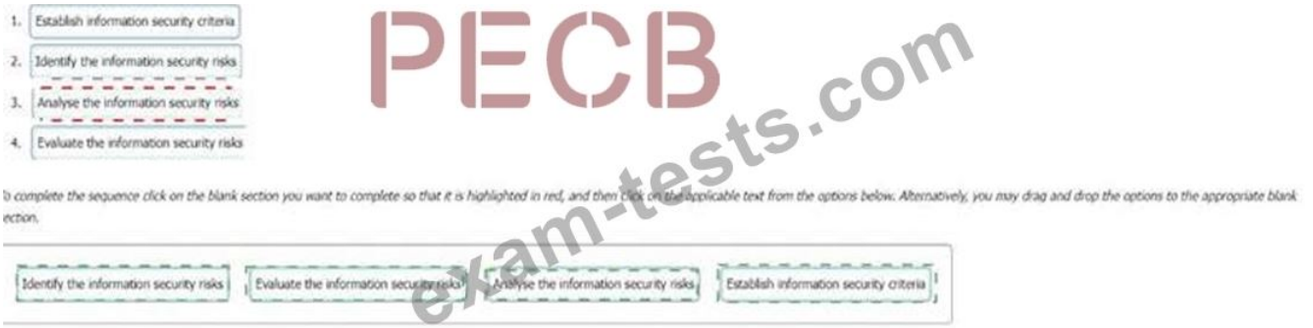
You see a blue color sticker on certain physical assets. This signifies that the asset is high critical and its failure will affect a group/s/project's work in the organization. A blue color sticker is a type of label that indicates the level of criticality of an asset, which is a measure of how important an asset is for the organization's operations and objectives. A high critical asset is an asset that has a significant impact on the organization's activities, and its loss or damage would cause major disruption or loss of service. A blue color sticker also implies that the asset requires a high level of protection and security, and should be handled with care. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36. : [ISO/IEC 27001 Brochures | PECB], page 6.

NEW QUESTION: 130

Select the correct sequence for the information security risk assessment process in an ISMS.

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

Answer:



Explanation:

A group of black text Description automatically generated

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

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

The first step is to establish the information security criteria, which include the risk assessment methodology, the risk acceptance criteria, and the risk evaluation criteria. These criteria define how the organization will perform the risk assessment, what level of risk is acceptable, and how the risks will be compared and prioritized.

The second step is to identify the information security risks, which involve identifying the assets, threats, vulnerabilities, and existing controls that are relevant to the ISMS. The organization should also identify the potential consequences and likelihood of each risk scenario.

The third step is to analyse the information security risks, which involve estimating the level of risk for each risk scenario based on the criteria established in the first step. The organization should also consider the sources of uncertainty and the confidence level of the risk estimation.

The fourth step is to evaluate the information security risks, which involve comparing the estimated risk levels with the risk acceptance criteria and determining whether the risks are acceptable or need treatment. The organization should also prioritize the risks based on the risk evaluation criteria and the objectives of the ISMS.

References: ISO 27001:2022 Clause 6.1.2 Information security risk assessment, ISO 27001 Risk Assessment
& Risk Treatment: The Complete Guide - Advisera, ISO 27001 Risk Assessment: 7 Step Guide - IT Governance UK Blog

NEW QUESTION: 131

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: A (LEAVE A REPLY)
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.

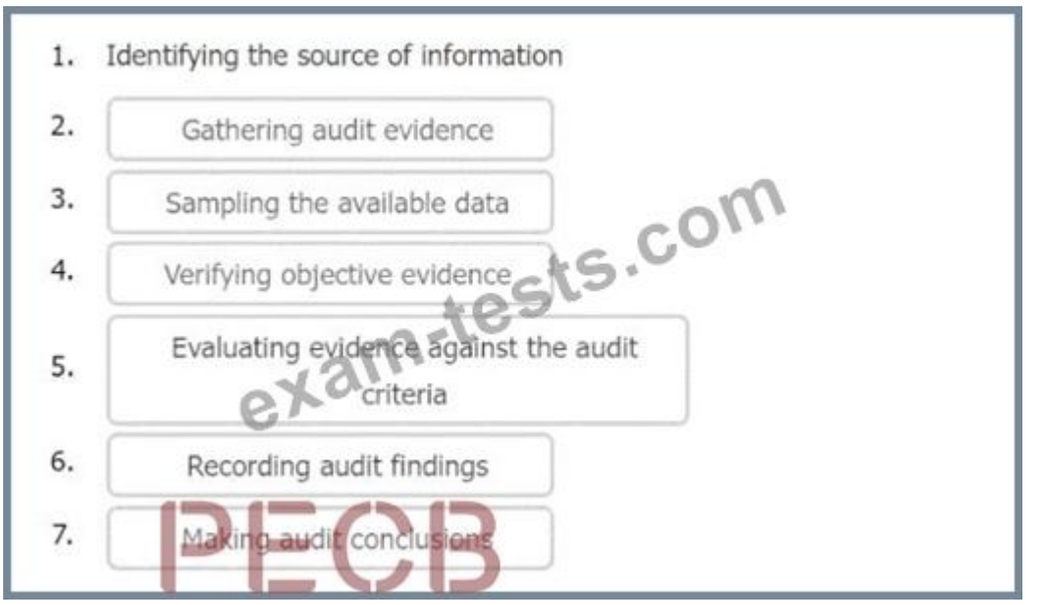
NEW QUESTION: 132
Which one option best describes the purpose of retaining documented information related to the Information Security Management System (ISMS) of an organisation?
A. To ensure that all workers will follow the established procedure.

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

NEW QUESTION: 133
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:

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:

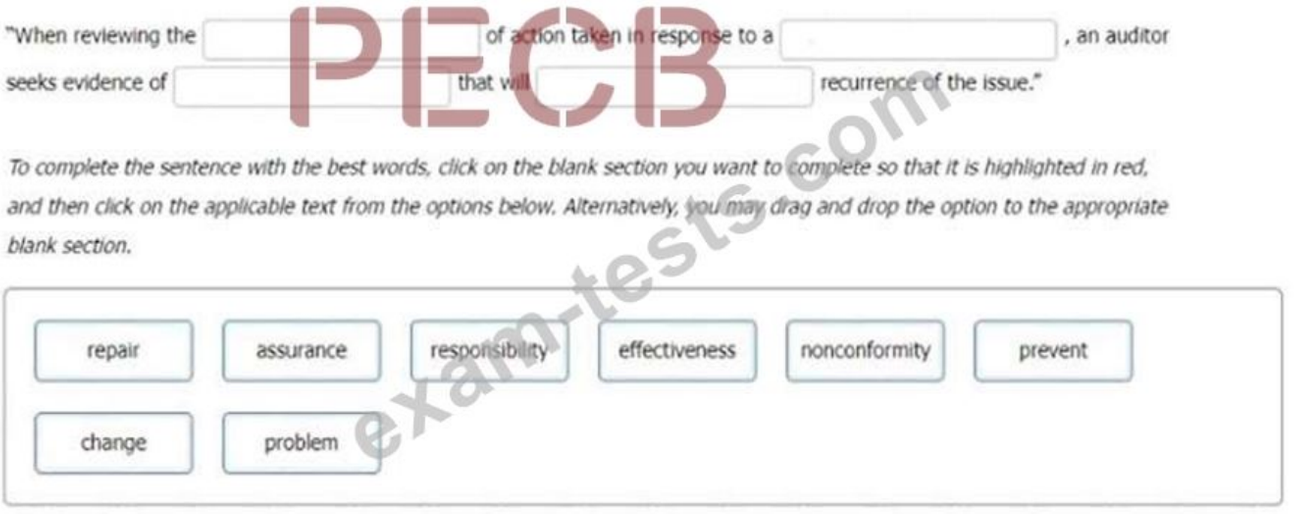
1. Identifying the source of information 2. Gathering audit evidence 3. Sampling the available data 4.
Verifying objective evidence 5. Evaluating evidence against the audit criteria 6. Recording audit findings 7.
Making audit conclusions

NEW QUESTION: 134

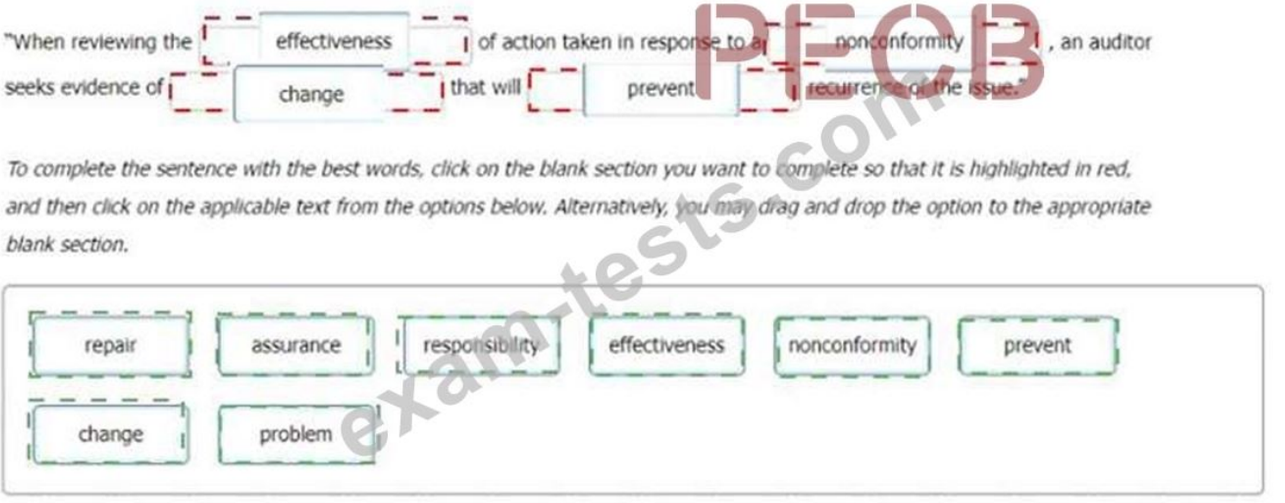
You are performing an ISMS audit at a European-based residential nursing home called ABC that provides healthcare services. The next step in your audit plan is to verify the effectiveness of the continual improvement process.

During the audit, you learned most of the residents' family members (90%) receive WeCare medical devices promotion advertisements through email and SMS once a week via ABC's healthcare mobile app. All of them do not agree on the use of the collected personal data for

marketing or any other purposes than nursing and medical care on the signed service agreement with ABC. They have very strong reason to believe that ABC is leaking residents' and family members' personal information to a non-relevant third party and they have filed complaints.
The Service Manager says that, after investigation, all these complaints have been treated as nonconformities.
The corrective actions have been planned and implemented according to the nonconformity and corrective management procedure (Document reference ID: ISMS_L2_10.1, version 1).
You write a nonconformity which you will follow up on later. Select the words that best complete the sentence:



Answer:



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

continual improvement is to identify and correct nonconformities and take actions to eliminate their causes and prevent their recurrence.
Therefore, when reviewing the effectiveness of the corrective actions, an auditor should look for evidence that the organization has analyzed the root cause of the nonconformity, implemented appropriate changes to the ISMS, and verified that the changes have resulted in the desired improvement and prevented the recurrence of the issue. References: =
* ISO/IEC 27001:2022, clause 10.1, Nonconformity and corrective action
* ISO/IEC 27001:2022, clause 10.2, Continual improvement
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION: 135
CEO sends a mail giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it. The mail should be classified as
A. Internal Mail
B. Public Mail
C. Confidential Mail
D. Restricted Mail
Answer: A (LEAVE A REPLY)
The mail sent by the CEO giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it should be classified as internal mail. Internal mail is a type of classification that indicates that the information is intended for internal use only, and should not be disclosed to external parties without authorization. The mail sent by the CEO contains information that is relevant and important for the employees of the company, but may not be suitable for public disclosure, as it may contain sensitive or confidential information about the company's performance, goals, or plans. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 37. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 14.

NEW QUESTION: 136
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: C,D,E,G (LEAVE A REPLY)

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: 137
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: (SHOW ANSWER)
Explanation
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). 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 Indirect Damage?]

NEW QUESTION: 138
What type of legislation requires a proper controlled purchase process?
A. Personal data protection act
B. Computer criminality act
C. Government information act
D. Intellectual property rights act
Answer: (SHOW ANSWER)
An intellectual property rights act is a type of legislation that requires a proper controlled purchase process. Intellectual property rights are legal rights that protect creations of the mind, such as inventions, literary and artistic works, designs, symbols, names and images. Intellectual property rights can include patents, trademarks, copyrights, trade secrets, etc. A proper controlled purchase process is a process that ensures that the organization obtains valid licenses or permissions from the owners or authorized parties of the intellectual property rights before using or acquiring any intellectual property assets. This process helps to avoid infringing on the intellectual property rights of others, which may result in legal actions, fines, damages or reputational harm. ISO/IEC 27001:2022 requires the organization to comply with relevant legal and contractual obligations related to intellectual property rights (see clause A.18.1.4). 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 Intellectual Property?

NEW QUESTION: 139
Which two of the following phrases are 'objectives' in relation to a first-party audit?
A. Apply international standards
B. Prepare the audit report for the certification body
C. Confirm the scope of the management system is accurate
D. Complete the audit on time
E. Apply Regulatory requirements
F. Update the management policy
Answer: C,F (LEAVE A REPLY)
Explanation
A first-party audit is an internal audit conducted by the organization itself or by an external party on its behalf. The objectives of a first-party audit are to: 12
* Confirm the scope of the management system is accurate, i.e., it covers all the processes, activities, locations, and functions that are relevant to the information security objectives and requirements of the organization.

* Update the management policy, i.e., review and revise the policy statement, roles and responsibilities, and objectives and targets of the information security management system (ISMS) based on the audit findings and feedback.
The other phrases are not objectives of a first-party audit, but rather:
* Apply international standards: This is a requirement for the ISMS, not an objective of the audit. The ISMS must conform to the ISO/IEC 27001 standard and any other applicable standards or regulations12
* Prepare the audit report for the certification body: This is an activity of a third-party audit, not a first-party audit. A third-party audit is an external audit conducted by an independent certification body
* to verify the conformity and effectiveness of the ISMS and to issue a certificate of compliance12
* Complete the audit on time: This is a performance indicator, not an objective of the audit. The audit should be completed within the planned time frame and budget, but this is not the primary purpose of the audit12
* Apply regulatory requirements: This is also a requirement for the ISMS, not an objective of the audit. The ISMS must comply with the legal and contractual obligations of the organization regarding information security12 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: 140
Which two of the following phrases are 'objectives' in relation to a first-party audit?
A. Apply international standards
B. Prepare the audit report for the certification body
C. Confirm the scope of the management system is accurate
D. Complete the audit on time
E. Apply Regulatory requirements
F. Update the management policy
Answer: (SHOW ANSWER)
A first-party audit is an internal audit conducted by the organization itself or by an external party on its behalf. The objectives of a first-party audit are to: 12 Confirm the scope of the management system is accurate, i.e., it covers all the processes, activities, locations, and functions that are relevant to the information security objectives and requirements of the organization.
Update the management policy, i.e., review and revise the policy statement, roles and responsibilities, and objectives and targets of the information security management system (ISMS) based on the audit findings and feedback.
The other phrases are not objectives of a first-party audit, but rather:
Apply international standards: This is a requirement for the ISMS, not an objective of the audit. The ISMS must conform to the ISO/IEC 27001 standard and any other applicable standards or regulations12 Prepare the audit report for the certification body: This is an activity of a third-party audit, not a first-party audit. A third-party audit is an external audit conducted by an independent

certification body to verify the conformity and effectiveness of the ISMS and to issue a certificate of compliance12 Complete the audit on time: This is a performance indicator, not an objective of the audit. The audit should be completed within the planned time frame and budget, but this is not the primary purpose of the audit12 Apply regulatory requirements: This is also a requirement for the ISMS, not an objective of the audit. The ISMS must comply with the legal and contractual obligations of the organization regarding information security12 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: 141
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: 142
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.
You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that he electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.
To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.
Select four options for the clauses and/or controls of ISO/IEC 27001:2022 that are directly relevant to the verification of the scope of the ISMS.
A. Control 5.3 Organizational roles, responsibilites and authorities
B. Clause 4.2 Understanding the needs and expectations of interested parties
C. Control 5.3 Legal, statutory, regulatory and contractual requirements
D. Control 6.3 Information security awareness, education, and training
E. Clause 5.2 Policy
F. Clause 4.1 Understanding the organization and its context
G. Control 7.6 Working in secure areas
H. Clause 4.3 Determining the scope of the information security management system

Answer: B,E,F,H (LEAVE A REPLY)

* B. This clause requires the organisation to determine the interested parties that are relevant to the ISMS, and the requirements of these interested parties12. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to identify the stakeholders that have an influence or an interest in the information security of the organisation, such as customers, suppliers, regulators, employees, etc. The organisation should also consider the needs and expectations of these interested parties when defining the scope of the ISMS, and ensure that they are met and communicated.
* E. This clause requires the organisation to establish an information security policy that provides the framework for setting the information security objectives and guiding the information security activities13. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to define the direction and principles of the ISMS, and to align them with the strategic
* goals and context of the organisation. The information security policy should also be consistent with the scope of the ISMS, and should be communicated and understood within the organisation and by relevant interested parties.
* F. This clause requires the organisation to determine the internal and external issues that are relevant to the purpose and the context of the organisation, and that affect its ability to achieve the intended outcomes of the ISMS14. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to understand the factors and conditions that influence the information security of the organisation, such as the legal, technological, social, economic, environmental, etc. The organisation should also monitor and review these issues, and consider them when defining the scope of the ISMS.
* H. This clause requires the organisation to determine the boundaries and applicability of the ISMS to establish its scope15. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to describe the information and processes that are included in the ISMS, and to document the scope in a clear and concise manner. The organisation should also consider the issues, requirements, and interfaces identified in clauses 4.1, 4.2, and 4.3 when determining the scope of the ISMS, and ensure that the scope is appropriate to the nature and scale of the organisation.

References:

1: PECB Candidate Handbook - ISO 27001 Lead Auditor, page 17 2: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause
4.2 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 5.2 4: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.1 5: ISO/IEC
27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.3

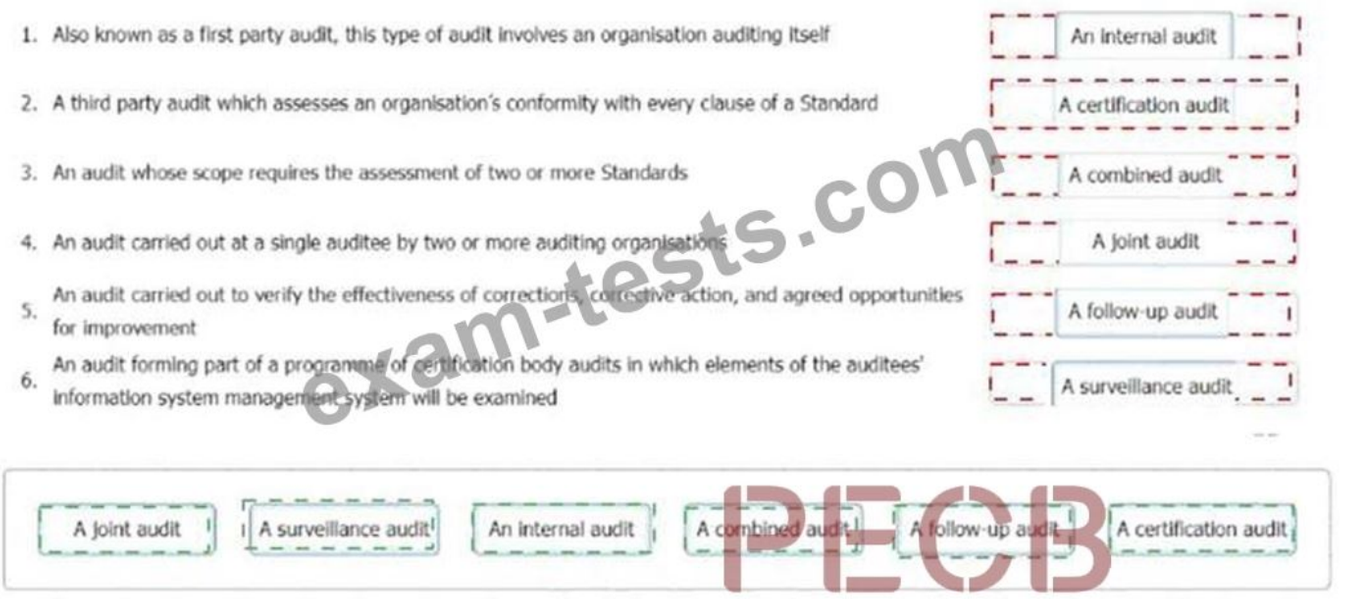
NEW QUESTION: 143

You are an experienced ISMS audit team leader. An auditor in training has approached you to ask you to clarify the different types of audits she may be required to undertake.

Match the following audit types to the descriptions.

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

Answer:



1.	Also known as a first party audit, this type of audit involves an organisation auditing itself	An internal audit
2.	A third party audit which assesses an organisation's conformity with every clause of a Standard	A certification audit
3.	An audit whose scope requires the assessment of two or more Standards	A combined audit
4.	An audit carried out at a single auditee by two or more auditing organisations	A joint audit
5.	An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement	A follow-up audit
6.	An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined	A surveillance audit

NEW QUESTION: 144

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.

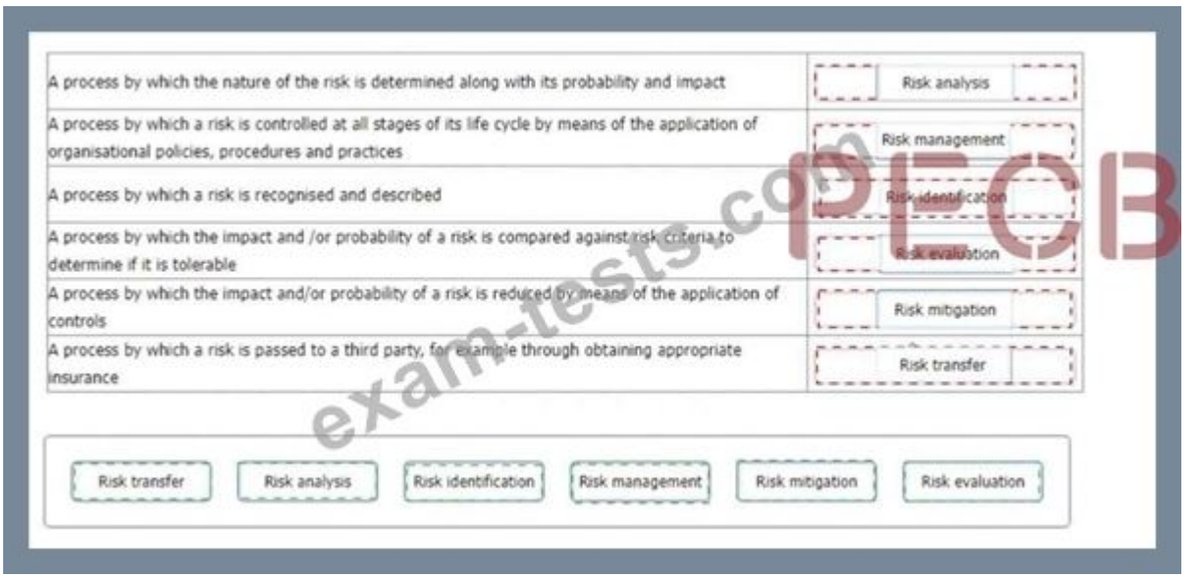
Match each of the descriptions provided to one of the following risk management processes.

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.

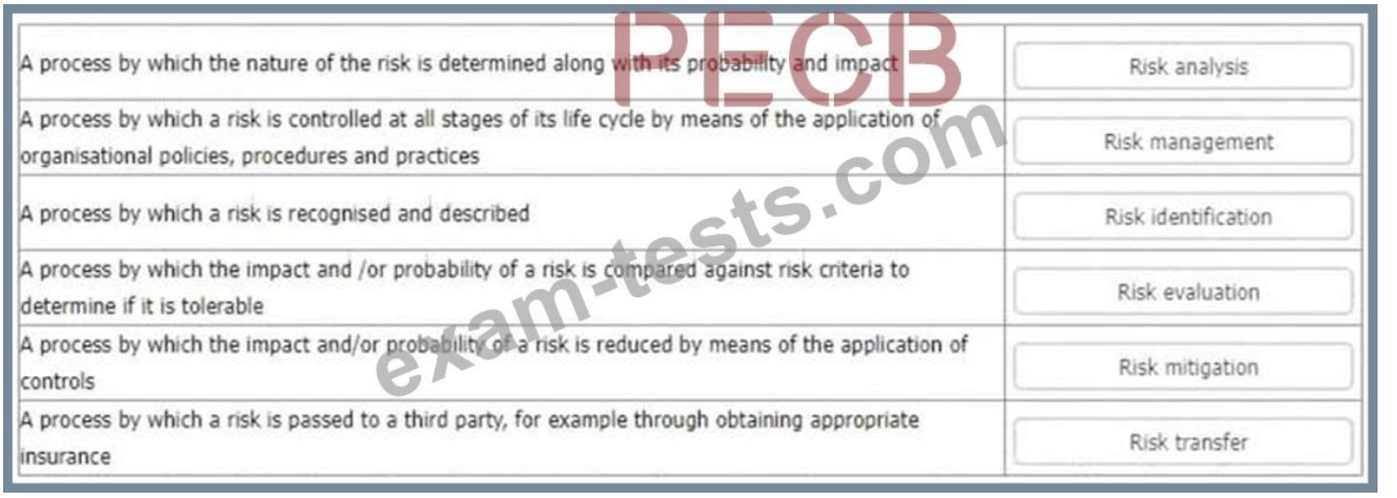
A process by which the nature of the risk is determined along with its probability and impact	
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	
A process by which a risk is recognised and described	
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:



Explanation:



* 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: 145
You are a certification body auditor, conducting a surveillance audit to ISO/IEC 27001:2022 of a data centre operated by a client who provides hosting services for ICT facilities.
You and your guide are currently in one of the private suites that the client rents out to customers. Access to each suite is controlled using a combination lock. CCTV is also installed in every suite. Within each suite are three data cabinets in which the client can locate mission-critical servers and other items of networking equipment such as switches and routers.
You notice that whilst two of the cabinets in your suite are locked, the third is unlocked. You ask the guide why. They reply "This is because the client is currently swapping out a hard drive unit. Their technician is currently on a lunch break".
What three actions should you undertake next?
A. Do nothing, the room appears adequately protected so it is unlikely that a security incident has taken place.
B. Raise a nonconformity against control 5.16 'identity management' as it may not be possible to identify who left the cabinet unlocked.
C. Raise a nonconformity against control 7.2 'physical entry' as the area where the client's equipment is located is not protected.

D. Raise a nonconformity against control 7.4 'physical security monitoring' as the private suite is not being continuously monitored for unauthorised physical access.
E. Raise an opportunity for improvement suggesting cabinet doors are locked whenever clients leave their suites, even if they intend to return within a short time.
F. Review the CCTV records to ensure that only the client has accessed the cabinet since it was last confirmed as locked.
G. When the technician returns from lunch, reprimand them for leaving the cabinet open.
H. With the permission of the guide, speak to the customer to confirm that they are in the process of swapping out a drive.
Answer: (SHOW ANSWER)
Leaving the cabinet unlocked while the technician is on a lunch break exposes the client's equipment and data to potential physical security risks, such as theft, damage, or tampering. This is a violation of the ISO/IEC
27001:2022 requirements for physical entry (control 7.2) and physical security monitoring (control 7.4), which aim to prevent unauthorized access to information processing facilities and assets.
Therefore, the appropriate actions for the auditor are:
* Raise an opportunity for improvement (OFI) suggesting that the cabinet doors are locked whenever clients leave their suites, even if they intend to return within a short time. This would enhance the security of the client's equipment and data, and reduce the likelihood of security incidents.
* Review the CCTV records to ensure that only the client has accessed the cabinet since it was last confirmed as locked. This would verify the integrity and availability of the client's equipment and data, and identify any possible unauthorized access or interference.
* With the permission of the guide, speak to the customer to confirm that they are in the process of swapping out a drive. This would validate the reason for leaving the cabinet unlocked, and assess the impact and risk of the activity on the client's information security.
References: =
* ISO/IEC 27001:2022, clause 7.2, Physical entry
* ISO/IEC 27001:2022, clause 7.4, Physical security monitoring
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION: 146
In the context of a third-party certification audit, confidentiality is an issue in an audit programme. Select two options which correctly state the function of confidentiality in an audit
A. Auditors are forced by regulatory requirements to maintain confidentiality in an audit
B. Observers in an audit team cannot access any confidential information
C. Confidentiality is one of the principles of audit conduct
D. Auditors should obtain the auditee's permission before using a camera or recording equipment
E. Audit information can be used for improving personal competence by the auditor

F. As an auditor is always accompanied by a guide, there is no risk to the auditee's sensitive information

Answer: C,D (LEAVE A REPLY)

Confidentiality is one of the principles of audit conduct that auditors should adhere to when performing audits. Confidentiality means that auditors should exercise discretion in the use and protection of information acquired in the course of their duties3. Auditors should respect the intellectual property rights of the auditee and other parties involved in the audit, and should not disclose any information that is sensitive, proprietary, or confidential without prior approval from the auditee or other authorized parties3. Auditors should also obtain the auditee's permission before using a camera or recording equipment during an audit, as these devices may capture confidential information or infringe on the privacy of individuals3. Therefore, these two options correctly state the function of confidentiality in an audit. The other options are either incorrect or irrelevant to confidentiality. For example, auditors are not forced by regulatory requirements to maintain confidentiality in an audit, but rather by ethical obligations and contractual agreements3. Observers in an audit team can access confidential information if they have signed a confidentiality agreement and have been authorized by the auditee3. Audit information can be used for improving personal competence by the auditor only if it does not compromise confidentiality or conflict with other interests3. As an auditor is always accompanied by a guide, there is still a risk to the auditee's sensitive information if the guide is not trustworthy or authorized to access such information3. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 147

You are performing an ISMS audit at a residential nursing home that provides healthcare services and are reviewing the Software Code Management (SCM) system. You found a total of 10 user accounts on the SCM.

You confirm that one of the users, Scott, resigned 9-months

ago. The SCM System Administrator confirmed Scott's last check-out of the source code was found 1 month ago. He was using one of the uthorized desktops from the local network in a secure area.

You check with the user de-registration procedure which states "Managers have to make sure of deregistration of the user account and authorisation immediately from the relevant ICT system and/or equipment after resignation approval." There was no deregistration record for user Scott.

The IT Security Manager explains that Scott still comes back to the office every month after he resigned to provide support on source code maintenance. That's why his account on SCM still exists.

You would like to investigate other areas further to collect more audit evidence. Select three options that would not be valid audit trails.

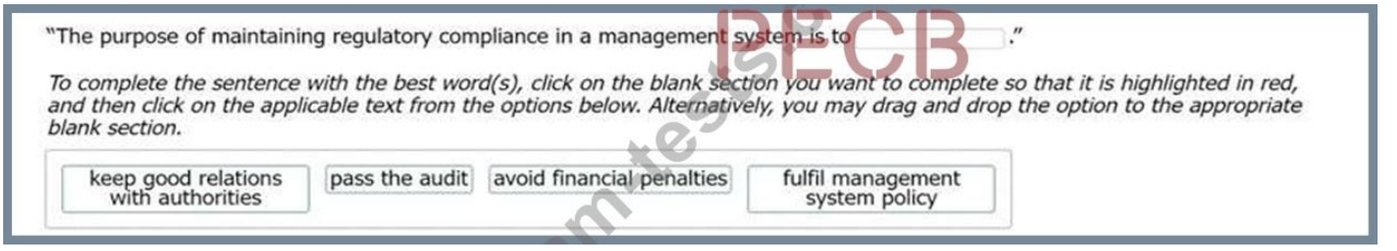
A. Collect more evidence on how access controls are periodically reviewed to maintain security (Relevant to control A.5.35)

B. Collect more evidence on how the transition of Scott from full-time to part-time employment was managed (relevant to control A.6.5)
C. Collect more evidence from Scott's background verification checks performed by the human resource department under the new employment relationship. (Relevant to control A.6.1)
D. Collect more evidence of why Scott resigned and whether his re-engagement represents a conflict of interest. (relevant to control A.5.3)
E. Collect more evidence on how Scott can access the employee's desktop and local network. (Relevant to control A.5.15)
F. Collect more evidence on how Scott can access the secure area. (Relevant to control A.8.4)
G. Collect more evidence on how the organization pays for Scott's source code maintenance support service. (Relevant to control A.6.2)
H. Collect more evidence on where Scott kept the source code that he checked out and how it was secured.
(Relevant to control A.8.4)
Answer: (SHOW ANSWER)
The options B, D, and G are not valid audit trails because they are not directly related to the ISMS requirements or the audit criteria. They are more relevant to the human resource management or the contractual arrangements of the organization, which are outside the scope of the ISMS audit. The other options are valid audit trails because they can provide evidence of how the organization implements and maintains the ISMS controls related to access control, secure areas, and information security aspects of business continuity management. References:
* PECB Candidate Handbook ISO/IEC 27001 Lead Auditor, page 16, section 4.2.1
* ISO/IEC 27001:2013, clauses A.5.3, A.5.15, A.5.35, A.6.1, A.6.2, A.6.5, A.8.4, A.17.1
* ISO 19011:2018, clause 6.2.2

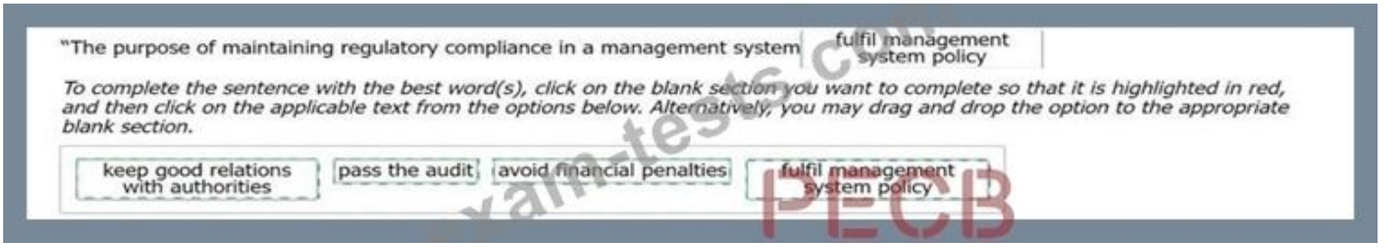
NEW QUESTION: 148
What controls can you do to protect sensitive data in your computer when you go out for lunch?
A. You activate your favorite screen-saver
B. You are confident to leave your computer screen as is since a password protected screensaver is installed and it is set to activate after 10 minutes of inactivity
C. You lock your computer by pressing Windows+L or CTRL-ALT-DELETE and then click "Lock Computer".
D. You turn off the monitor
Answer: C (LEAVE A REPLY)
Explanation
You should lock your computer by pressing Windows+L or CTRL-ALT-DELETE and then click "Lock Computer", because this is the most effective way to protect sensitive data in your computer when you go out for lunch. By locking your computer, you are preventing unauthorized access to your computer and its contents, as well as complying with the organization's access control policy and information security policy.

Locking your computer requires a password or a biometric authentication to unlock it, which adds a layer of security to your data. The other options are not sufficient or reliable, as they do not prevent someone from accessing your computer or viewing your screen. 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, How to lock your PC

NEW QUESTION: 149
Select the words that best complete the sentence:
"The purpose of maintaining regulatory compliance in a management system is to 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
According to ISO 27001:2013, clause 5.2, the top management of an organization must establish, implement and maintain an information security policy that is appropriate to the purpose of the organization and provides a framework for setting information security objectives. The information security policy must also include a commitment to comply with the applicable legal, regulatory and contractual requirements, as well as any other requirements that the organization subscribes to. Therefore, maintaining regulatory compliance is part of fulfilling the management system policy and ensuring its effectiveness and suitability. References:
ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 5.2 PECB Candidate Handbook ISO 27001 Lead Auditor, page 10 ISO 27001 Policy: How to write it according to ISO 27001

NEW QUESTION: 150
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

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

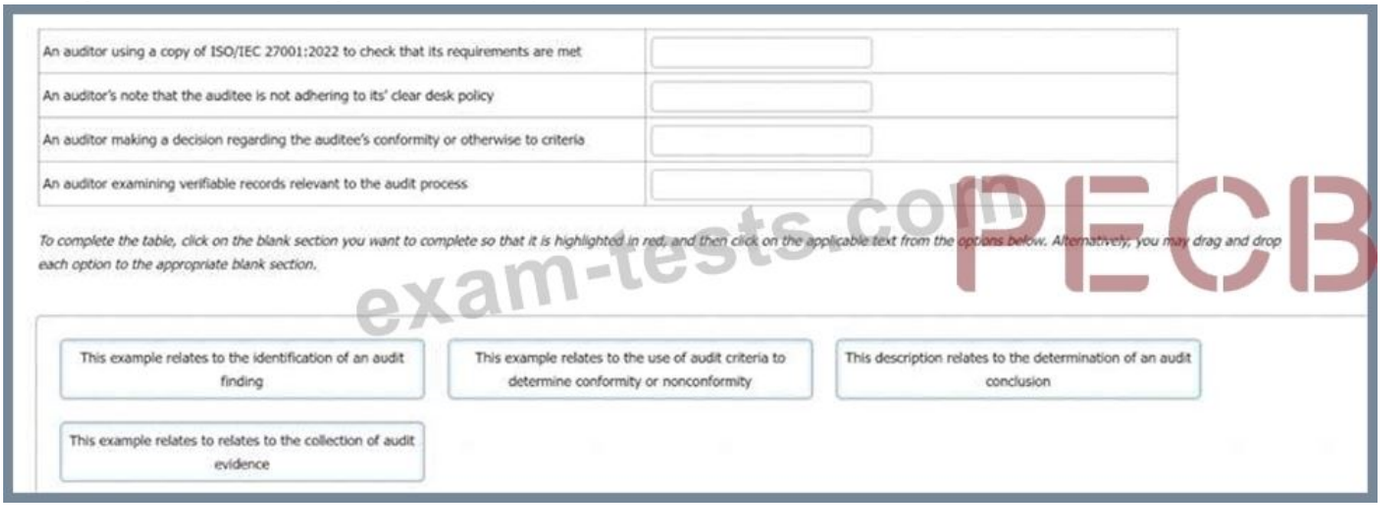
Explanation

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

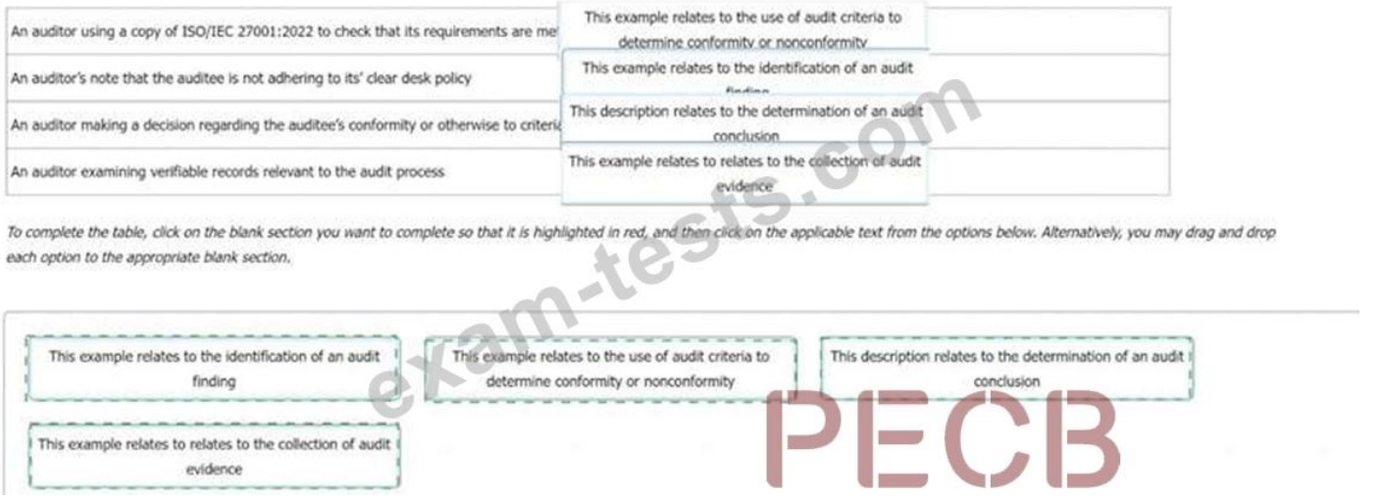
* Risk analysis is the process by which the nature of the risk is determined along with its probability and impact. Risk analysis involves estimating the likelihood and consequences of potential events or situations that could affect the organization's information security objectives or requirements12. 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: 151
You are an experienced ISMS audit team leader, assisting an auditor in training to write their first audit report.
You want to check the auditor in training's understanding of terminology relating to the contents of an audit report and chose to do this by presenting the following examples.
For each example, you ask the auditor in training what the correct term is that describes the activity Match the activity to the description.

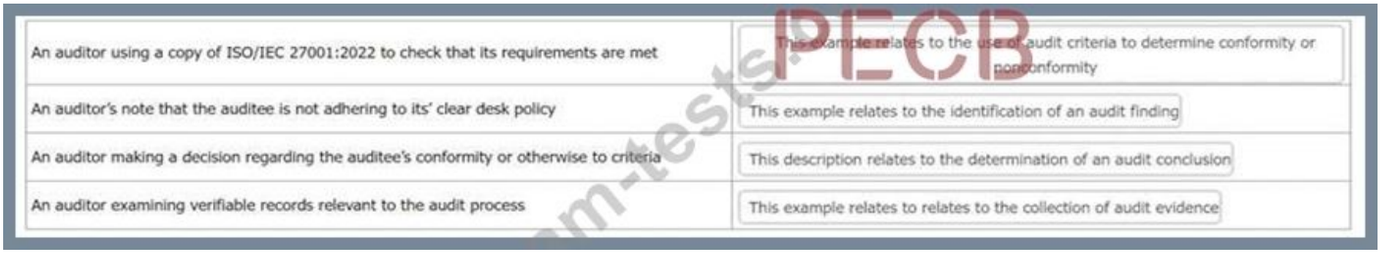


Answer:



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

Justification: The auditor is comparing the auditee's information security management system (ISMS) against the established criteria outlined in the ISO/IEC 27001:2022 standard. This activity falls under the use of audit criteria to determine conformity or nonconformity.
2. An auditor's note that the auditee is not adhering to its clear desk policy:
Termed: Identifying an audit finding.
Justification: The auditor has observed a deviation from the auditee's established policy on clear desks. This observation is documented as a potential nonconformity, which requires further investigation and evaluation.
3. An auditor making a decision regarding the auditee's conformity or otherwise to criteria:
Termed: Determining an audit conclusion.
Justification: Based on the collected audit evidence and evaluation against the established criteria, the auditor forms an opinion about the overall compliance of the auditee's ISMS. This opinion is the audit conclusion and is a key element of the audit report.
4. An auditor examining verifiable records relevant to the audit process:
Termed: Collecting audit evidence.
Justification: The auditor is gathering objective and verifiable information to support their findings and conclusions. This information comes from various sources, including documents, records, interviews, and observations.



NEW QUESTION: 152
Objectives, criteria, and scope are critical features of a third-party ISMS audit. Which two issues are audit objectives?
A. Evaluate customer processes and functions
B. Assess conformity with ISO/IEC 27001 requirements
C. Fulfil the audit plan
D. Confirm sites operating the ISMS

E. Determine the scope of the ISMS
F. Review organisation efficiency
Answer: B,D (LEAVE A REPLY)
Explanation
Audit objectives are the specific purposes or goals that the customer or the certification body wants to achieve through the audit. They define what the audit intends to accomplish and provide the basis for planning and conducting the audit. Audit objectives may vary depending on the type, scope, and criteria of the audit, but they should be clear, measurable, and achievable.
Some examples of audit objectives for a third-party ISMS audit are:
* Assess conformity with ISO/IEC 27001 requirements: This objective means that the audit aims to verify that the organisation's ISMS meets the requirements of the ISO/IEC 27001 standard, which specifies the best practices for establishing, implementing, maintaining, and improving an information security management system. The audit will evaluate the organisation's ISMS documentation, processes, controls, and performance against the standard's clauses and annex A controls.
* Confirm sites operating the ISMS: This objective means that the audit aims to confirm that the organisation's ISMS covers all the relevant sites or locations where the organisation operates or provides its services. The audit will verify that the scope of the ISMS is accurate and consistent with the organisation's context, objectives, and risks.
The other phrases are not audit objectives, but rather:
* Evaluate customer processes and functions: This is not an audit objective, but rather a possible audit criterion or a requirement that the organisation's processes and functions should meet. The audit criterion is the reference against which the audit evidence is compared to determine conformity or nonconformity. The audit criterion may include ISO/IEC 27001 requirements, customer requirements, or other applicable standards or regulations.
* Fulfil the audit plan: This is not an audit objective, but rather a task or an activity that the auditor performs during the audit. The audit plan is a document that describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. The auditor should follow and fulfil the audit plan to ensure that the audit is conducted effectively and efficiently.
* Determine the scope of the ISMS: This is not an audit objective, but rather a prerequisite or an input for conducting the audit. The scope of the ISMS is the extent and boundaries of the information security management system within the organisation. It defines what processes, activities, locations, assets, and stakeholders are included or excluded from the ISMS. The scope of the ISMS should be determined by the organisation before applying for certification or undergoing an audit.
* Review organisation efficiency: This is not an audit objective, but rather a possible outcome or a result of conducting an audit. The organisation efficiency is a measure of how well the organisation uses its

* resources to achieve its goals and objectives. The audit may help review and improve the organisation efficiency by identifying strengths, weaknesses, opportunities, and threats in its information security management system.
References:
* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB
* ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION: 153
What type of compliancy standard, regulation or legislation provides a code of practice for information security?
A. ISO/IEC 27002
B. Personal data protection act
C. Computer criminality act
D. IT Service Management
Answer: A (LEAVE A REPLY)
ISO/IEC 27002:2022 is an international standard that provides a code of practice for information security controls4. A code of practice is a set of guidelines and recommendations for implementing, maintaining, and improving information security in an organization5. ISO/IEC 27002:2022 covers various aspects of information security, such as organizational, human, technical, physical, and environmental controls. It is designed to be used as a reference for selecting, implementing, and managing controls within the process of establishing an ISMS based on ISO/IEC 27001:20224. Reference: ISO/IEC 27002:2022, Foreword and Introduction; ISO/IEC 27000:2022, clause 3.10.

NEW QUESTION: 154
A key audit process is the way auditors gather information and determine the findings' characteristics. Put the actions listed in the correct order to complete this process. The last one has been done for you.

Answer:

Explanation

* Determine source of information
* Collect by means of appropriate sampling
* Reviewing
* Audit evidence
* Evaluating against audit criteria
* Audit findings
* Audit conclusions

The reviewing step involves checking the accuracy, completeness, and relevance of the collected information.

The audit evidence step involves documenting the information in a verifiable and traceable manner. The evaluating against audit criteria step involves comparing the audit evidence with the requirements of the ISO

27001 standard and the organization's own policies and objectives. The audit findings step involves identifying any nonconformities, weaknesses, or opportunities for improvement in the ISMS. The audit conclusions step involves summarizing the audit results and providing recommendations for corrective actions or enhancements.

NEW QUESTION: 155

Which one of the following options is the definition of an interested party?

A. A third party can appeal to an organisation when it perceives itself to be affected by a decision or activity

B. A person or organisation that can affect, be affected by or perceive itself to be affected by a decision or activity

C. A group or organisation that can interfere in or perceive itself to be interfered with by a management decision

D. 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)

Explanation

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

NEW QUESTION: 156

----------is an asset like other important business assets has value to an organization and consequently needs to be protected.

A. Security

B. Infrastructure

C. Information

D. Data

Answer: C (LEAVE A REPLY)

NEW QUESTION: 157

The following are the guidelines to protect your password, except:

A. Don't use the same password for various company system security access

B. Do not share passwords with anyone

C. For easy recall, use the same password for company and personal accounts

D. Change a temporary password on first log-on

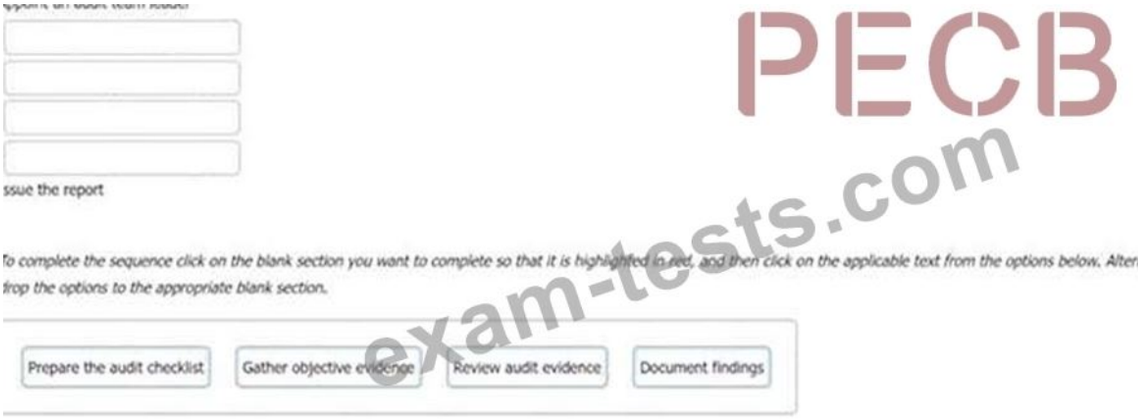
Answer: B,C (LEAVE A REPLY)

The following are guidelines to protect your password, except for easy recall use the same password for company and personal accounts; do not share passwords with anyone. Using the same password for company and personal accounts is not a guideline to protect your password, as it increases the risk of compromising your password if one of your accounts is hacked or breached. You should use different and unique passwords for each account, and change them regularly. Sharing passwords with anyone is not a guideline to protect your password, as it reduces the security and accountability of your password. You should keep your password confidential and never disclose it to anyone, even if they claim to be authorized or trustworthy. Don't use the same password for various company system security access is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if one of the systems is compromised or breached.

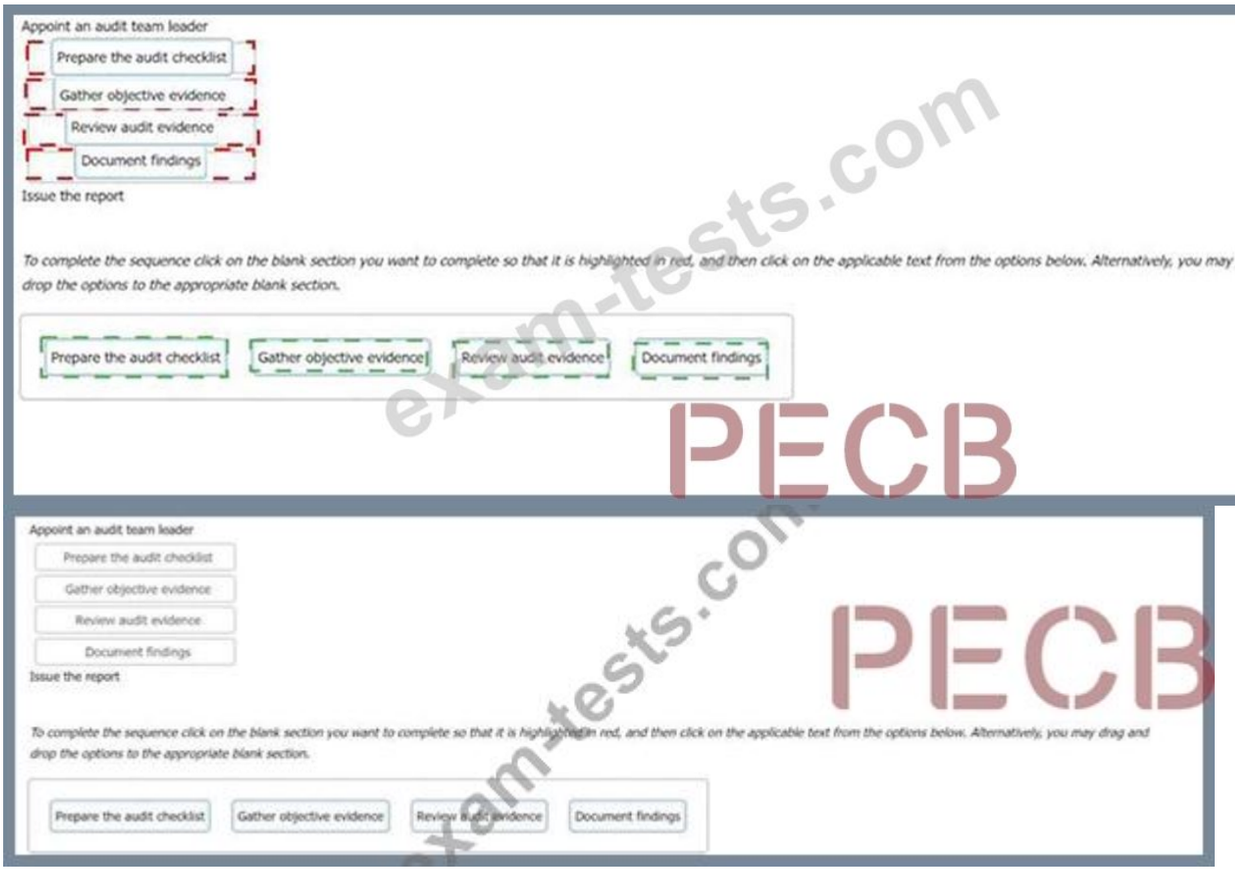
You should use different and complex passwords for each system, and follow the password policies and standards of the organization. Change a temporary password on first log-on is a guideline to protect your password, as it prevents unauthorized access or misuse of your password if the temporary password is intercepted or leaked. You should change the temporary password to a personal and secure password as soon as possible, and avoid using default or predictable passwords. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 43. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

NEW QUESTION: 158
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.
References:
* 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: 159
The following options are key actions involved in a first-party audit. Order the stages to show the sequence in which the actions should take place.



Answer:



NEW QUESTION: 160

Who is authorized to change the classification of a document?

A. The author of the document

B. The administrator of the document

C. The owner of the document

D. The manager of the owner of the document

Answer: C (LEAVE A REPLY)

Explanation

The owner of the document is authorized to change the classification of the document. The owner of the document is the person who has the ultimate responsibility for the creation, maintenance,

and protection of the document. The author of the document is not necessarily the owner of the document, as they may create the document on behalf of someone else. The administrator of the document is not authorized to change the classification of the document, as they only provide technical support for managing and storing documents.
The manager of the owner of the document is not authorized to change the classification of the document, unless they are delegated by the owner or have a higher authority in the organization.
References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 37. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 38. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page
39. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 40. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 41.

NEW QUESTION: 161
CMM stands for?
A. Capability Maturity Matrix
B. Capacity Maturity Matrix
C. Capability Maturity Model
D. Capable Mature Model
Answer: C (LEAVE A REPLY)
Explanation
Capability Maturity Model (CMM) is a framework that describes the key elements of an effective software process. It defines five levels of maturity for software development organizations, from initial to optimized. The CMM helps organizations to assess their current level of process capability and identify the areas for improvement1. References: ISO/IEC 27001:2022 Lead Auditor - IECB

NEW QUESTION: 162
Who is authorized to change the classification of a document?
A. The author of the document
B. The administrator of the document
C. The owner of the document
D. The manager of the owner of the document
Answer: C (LEAVE A REPLY)
The owner of the document is authorized to change the classification of the document. The owner of the document is the person who has the ultimate responsibility for the creation, maintenance, and protection of the document. The author of the document is not necessarily the owner of the document, as they may create the document on behalf of someone else. The administrator of the document is not authorized to change the classification of the document, as they only provide technical support for managing and storing documents. The manager of the owner of the document is not authorized to change the classification of the document, unless they are delegated by the owner or have a higher authority in the organization. Reference: : CQI & IRCA

ISO 27001:2022 Lead Auditor Course Handbook, page 37. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 38. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 39. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 40. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 41.

NEW QUESTION: 163
In the event of an Information security incident, system users' roles and responsibilities are to be observed, except:
A. Report suspected or known incidents upon discovery through the Servicedesk
B. Preserve evidence if necessary
C. Cooperate with investigative personnel during investigation if needed
D. Make the information security incident details known to all employees
Answer: D (LEAVE A REPLY)
The role and responsibility that system users should not observe in the event of an information security incident is D: make the information security incident details known to all employees. This is not a proper role or responsibility for system users, as it could cause unnecessary panic, confusion or speculation among employees who are not involved in the incident response process. It could also compromise the confidentiality and integrity of the incident information, which could be sensitive or confidential in nature. Making the information security incident details known to all employees could also violate the information security policies and procedures of the organization, which may require a certain level of discretion and confidentiality when dealing with incidents. The other roles and responsibilities are correct, as they describe what system users should do in the event of an information security incident, such as reporting the incident to the Servicedesk (A), preserving evidence if necessary (B), and cooperating with investigative personnel if needed. These roles and responsibilities help to ensure a quick, effective and orderly response to information security incidents. ISO/IEC 27001:2022 requires the organization to implement procedures for reporting and managing information security incidents (see clause A.16.1). 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 Security Incident Management?

NEW QUESTION: 164
You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.
The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.

A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
E. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
F. I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest
Answer: A,B,E,F (LEAVE A REPLY)
Explanation
* A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship
* with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12
* B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO
27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12
* E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to

measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12

* F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO 27001:2022:

* C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12

* D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12

* G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the

* information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12

* H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work

based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 165
Which four of the following statements about audit reports are true?
A. Audit reports should be produced within an agreed timescale
B. Audit reports that are no longer required can be destroyed as part of the organisation's general waste
C. Audit reports should include or refer to the audit plan
D. Audit reports should be produced by the audit team leader with input from the audit team
E. Audit reports should only evidence nonconformity
F. Audit reports should be assumed suitable for general circulation unless they are specifically marked confidential
G. Audit reports should always be reviewed by the client, dated, and signed as 'accepted'
H. Audit reports should be sent to the organisation's top management first because their contents could be embarrassing
Answer: A,C,D,G (LEAVE A REPLY)

NEW QUESTION: 166
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: (SHOW ANSWER)
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

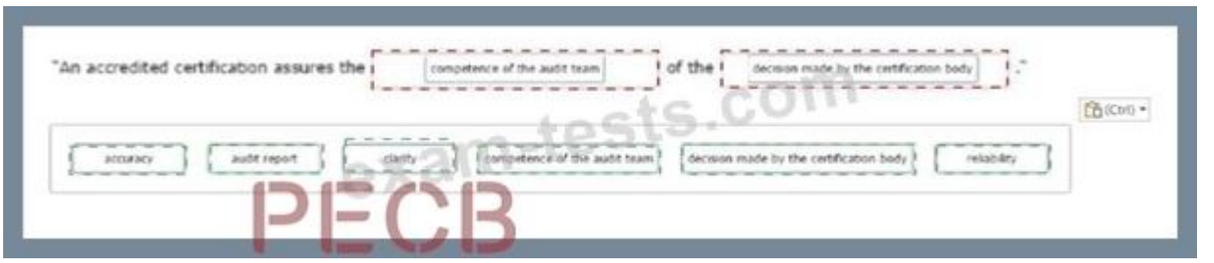
of the nature and limitations of the audit, and to avoid any misunderstandings or false expectations. The other options are not appropriate for inclusion in the closing meeting agenda, as they are either irrelevant, incorrect, or incomplete.
For example:
*A detailed explanation of the certification body's 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: 167
You are the person responsible for managing the audit programme and deciding the size and composition of the audit team for a specific audit. Select the two factors that should be considered.
A. The audit scope and criteria
B. Customer relationships
C. The overall competence of the audit team needed to achieve audit objectives
D. Seniority of the audit team leader
E. The cost of the audit
F. The duration preferred by the auditee
Answer: (SHOW ANSWER)
Explanation
The overall competence of the12:
The audit scope and criteria: The audit scope defines the extent and boundaries of the audit, such as the locations, processes, functions, and time period to be audited. The audit criteria are the set of policies, procedures, standards, or requirements used as a reference against which the audit evidence is compared.
The audit scope and criteria determine the complexity and extent of the audit, and thus influence the number and expertise of the auditors needed to cover all the relevant aspects of the audit.
The overall competence of the audit team needed to achieve audit objectives: The audit team should have the appropriate knowledge, skills, and experience to conduct the audit effectively and efficiently, and to provide credible and reliable audit results. The audit team competence should include the following elements12:
Generic competence: The ability to apply the principles and methods of auditing, such as planning, conducting, reporting, and following up the audit, as well as the personal behaviour and attributes of the auditors, such as ethical conduct, fair presentation, professional care, independence, and impartiality.
Discipline and sector-specific competence: The ability to understand and apply the audit criteria and the relevant technical or industry aspects of the audited organization, such as the information security management system (ISMS) requirements, the information security risks and controls, the legal and regulatory obligations, the organizational context and culture, the processes and activities, the products and services, etc.
Audit team leader competence: The ability to manage the audit team and the audit process, such as coordinating the audit activities, communicating with the audit programme manager and the auditee, resolving any audit-related problems, ensuring the quality and consistency of the audit work and the audit report, etc.

The person responsible for managing the audit programme should not consider the following factors when deciding the size and composition of the audit team for a specific audit, as they are either irrelevant or inappropriate for the audit process12:
Customer relationships: The audit team should not be influenced by any personal or professional relationships with the auditee or other interested parties, as this may compromise the objectivity and impartiality of the audit. The audit team should avoid any conflicts of interest or self-interest that may affect the audit results or the audit decisions.
Seniority of the audit team leader: The audit team leader should be selected based on their competence and experience, not on their seniority or rank within the organization or the audit programme. The audit team leader should have the authority and responsibility to manage the audit team and the audit process, regardless of their seniority or position.
The cost of the audit: The cost of the audit should not be the primary factor for determining the size and composition of the audit team, as this may compromise the quality and effectiveness of the audit. The audit team should have sufficient resources and time to conduct the audit in accordance with the audit objectives, scope, and criteria, and to provide accurate and reliable audit results and recommendations.
The duration preferred by the auditee: The duration of the audit should be based on the audit objectives, scope, and criteria, and the availability and cooperation of the auditee, not on the preference or convenience of the auditee. The audit team should have enough time to conduct the audit in a thorough and systematic manner, and to collect and evaluate sufficient and relevant audit evidence.
References:
ISO 19011:2018 - Guidelines for auditing management systems
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-20

NEW QUESTION: 168
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: 169
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: G (LEAVE A REPLY)
Explanation
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: 170
Which two of the following statements are true?
A. The role of a certification body auditor involves evaluating the organisation's processes for ensuring compliance with their legal requirements
B. Curing a third-party audit, the auditor evaluates how the organisation ensures that 4 6 made aware of changes to the legal requirements
C. As part of a certification body audit the auditor is resporable for verifying the organisation's legal compliance status
Answer: A,B (LEAVE A REPLY)
The following statements are true:
* The role of a certification body auditor involves evaluating the organization's processes for ensuring compliance with their legal requirements. This is part of the auditor's responsibility to assess the effectiveness and conformity of the organization's ISMS against the ISO/IEC 27001:2022 standard and the applicable legal and regulatory requirements.
* During a third-party audit, the auditor evaluates how the organization ensures that they are made aware of changes to the legal requirements. This is part of the auditor's responsibility to verify that the organization has established and maintained a process for identifying and updating their legal and other requirements related to information security. The following statement is false:
* As part of a certification body audit, the auditor is responsible for verifying the organization's legal compliance status. This is not true, as the auditor is not authorized or qualified to provide legal advice or judgment on the organization's compliance status. The auditor can only report on the evidence of compliance or noncompliance observed during the audit, but the ultimate responsibility for ensuring legal compliance lies with the organization. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 66. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 67. ISO/IEC 27001 LEAD AUDITOR - PECB, page 22.

NEW QUESTION: 171
Which two of the following are examples of audit methods that 'do not' involve human interaction?
A. Conducting an interview using a teleconferencing platform
B. Performing a review of auditees procedures in preparation for an audit
C. Reviewing the auditee's response to an audit finding
D. Analysing data by remotely accessing the auditee's server
E. Observing work performed by remote surveillance
F. Confirming the date and time of the audit
Answer: (SHOW ANSWER)

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: 172
In which order is an Information Security Management System set up?
A. Implementation, operation, improvement, maintenance
B. Implementation, operation, maintenance, establishment
C. Establishment, operation, monitoring, improvement
D. Establishment, implementation, operation, maintenance
Answer: D (LEAVE A REPLY)
The establishment phase of an ISMS involves defining the scope, context, objectives, and leadership commitment for information security management within an organization. It also involves identifying and assessing the risks and opportunities related to information security and selecting the appropriate controls to treat them. The implementation phase of an ISMS involves executing the plans and actions to achieve the information security objectives and implement the selected controls. It also involves ensuring the availability of resources and competencies for information security management. The operation phase of an ISMS involves monitoring and measuring the performance and effectiveness of the ISMS and reporting on the results. It also involves addressing nonconformities and taking corrective actions to prevent recurrence. The maintenance phase of an ISMS involves reviewing and evaluating the ISMS at planned intervals and identifying opportunities for improvement. It also involves updating the ISMS as necessary to reflect changes in the internal and external context of the organization. Therefore, an ISMS is set

up in the following order: establishment, implementation, operation, maintenance. Reference: ISO/IEC 27001:2022, clauses 6-10; ISO/IEC 27000:2022, clause 4.

NEW QUESTION: 173
What is the worst possible action that an employee may receive for sharing his or her password or access with others?
A. Forced roll off from the project
B. The lowest rating on his or her performance assessment
C. Three days suspension from work
D. Termination
Answer: (SHOW ANSWER)
The worst possible action that an employee may receive for sharing his or her password or access with others is termination, because this is a serious breach of the organization's information security policy and access control policy. Sharing password or access with others may allow unauthorized users to access sensitive or confidential information, or to perform malicious or fraudulent activities on behalf of the employee. The employee should keep his or her password or access confidential and secure, and should not disclose it to anyone under any circumstances. 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 access control policy

NEW QUESTION: 174
You are an experienced ISMS audit team leader providing guidance to an auditor in training. She asks you why it is important to have specific criteria relating to the grading of nonconformities. Which one of the following responses is correct?
A. Because grading criteria provide a common basis for the evaluation of nonconformities across the organization
B. Because ISO/IEC 27001:2022 requires it
C. Because the establishment and implementation of grading criteria demonstrate a high level of commitment to the corrective action process
D. Because grading criteria will ensure that all auditors score nonconformities in exactly the same way
Answer: A (LEAVE A REPLY)
Explanation
The correct response is A, because grading criteria provide a common basis for the evaluation of nonconformities across the organization. Grading criteria are the rules or standards that define the severity or impact of nonconformities, and help to determine the appropriate corrective actions and follow-up activities.
Grading criteria are important for several reasons, such as:

They ensure consistency and objectivity in the assessment and reporting of nonconformities, and avoid subjective or arbitrary judgments.
They facilitate the communication and understanding of nonconformities among the auditors, the auditees, and the audit clients, and enable the comparison and benchmarking of nonconformities across different processes, functions, or locations.
They support the prioritization and allocation of resources for the resolution of nonconformities, and the monitoring and measurement of the effectiveness of the corrective actions.
They demonstrate the commitment and accountability of the organization to the continual improvement of the ISMS, and the compliance with the ISMS requirements and expectations.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy ISO 19011:2022, Guidelines for auditing management systems

NEW QUESTION: 175
Select the words that best complete the sentence:

Answer:

Explanation:
A third-party audit is an independent assessment of an organisation's management system by an external auditor, who is not affiliated with the organisation or its customers. The auditor verifies that the management system meets the requirements of a specific standard, such as ISO 27001, and evaluates its effectiveness and performance. The auditor also identifies any strengths, weaknesses, opportunities, or risks of the management system, and provides recommendations for improvement. The purpose of a third-party audit is to provide an objective and impartial evaluation of the organisation's management system, and to inform a certification decision by a certification body. A certification body is an organisation that grants a certificate of conformity to the organisation, after reviewing the audit report and evidence, and confirming that the

management system meets the certification criteria. A certification decision is the outcome of the certification process, which can be positive (granting, maintaining, renewing, or expanding the scope of certification) or negative (suspending, withdrawing, or reducing the scope of certification). References:
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
ISO 19011:2018 - Guidelines for auditing management systems
The ISO 27001 audit process | ISMS.online

NEW QUESTION: 176
Which of the following does a lack of adequate security controls represent?
A. Threat
B. Asset
C. Vulnerability
D. Impact
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
An external auditor received an offer to conduct an ISMS audit at a research development company. Before accepting it, they discussed with the internal auditor of the auditee, who was their friend, about previous audit reports. Is this acceptable?
A. No, the external auditor should discuss about the auditee's previous audit reports only with the certification body
B. Yes, the auditor can review and discuss the previous audit reports before accepting an audit mandate
C. No, the auditor should uphold objectivity even when deciding whether to accept the audit mandate or not
Answer: C (LEAVE A REPLY)
No, the auditor should uphold objectivity even when deciding whether to accept the audit mandate or not.
Discussing previous audit reports with a friend who is an internal auditor at the auditee may compromise the external auditor's objectivity and independence.
References: ISO 19011:2018, Guidelines for auditing management systems, which emphasizes the need for auditors to maintain impartiality and confidentiality.

NEW QUESTION: 178
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: 179
Which three of the following options are an advantage of using a sampling plan for the audit?
A. Overrules the auditor's instincts
B. Use of the plan for consecutive audits
C. Provides a suitable understanding of the ISMS
D. Implements the audit plan efficiently
E. Gives confidence in the audit results
F. Misses key issues
Answer: (SHOW ANSWER)
According to ISO 19011:2018, which provides guidelines for auditing management systems, a sampling plan is a method for selecting a representative subset of the audit evidence from a defined population1. A sampling plan can have several advantages for the audit, such as providing a suitable understanding of the ISMS by covering its key processes, activities, and controls; implementing the audit plan efficiently by optimizing the use of time and resources; and giving confidence in the audit results by ensuring that the sample is sufficient, reliable, and unbiased1. Therefore, these three options are examples of advantages of using a sampling plan for the audit. The other options are not advantages, but rather disadvantages or risks of using a sampling plan. For example, overruling the auditor's instincts may lead to missing important evidence or issues that are not covered by the sampling plan; using the same plan for consecutive audits may reduce the effectiveness and validity of the audit results; and missing key issues may result from an inadequate or inappropriate sampling plan1. Reference: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 180
Stages of Information
A. creation, distribution, use, maintenance, disposition
B. creation, use, disposition, maintenance, evolution

C. creation, distribution, maintenance, disposition, use
D. creation, evolution, maintenance, use, disposition
Answer: (SHOW ANSWER)

NEW QUESTION: 181
Which one of the following options describes the main purpose of a Stage 1 audit?
A. To determine readiness for Stage 2
B. To check for legal compliance by the organisation
C. To get to know the organisation
D. To compile the audit plan
Answer: A (LEAVE A REPLY)
The main purpose of a Stage 1 audit is to evaluate the adequacy and effectiveness of the organisation's ISMS documentation, and to assess whether the organisation is prepared for the Stage 2 audit, where the implementation and operation of the ISMS will be verified. The Stage 1 audit also involves verifying the scope, objectives, and context of the ISMS, as well as identifying any areas of concern or nonconformities that need to be addressed before the Stage 2 audit.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems Section 7.3.1

NEW QUESTION: 182
You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including misaddressed labels and, in 15% of cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).
You: Are items checked before being dispatched?

SM: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.
You: What action is taken when items are returned?
SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.
You raise a nonconformity against ISO 27001:2022 based on the lack of control of the labelling process.
At the closing meeting, the Shipping Manager issues an apology to you that his comments may have been misunderstood. He says that he did not realise that there is a background IT process that automatically checks that the right label goes onto the right parcel otherwise the parcel is ejected at labelling. He asks that you withdraw your nonconformity.
Select three options of the correct responses that you as the audit team leader would make to the request of the Shipping Manager.
A. Advise the Shipping Manager that his request will be included in the audit report
B. Advise management that the new information provided will be discussed when the auditors have more time
C. Inform the Shipping Manager that the nonconformity is minor and should be quickly corrected
D. Ask the audit team members to state what they think should happen
E. Inform him of your understanding and withdraw the nonconformity
F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed
G. Advise the Shipping Manager that the nonconformity must stand since the evidence obtained for it was dear
H. Indicate that the nonconformity is evidence of a deeper system failure that needs to be rectified
Answer: A,B,F (LEAVE A REPLY)
Explanation
* A. Advise the Shipping Manager that his request will be included in the audit report. This is true because the audit report should document all the relevant information and evidence related to the audit, including any requests or objections raised by the auditee. The audit report should also provide the rationale for the audit conclusions and recommendations12.
* B. Advise management that the new information provided will be discussed when the auditors have more time. This is true because the auditors should not make hasty decisions based on incomplete or unverified information. The auditors should review and evaluate the new information in a systematic and objective manner, and determine whether it affects the audit findings, nonconformities, or conclusions12.
* F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed. This is true because the auditors should acknowledge and appreciate the cooperation and transparency of the auditee, but also maintain their professional integrity and independence. The auditors should not withdraw a nonconformity unless they are satisfied that it was raised in error or that it has been effectively corrected and verified12.

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

NEW QUESTION: 183
There is a network printer in the hallway of the company where you work. Many employees don't pick up their printouts immediately and leave them on the printer.
What are the consequences of this to the reliability of the information?
A. The integrity of the information is no longer guaranteed.
B. The availability of the information is no longer guaranteed.
C. The confidentiality of the information is no longer guaranteed.
D. The Security of the information is no longer guaranteed.
Answer: (SHOW ANSWER)
Confidentiality is one of the Confidentiality, Integrity, Availability (CIA) principles of information security 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. Often, people do not pick up their prints from a shared printer. This can affect the confidentiality of information, as anyone who passes by the printer can see or take the printed documents that may contain confidential or personal information. This can lead to information leakage, identity theft, fraud, or other malicious activities. Therefore, the correct answer is C.
Reference: ISO/IEC 27000:2022, clause 3.8; How & Where to Print Sensitive Documents on a Shared Printer.

NEW QUESTION: 184
As the Information Security Management System audit team leader, you are conducting a second-party audit of an international logistics company on behalf of an online retailer.
During the audit, one of your team members reports a nonconformity relating to control 5.18 (Access rights) of Appendix A of ISO/IEC 27001:2022.
She found evidence that removing the server access protocols of 20 people who left in the last 3 months took up to 1 week whereas the policy required removing access within 24 hours of their departure.
When the auditee was asked why there was a delay in removing access they replied, 'no one was available in the IT department during that period as a result of COVID-19.
As soon as an IT officer became available the rights were removed.
You note that she intends to raise a minor non-conformity against Access rights control (5.18).
How should you respond to this?
A. Agree with the raising of a minor non-conformity but against control 5.15, not 5.18.
B. Agree with the raising of the minor non-conformity against 5.18.
C. Disagree with the raising of a minor conformity as appropriate action was taken at the earliest opportunity Take no further action.

D. Require additional audit evidence to be obtained before determining whether a non-conformity is appropriate.
E. Disagree with the raising of the minor nonconformity, there is sufficient evidence to justify an escalation to a major non-conformity.
F. Disagree with the raising of the minor nonconformity as appropriate action was taken at the earliest opportunity. Instead raise an opportunity for improvement.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 185
An employee caught temporarily storing an MP3 file in his workstation will not receive an IR.
A. True
B. False
Answer: (SHOW ANSWER)
Explanation
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. 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], Example of an information security policy, Example of an acceptable use policy

NEW QUESTION: 186
You receive the following mail from the IT support team: Dear User,Starting next week, we will be deleting all inactive email accounts in order to create spaceshare the below details in order to continue using your account. In case of no response, Name:
Email ID:
Password:
DOB:
Kindly contact the webmail team for any further support. Thanks for your attention.
Which of the following is the best response?
A. Respond it by saying that one should not share the password with anyone
B. Ignore the email
C. One should not respond to these mails and report such email to your supervisor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187

You are the audit team leader conducting a third-party audit of an online insurance organisation. During Stage
1, you found that the organisation took a very cautious risk approach and included all the information security controls in ISO/IEC 27001:2022 Appendix A in their Statement of Applicability.
During the Stage 2 audit, your audit team found that there was no evidence of the implementation of the three controls (5.3 Segregation of duties, 6.1 Screening, 7.12 Cabling security) shown in the extract from the Statement of Applicability. No risk treatment plan was found.

Control Reference	Objective	Control driven by			Applicable	Last Assessed	Justification if not applicable
		Business Risk	Legal requirement	Customer Contract			
5.3	Avoid conflicts of interest	Yes	No	No	Yes	02/202X	None
6.1	Screen personnel	Yes	No	Yes	Yes	02/202X	None
7.12	Cable protection	Yes	Yes	No	Yes	02/202X	None

Select three options for the actions you would expect the auditee to take in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:2022.
A. Allocate responsibility for producing evidence to prove to auditors that the controls are implemented.
B. Compile plans for the periodic assessment of the risks associated with the controls.
C. Implement the appropriate risk treatment for each of the applicable controls.
D. Incorporate written procedures for the controls into the organisation's Security Manual.
E. Remove the three controls from the Statement of Applicability.
F. Revise the relevant content in the Statement of Applicability to justify their exclusion.
G. Revisit the risk assessment process relating to the three controls.
H. Undertake a survey of customers to find out if the controls are needed by them.
Answer: C,F,G (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the auditee should take the following actions in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:20221:
* Implement the appropriate risk treatment for each of the applicable controls, as this is the main requirement of clause 6.1.3.e and the objective of the risk treatment process2.
* Revise the relevant content in the Statement of Applicability to justify their exclusion, as this is the expected output of the risk treatment process and the evidence of the risk-based decisions3.
* Revisit the risk assessment process relating to the three controls, as this is the input for the risk treatment process and the source of identifying the risks and the controls4.
The other options are not correct because:

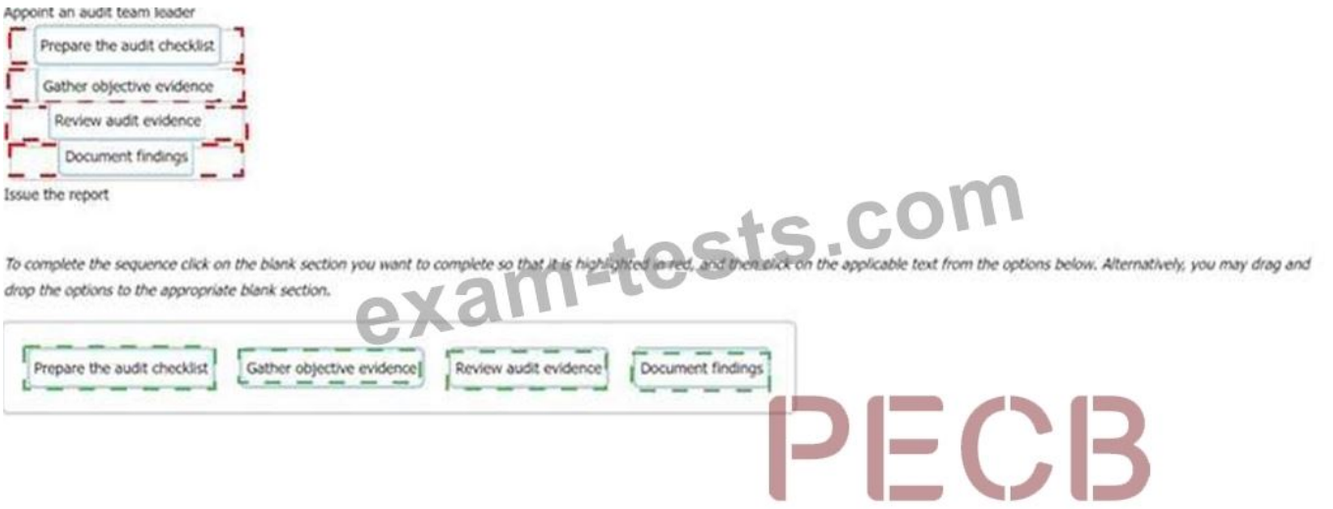
* Allocating responsibility for producing evidence to prove to auditors that the controls are implemented is not a valid action, as the audit team already found that there was no evidence of the implementation of the three controls.
* Compiling plans for the periodic assessment of the risks associated with the controls is not a valid action, as this is part of the risk monitoring and review process, not the risk treatment process5.
* Incorporating written procedures for the controls into the organisation's Security Manual is not a valid action, as this is part of the documentation and operation of the ISMS, not the risk treatment process.
* Removing the three controls from the Statement of Applicability is not a valid action, as this is not a sufficient justification for their exclusion and does not reflect the risk treatment process.
* Undertaking a survey of customers to find out if the controls are needed by them is not a valid action, as this is not a relevant criterion for the risk assessment and treatment process, which should be based on the organisation's own context and objectives.
References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 36, section 4.5.22:
ISO/IEC 27001:2022, clause 6.1.3.e3: ISO/IEC 27001:2022, clause 6.1.3.f4: ISO/IEC 27001:2022, clause
6.1.25: ISO/IEC 27001:2022, clause 6.2. : ISO/IEC 27001:2022, clause 7.5 and 8. : ISO/IEC 27001:2022, clause 6.1.3.d. : ISO/IEC 27001:2022, clause 4.1 and 4.2.

NEW QUESTION: 188
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:
Which risk treatment option has Knight used in replacing FTP with SSH? Refer to scenario 2.
A. Risk retention
B. Risk avoidance
C. Risk modification
Answer: C (LEAVE A REPLY)
Risk modification involves implementing controls to reduce the likelihood or impact of a risk. By replacing FTP with SSH, Knight has modified the risk associated with the transfer of files by ensuring that the data is encrypted, thereby reducing the likelihood of unauthorized access through traffic capturing1. References: = This answer is based on the standard risk treatment options provided in ISO/IEC 27001, which include avoiding, modifying, sharing, or retaining risks as part of the risk management process

NEW QUESTION: 189
The following options are key actions involved in a first-party audit. Order the stages to show the sequence in which the actions should take place.

Answer:



Explanation:

The correct order of the stages is:

* Prepare the audit checklist
* Gather objective evidence
* Review audit evidence
* Document findings
* Audit preparation: This stage involves defining the audit objectives, scope, criteria, and plan. The auditor also prepares the audit checklist, which is a list of questions or topics that will be covered during the audit. The audit checklist helps the auditor to ensure that all relevant aspects

of the ISMS are addressed and that the audit evidence is collected in a systematic and consistent manner12.
* Audit execution: This stage involves conducting the audit activities, such as opening meeting, interviews, observations, document review, and closing meeting. The auditor gathers objective evidence, which is any information that supports the audit findings and conclusions. Objective evidence can be qualitative or quantitative, and can be obtained from various sources, such as records, statements, physical objects, or observations123.
* Audit reporting: This stage involves reviewing the audit evidence, evaluating the audit findings, and documenting the audit results. The auditor reviews the audit evidence to determine whether it is sufficient, reliable, and relevant to support the audit findings. The auditor evaluates the audit findings to determine the degree of conformity or nonconformity of the ISMS with the audit criteria. The auditor
* documents the audit results in an audit report, which is a formal record of the audit process and outcomes. The audit report typically includes the following elements123:
* An introduction clarifying the scope, objectives, timing and extent of the work performed
* An executive summary indicating the key findings, a brief analysis and a conclusion
* The intended report recipients and, where appropriate, guidelines on classification and circulation
* Detailed findings and analysis
* Recommendations for improvement, where applicable
* A statement of conformity or nonconformity with the audit criteria
* Any limitations or exclusions of the audit scope or evidence
* Any deviations from the audit plan or procedures
* Any unresolved issues or disagreements between the auditor and the auditee
* A list of references, abbreviations, and definitions used in the report
* A list of appendices, such as audit plan, audit checklist, audit evidence, audit team members, etc.
* Audit follow-up: This stage involves verifying the implementation and effectiveness of the corrective actions taken by the auditee to address the audit findings. The auditor monitors the progress and completion of the corrective actions, and evaluates their impact on the ISMS performance and conformity. The auditor may conduct a follow-up audit to verify the corrective actions on-site, or may rely on other methods, such as document review, remote interviews, or self-assessment by the auditee.
The auditor documents the follow-up results and updates the audit report accordingly123.
References:
* PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
* ISO 19011:2018 - Guidelines for auditing management systems
* The ISO 27001 audit process | ISMS.online

NEW QUESTION: 190

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: C,D,E,G (LEAVE A REPLY)

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: 191
You are an experienced ISMS audit team leader providing guidance to an auditor in training. She asks you why it is important to have specific criteria relating to the grading of nonconformities. Which one of the following responses is correct?
A. Because grading criteria provide a common basis for the evaluation of nonconformities across the organization
B. Because ISO/IEC 27001:2022 requires it
C. Because the establishment and implementation of grading criteria demonstrate a high level of commitment to the corrective action process
D. Because grading criteria will ensure that all auditors score nonconformities in exactly the same way
Answer: A (LEAVE A REPLY)
The correct response is A, because grading criteria provide a common basis for the evaluation of nonconformities across the organization. Grading criteria are the rules or standards that define the severity or impact of nonconformities, and help to determine the appropriate corrective actions and follow-up activities.
Grading criteria are important for several reasons, such as:
They ensure consistency and objectivity in the assessment and reporting of nonconformities, and avoid subjective or arbitrary judgments.
They facilitate the communication and understanding of nonconformities among the auditors, the auditees, and the audit clients, and enable the comparison and benchmarking of nonconformities across different processes, functions, or locations.

They support the prioritization and allocation of resources for the resolution of nonconformities, and the monitoring and measurement of the effectiveness of the corrective actions.
They demonstrate the commitment and accountability of the organization to the continual improvement of the ISMS, and the compliance with the ISMS requirements and expectations.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy ISO 19011:2022, Guidelines for auditing management systems

NEW QUESTION: 192
Which one of the following options describes the main purpose of a Stage 1 audit?
A. To determine readiness for Stage 2
B. To check for legal compliance by the organisation
C. To get to know the organisation
D. To compile the audit plan
Answer: A (LEAVE A REPLY)
Explanation
The main purpose of a Stage 1 audit is to evaluate the adequacy and effectiveness of the organisation's ISMS documentation, and to assess whether the organisation is prepared for the Stage 2 audit, where the implementation and operation of the ISMS will be verified. The Stage 1 audit also involves verifying the scope, objectives, and context of the ISMS, as well as identifying any areas of concern or nonconformities that need to be addressed before the Stage 2 audit.
References:
* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB
* ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems Section 7.3.1

NEW QUESTION: 193
Which of the following does an Asset Register contain? (Choose two)
A. Asset Type
B. Asset Owner
C. Asset Modifier
D. Process ID
Answer: (SHOW ANSWER)
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: 194
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: 195

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: D (LEAVE A REPLY)
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: 196
During a Stage 1 audit opening meeting, the Management System Representative (MSR) asks to extend the audit scope to include a new site overseas which they have expanded into since the certification application was made.
Select two options for how the auditor should respond.
A. Advise the MSR that an extension of the scope may be incorporated but will have to go through established procedures
B. Advise the MSR that the audit scope has been determined based on their initial application so the audit has to proceed as planned
C. Suggest that the MSR cancels the audit contract and reapplies for the new situation
D. Determine whether the Management System covers the processes at the new site and, if so, proceed with the audit
E. Advise the MSR that, within the existing scope, the new work area can be included without any problem
F. Confirm that the auditor will advise the auditee that the audit scope will be revised to include the new work area
Answer: (SHOW ANSWER)
Explanation
The correct options for how the auditor should respond are:
* A. Advise the MSR that an extension of the scope may be incorporated but will have to go through established procedures
* D. Determine whether the Management System covers the processes at the new site and, if so, proceed with the audit These options are consistent with the ISO/IEC 27006:2015 standard,

which states that any changes to the scope of certification should be notified by the client to the certification body, and that the certification body should evaluate and decide on these changes in accordance with its procedures1. The auditor should also verify that the ISMS is implemented and maintained at all sites included in the scope of certification1.
The other options are not appropriate for how the auditor should respond, because:
* B. Advise the MSR that the audit scope has been determined based on their initial application so the audit has to proceed as planned: This option is too rigid and does not allow for any flexibility or adaptation to the client's situation. The auditor should be open to consider any changes to the scope of
* certification that may have occurred since the initial application, as long as they are properly notified and evaluated by the certification body.
* C. Suggest that the MSR cancels the audit contract and reapplies for the new situation: This option is too drastic and unnecessary, as it would cause delays and costs for both the client and the certification body.
The auditor should not suggest that the client cancels the audit contract, but rather that they follow the established procedures for requesting and approving an extension of the scope of certification.
* E. Advise the MSR that, within the existing scope, the new work area can be included without any problem: This option is too lenient and does not ensure that the new work area meets the requirements of ISO/IEC 27001 and the ISMS. The auditor should not assume that the new work area can be included within the existing scope without any problem, but rather that they need to verify that the ISMS is implemented and maintained at the new site, and that any changes to the scope of certification are approved by the certification body.
* F. Confirm that the auditor will advise the auditee that the audit scope will be revised to include the new work area: This option is too presumptuous and does not respect the authority of the certification body.
The auditor should not confirm that they will revise the audit scope to include the new work area, but rather that they will advise the certification body of the client's request for an extension of the scope of certification, and wait for their decision.

NEW QUESTION: 197

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

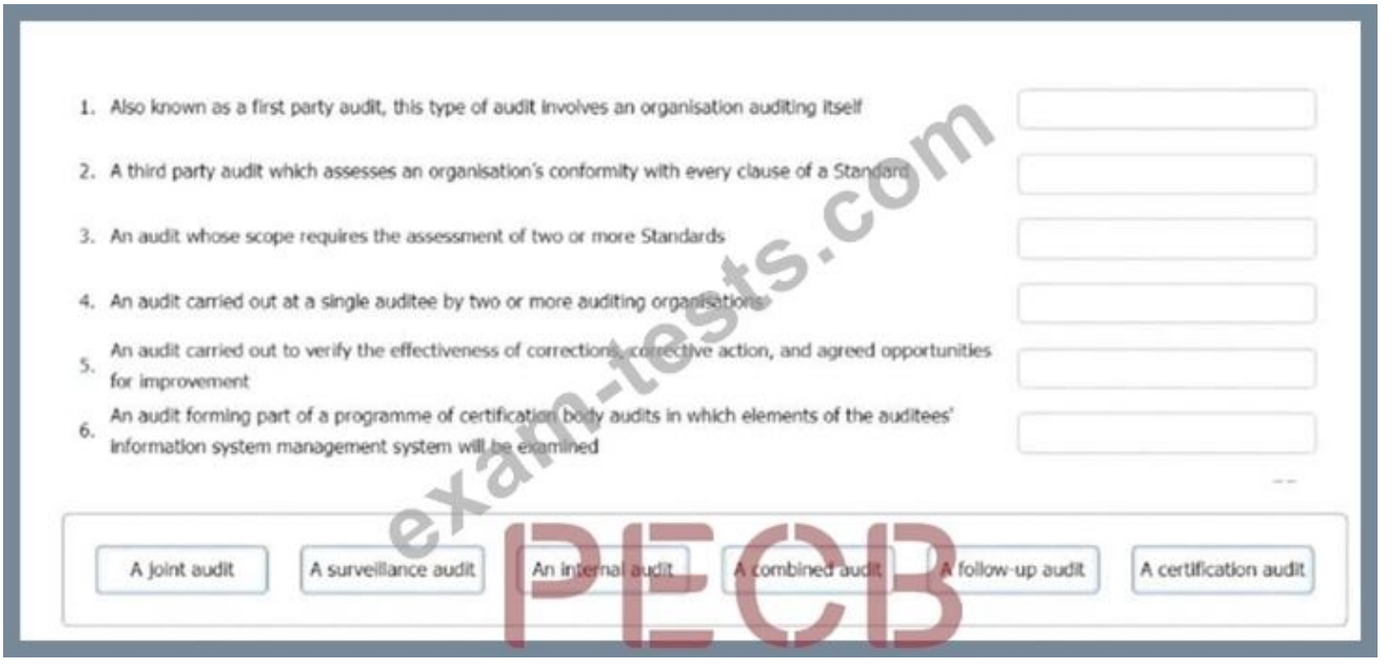
* Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.
* Advise the individual managing the audit programme of any decision taken regarding the outstanding
* nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.
* Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised by implementing effective corrective actions for most of them and agreeing on a plan for the remaining one. The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

NEW QUESTION: 198
Information has a number of reliability aspects. Reliability is constantly being threatened. Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.
Which of these examples is a threat to integrity?
A. accidental alteration of data
B. a loose cable
C. System restart
D. private use of data
Answer: (SHOW ANSWER)

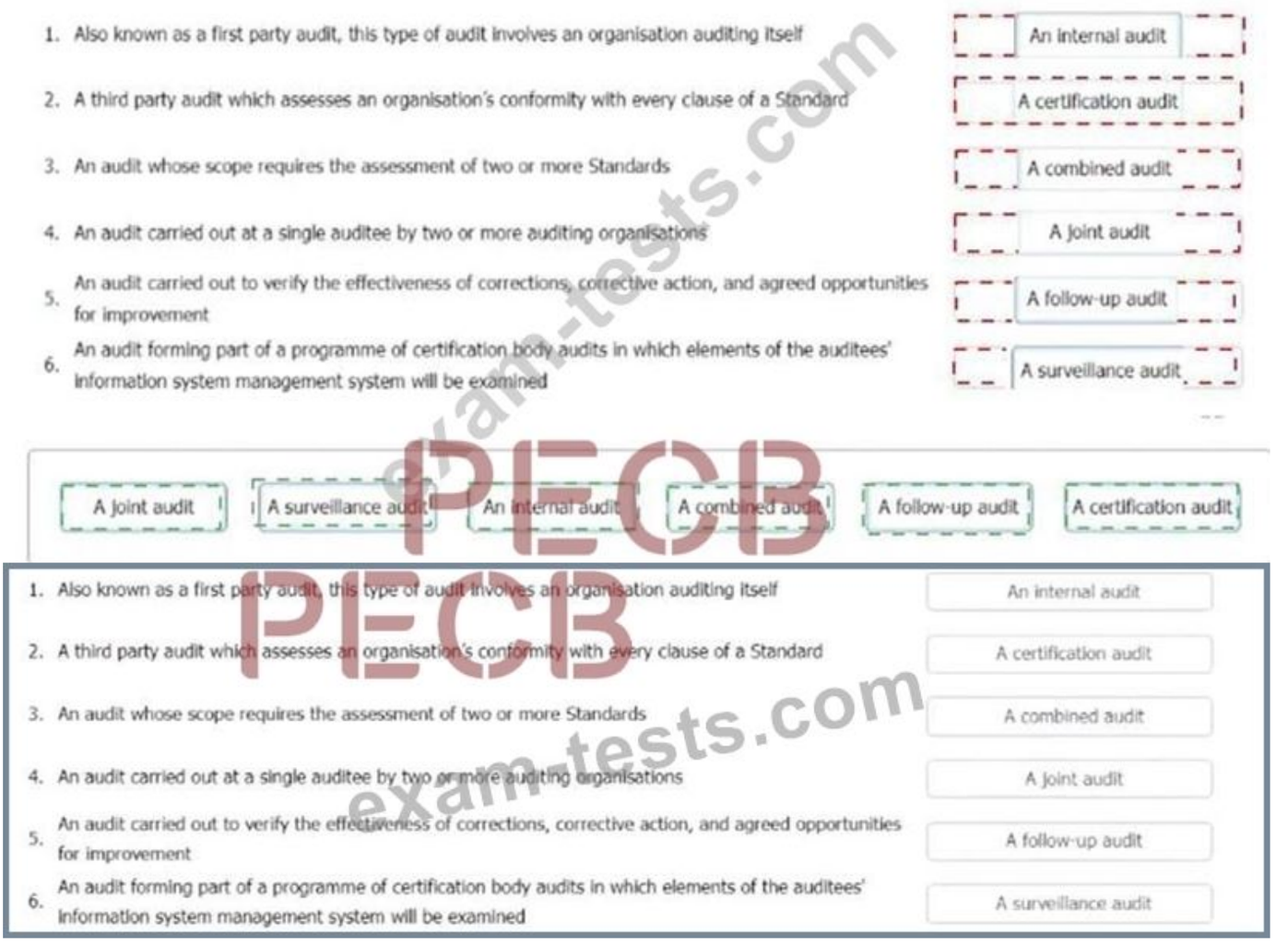
NEW QUESTION: 199
You are an experienced ISMS audit team leader conducting a third-party surveillance visit.
You notice that although the auditee is claiming conformity with ISO/IEC 27001:2022 they are still referring to Improvement as clause 10.2 (as it was in the 2013 edition) when this is now clause 10.1 in the 2022 edition. You have confirmed they are meeting all of the 2022 requirements set out in the standard.
Select one option of the action you should take.

A. Note the issue in the audit report
B. Raise a nonconformity against clause 7.5.3 - Control of documented information
C. Raise it as an opportunity for improvement
D. Bring the matter up at the closing meeting
Answer: (SHOW ANSWER)
Explanation
The correct action to take in this situation is to raise it as an opportunity for improvement. This is because the auditee is not violating any requirement of the standard, but rather using outdated terminology that does not reflect the current version of the standard. An opportunity for improvement is a suggestion for enhancing the performance or effectiveness of the ISMS1. It is not a nonconformity, which is a failure to fulfil a requirement2. Therefore, option B is incorrect. Option A is also incorrect, because noting the issue in the audit report without raising it as an opportunity for improvement would not provide any value or feedback to the auditee. Option D is also incorrect, because bringing the matter up at the closing meeting without documenting it as an opportunity for improvement would not ensure that the auditee takes any action to address it.
References: 1: ISMS Auditing Guideline - ISO27000, page 11; 2: ISO/IEC 27000:2022, 3.28; : ISMS Auditing Guideline - ISO27000; : ISO/IEC 27000:2022

NEW QUESTION: 200
You are an experienced ISMS audit team leader. An auditor in training has approached you to ask you to clarify the different types of audits she may be required to undertake.
Match the following audit types to the descriptions.
To complete the table click on the blank section you want to complete so that It is highlighted In fed, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.



Answer:



NEW QUESTION: 201

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)

Explanation

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.
References:
* 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: 202
Which two of the following phrases would apply to 'check' in the Plan-Do-Check-Act cycle for a business process?
A. Making improvements
B. Managing changes
C. Verifying training
D. Resetting objectives
E. Updating the Information Security Policy
F. Auditing processes
Answer: C,F (LEAVE A REPLY)
Explanation
The two phrases that would apply to 'check' in the Plan-Do-Check-Act cycle for a business process are:
C: Verifying training
F: Auditing processes
C: This phrase applies to 'check' in the PDCA cycle because it involves measuring and evaluating the effectiveness of the training activities that were implemented in the 'do' phase. Training is an important aspect of information security awareness, education, and competence, which are required by clause 7.2 of ISO 27001:20221. Verifying training can help the organisation to assess whether the staff have acquired the necessary knowledge, skills, and behaviour to perform their roles and responsibilities in relation to information security. Verifying training can also help the organisation to identify any gaps or weaknesses in the training program and to plan for improvement actions.
F: This phrase applies to 'check' in the PDCA cycle because it involves examining and reviewing the performance and conformity of the processes that were implemented in the 'do' phase. Auditing is a systematic, independent, and documented process for obtaining objective evidence and evaluating it to determine the extent to which the audit criteria are fulfilled2. Auditing processes can help the organisation to verify whether the information security objectives and requirements are met, whether the information security controls are effective and efficient, and whether the information security risks are adequately managed. Auditing processes can also help the organisation to identify any nonconformities or opportunities for improvement and to plan for corrective or preventive actions.

References:
1: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 7.2 2: ISO 19011:2018 - Guidelines for auditing management systems, clause 3.2

NEW QUESTION: 203
What type of system ensures a coherent Information Security organisation?
A. Federal Information Security Management Act (FISMA)
B. Information Technology Service Management System (ITSM)
C. Information Security Management System (ISMS)
D. Information Exchange Data System (IEDS)
Answer: C (LEAVE A REPLY)
An Information Security Management System (ISMS) is a systematic approach to managing the security of information assets within an organization. It includes the policies, processes, and controls that address the risks and opportunities related to information security. An ISMS is based on the Plan-Do-Check-Act (PDCA) cycle, which consists of four phases: establishment, implementation, operation, and maintenance. Therefore, an ISMS is set up in the following order: establishment, implementation, operation, maintenance. Reference: ISO/IEC 27000:2022, clause 3.24; ISO/IEC 27001:2022, clause 4.

NEW QUESTION: 204
You have a hard copy of a customer design document that you want to dispose off. What would you do
A. Throw it in any dustbin
B. Shred it using a shredder
C. Give it to the office boy to reuse it for other purposes
D. Be environment friendly and reuse it for writing
Answer: (SHOW ANSWER)
The best way to dispose of a hard copy of a customer design document is to shred it using a shredder. This is because shredding ensures that the document is destroyed and cannot be reconstructed or accessed by unauthorized persons. A customer design document may contain sensitive or confidential information that could cause harm or damage to the customer or the organization if disclosed. Therefore, it is important to protect the confidentiality and integrity of the document until it is securely disposed of. Throwing it in any dustbin, giving it to the office boy to reuse it for other purposes, or reusing it for writing are not secure ways of disposing of the document, as they could expose the document to unauthorized access, theft, loss or damage. ISO/IEC 27001:2022 requires the organization to implement procedures for the secure disposal of media containing information (see clause A.8.3.2). 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 Secure Disposal?

NEW QUESTION: 205
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: 206
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. Raise a nonconformity against control A.7.5, 'protecting against physical and environmental threats' because the drives have been left exposed on the desktop.
B. Record the finding but note no further action is required as the pickup has now been rescheduled.
C. 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'.
D. Record a nonconformity against control A.5.13 'labelling of information' as the disk drives' status was unclear

E. Ensure that the organisation's arrangements for the secure disposal and reuse of equipment have been adhered to.
F. Raise a nonconformity against control A.7.7, 'clear desk and clear screen' because the drives have been left unprotected on the desktop.
G. Ensure that the organisation's arrangements for the life cycle management of storage media have been adhered to.
H. Record an opportunity for improvement in respect of the external provider's inventory management arrangements.
Answer: C,E,G (LEAVE A REPLY)

NEW QUESTION: 207
As an auditor, you have noticed that ABC Inc. has established a procedure to manage the removable storage media. The procedure is based on the classification scheme adopted by ABC Inc. Thus, if the information stored is classified as "confidential," the procedure applies. On the other hand, the information that is classified as "public," does not have confidentiality requirements: thus, only a procedure for ensuring its integrity and availability applies. What type of audit finding is this?
A. Nonconformity
B. Anomaly
C. Conformity
Answer: C (LEAVE A REPLY)
This scenario represents a conformity because ABC Inc. has implemented procedures for managing removable storage media that align with the classification scheme of the information stored. When information is classified as "confidential," more stringent procedures apply, whereas for "public" information, the procedures focus only on integrity and availability, following the organization's defined information classification policy.
References: ISO/IEC 27001:2013, Clause A.8.2 (Information classification)

NEW QUESTION: 208
You are performing an ISMS audit at a nursing home where residents always wear an electronic wristband for monitoring their location, heartbeat, and blood pressure. The wristband automatically uploads this data to a cloud server for healthcare monitoring and analysis by staff. You now wish to verify that the information security policy and objectives have been established by top management. You are sampling the mobile device policy and identify a security objective of this policy is "to ensure the security of teleworking and use of mobile devices" The policy states the following controls will be applied in order to achieve this.
Personal mobile devices are prohibited from connecting to the nursing home network, processing, and storing residents' data.
The company's mobile devices within the ISMS scope shall be registered in the asset register.
The company's mobile devices shall implement or enable physical protection, i.e., pin-code protected screen lock/unlock, facial or fingerprint to unlock the device.

The company's mobile devices shall have a regular backup.
To verify that the mobile device policy and objectives are implemented and effective, select three options for your audit trail.
A. Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home
B. Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home
C. Review the internal audit report to make sure the IT department has been audited
D. Review the asset register to make sure all personal mobile devices are registered
E. Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register
F. Review the asset register to make sure all company's mobile devices are registered
G. Interview the supplier of the devices to make sure they are aware of the ISMS policy
H. Interview top management to verify their involvement in establishing the information security policy and the information security objectives
Answer: (SHOW ANSWER)
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 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: 209
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: A,C,D,E (LEAVE A REPLY)
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: 210
What is the goal of classification of information?
A. Applying labels making the information easier to recognize
B. To create a manual about how to handle mobile devices
C. Structuring information according to its sensitivity

Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
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: 212
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)
Explanation

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: 213
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:
Which type of audit risk was defined as "low* by the audit team? Refer to scenario 5.
A. Inherent
B. Control
C. Detection
Answer: (SHOW ANSWER)
The audit team stated that the risk of a significant defect occurring in Data Grid Inc.'s ISMS was low. This refers to "Control Risk," which is the risk that a misstatement could occur in any relevant assertion related to an ISMS and that the risk could not be prevented or detected on a timely basis by the organization's internal control systems.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 214
Which two of the following phrases would apply to 'check' in the Plan-Do-Check-Act cycle for a business process?
A. Making improvements
B. Managing changes
C. Verifying training
D. Resetting objectives
E. Updating the Information Security Policy
F. Auditing processes
Answer: C,F (LEAVE A REPLY)
The two phrases that would apply to 'check' in the Plan-Do-Check-Act cycle for a business process are:
C. Verifying training
F. Auditing processes
C. This phrase applies to 'check' in the PDCA cycle because it involves measuring and evaluating the effectiveness of the training activities that were implemented in the 'do' phase. Training is an important aspect of information security awareness, education, and competence, which are required by clause 7.2 of ISO 27001:20221. Verifying training can help the organisation to assess whether the staff have acquired the necessary knowledge, skills, and behaviour to perform their roles and responsibilities in relation to information security. Verifying training can also help the organisation to identify any gaps or weaknesses in the training program and to plan for improvement actions.
F. This phrase applies to 'check' in the PDCA cycle because it involves examining and reviewing the performance and conformity of the processes that were implemented in the 'do' phase. Auditing is a systematic, independent, and documented process for obtaining objective evidence

and evaluating it to determine the extent to which the audit criteria are fulfilled2. Auditing processes can help the organisation to verify whether the information security objectives and requirements are met, whether the information security controls are effective and efficient, and whether the information security risks are adequately managed. Auditing processes can also help the organisation to identify any nonconformities or opportunities for improvement and to plan for corrective or preventive actions.
References:
1: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 7.2 2: ISO 19011:2018 - Guidelines for auditing management systems, clause 3.2

NEW QUESTION: 215
You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.
The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.
Select three options that relate to ISO/IEC 27001:2022's requirements regarding external providers.
A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
E. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
F. I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest
Answer: A,B,E (LEAVE A REPLY)
A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO

27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12

B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO

27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12

E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12

F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO

27001:2022:

C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12

D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

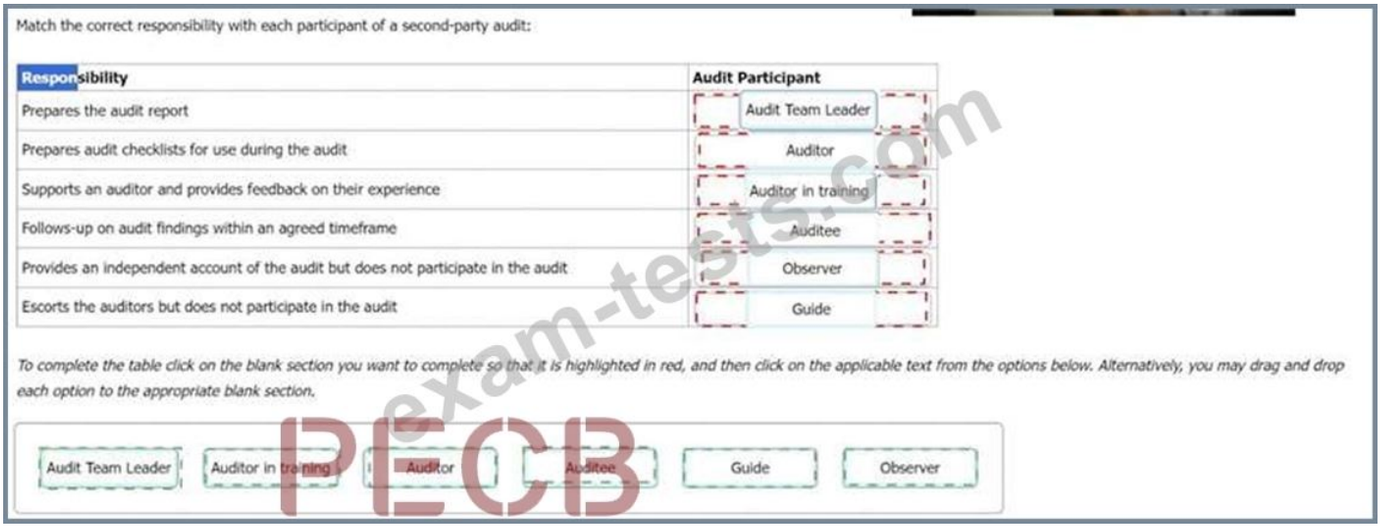
NEW QUESTION: 216
You receive an E-mail from some unknown person claiming to be representative of your bank and asking for your account number and password so that they can fix your account. Such an attempt of social engineering is called
A. Shoulder Surfing
B. Mountaineering
C. Phishing
D. Spoofing
Answer: C (LEAVE A REPLY)
An email from some unknown person claiming to be a representative of your bank and asking for your account number and password so that they can fix your account is an example of social engineering called phishing. 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. 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). 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 Phishing?

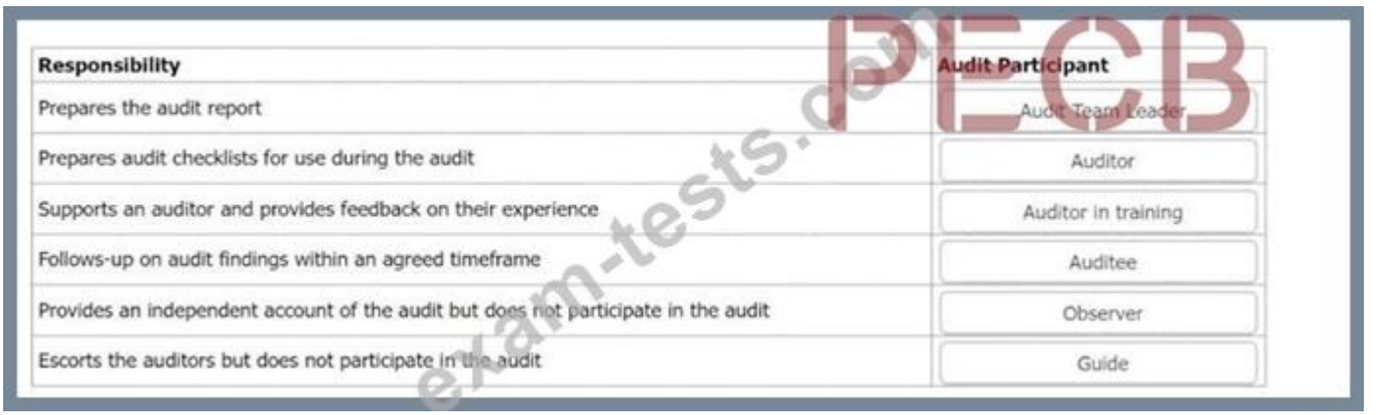
NEW QUESTION: 217

Match the correct responsibility with each participant of a second-party audit:

Answer:



Explanation



Responsibility	Audit Participant
Prepares the audit report	Audit Team Leader
Prepares audit checklists for use during the audit	Auditor
Supports an auditor and provides feedback on their experience	Auditor in training
Follows-up on audit findings within an agreed timeframe	Auditee
Provides an independent account of the audit but does not participate in the audit	Observer
Escorts the auditors but does not participate in the audit	Guide

The correct responsibility with each participant of a second-party audit is:

* Prepares the audit report: Audit Team Leader. The audit team leader is responsible for coordinating the audit activities, communicating with the auditee and the customer, and preparing and delivering the audit report that summarizes the audit findings and conclusions1.
* Prepares audit checklists for use during the audit: Auditor. The auditor is responsible for collecting and verifying objective evidence during the audit, using audit checklists as a tool to guide the audit process and ensure that all relevant aspects of the audit criteria are covered1.
* Supports an auditor and provides feedback on their experience: Auditor in training. The auditor in training is a person who is learning how to perform audits under the supervision of an experienced auditor. The auditor in training supports the auditor by observing and participating in the audit activities, and provides feedback on their experience to improve their skills and competence1.
* Follows-up on audit findings within an agreed timeframe: Auditee. The auditee is the organisation that is being audited by the customer or a third party on behalf of the customer. The auditee is responsible for providing access and cooperation to the auditors, and for following up on the audit findings within an agreed timeframe, by implementing corrective actions or improvement measures as needed1.
* Provides an independent account of the audit but does not participate in the audit: Observer. The observer is a person who accompanies the audit team but does not participate in the audit activities. The observer may be a representative of the customer, a regulatory body, or another interested party. The observer provides an independent account of the audit but does not interfere with or influence the audit process or outcome1.
* Escorts the auditors but does not participate in the audit: Guide. The guide is a person who is appointed by the auditee to assist the audit team during the audit. The guide may escort the auditors to different locations, facilitate access to information and personnel, or provide clarification or explanation as requested by the auditors. The guide does not participate in the audit or influence its results1.

NEW QUESTION: 218

All are prohibited in acceptable use of information assets, except:

A. Electronic chain letters

B. E-mail copies to non-essential readers

C. Company-wide e-mails with supervisor/TL permission.
D. Messages with very large attachments or to a large number ofrecipients.
Answer: C (LEAVE A REPLY)
The only option that is not prohibited in acceptable use of information assets is C: company-wide e-mails with supervisor/TL permission. This option implies that the sender has obtained the necessary authorization from their supervisor or team leader to send an e-mail to all employees in the organization. This could be done for legitimate business purposes, such as announcing important news, events or updates that are relevant to everyone. However, this option should still be used sparingly and responsibly, as it could cause unnecessary disruption or annoyance to the recipients if abused or misused. The other options are prohibited in acceptable use of information assets, as they could violate the information security policies and procedures of the organization, as well as waste resources and bandwidth. Electronic chain letters (A) are messages that urge recipients to forward them to multiple other people, often with false or misleading claims or promises. They are considered spam and could contain malicious links or attachments that could compromise information security. E-mail copies to non-essential readers (B) are messages that are sent to recipients who do not need to receive them or have no interest in them. They are considered unnecessary and could clutter the inbox and distract the recipients from more important messages. Messages with very large attachments or to a large number of recipients (D) are messages that consume a lot of network resources and could affect the performance or availability of the information systems. They could also exceed the storage capacity or quota limits of the recipients' mailboxes and cause problems for them. ISO/IEC 27001:2022 requires the organization to implement rules for acceptable use of assets (see clause A.8.1.3). 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 Acceptable Use?

NEW QUESTION: 219
Which is not a requirement of HR prior to hiring?
A. Applicant must complete pre-employment documentation requirements
B. Must undergo Awareness training on information security.
C. Undergo background verification
D. Must successfully pass Background Investigation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 220
Someone from a large tech company calls you on behalf of your company to check the health of your PC, and therefore needs your user-id and password. What type of threat is this?
A. Social engineering threat
B. Organisational threat
C. Technical threat

D. Malware threat

Answer: A (LEAVE A REPLY)

The type of threat that occurs when someone from a large tech company calls you on behalf of your company to check the health of your PC, and therefore needs your user-id and password, is a social engineering threat. Social engineering is a technique that manipulates people into revealing confidential or sensitive information, such as passwords, personal data, bank details, etc., by impersonating someone trustworthy or authoritative, such as an IT support staff, a manager, a colleague, etc. Social engineering can be done through various channels, such as phone calls, emails, text messages, etc., and can exploit human emotions, such as curiosity, fear, greed or sympathy. Social engineering is often used by hackers or cybercriminals to gain unauthorized access to information systems or networks, or to perform malicious or fraudulent activities. 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 Social Engineering?

NEW QUESTION: 221

Availability means

A. Service should be accessible at the required time and usable by all

B. Service should be accessible at the required time and usable only by the authorized entity

C. Service should not be accessible when required

Answer: B (LEAVE A REPLY)

Explanation

Availability means that service should be accessible at the required time and usable only by the authorized entity. Availability is one of the three main objectives of information security, along with confidentiality and integrity. Availability ensures that information and systems are not disrupted or denied by unauthorized actions or events. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24.

ISO/IEC 27001 Brochures | PECB, page 4.

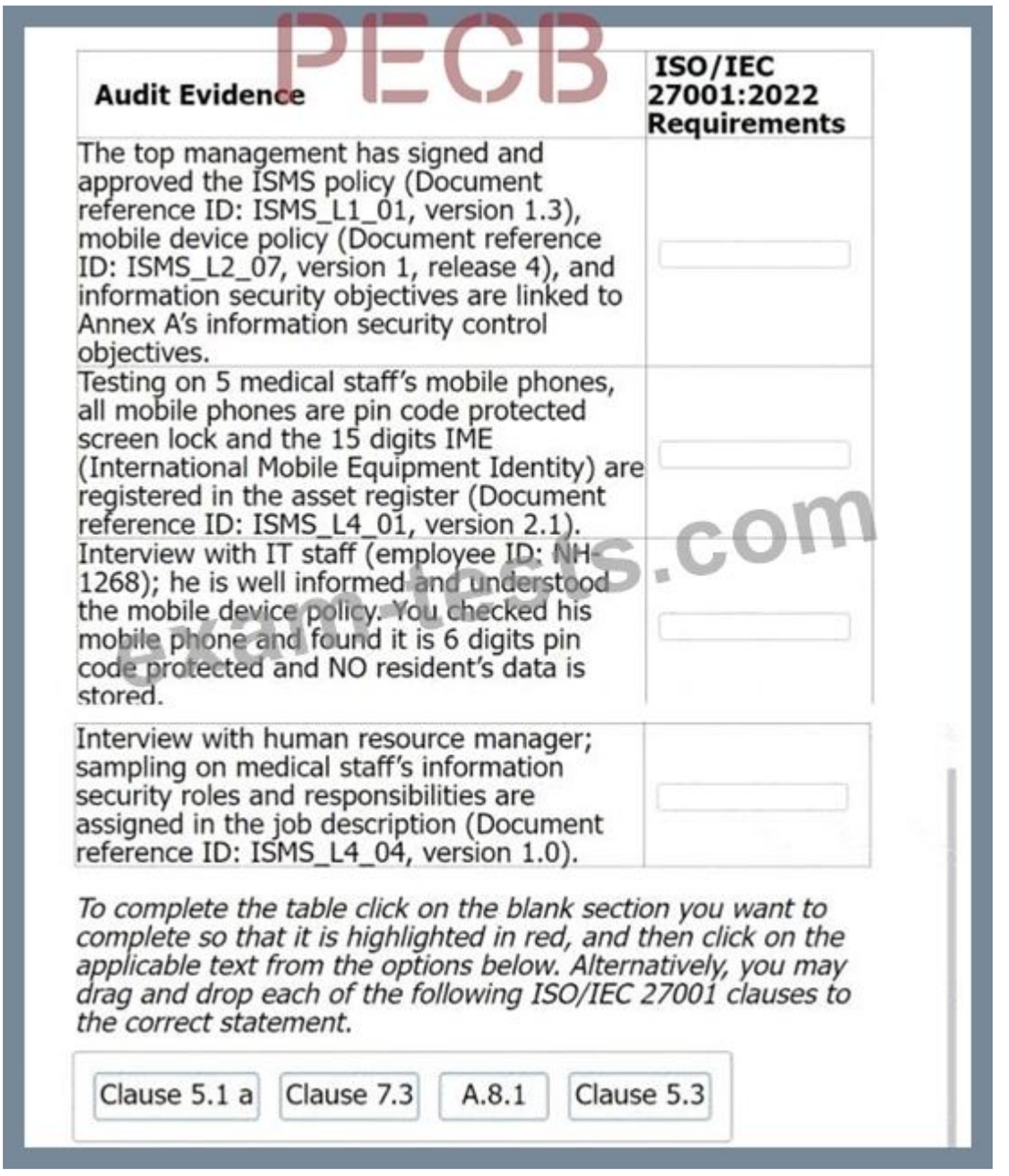
NEW QUESTION: 222

You are performing an ISMS audit at a European-based residential
nursing home called ABC that provides healthcare services. You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.

The next step in your audit plan is to verify that the information security policy and objectives have been established by top management.

During the audit, you found the following audit evidence.

Match the audit evidence to the corresponding requirement in ISO/IEC 27001:2022.



Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	

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 of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a | Clause 7.3 | A.8.1 | Clause 5.3

Answer:

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	Clause 5.1 a
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	A.8.1
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	Clause 7.3
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	Clause 5.3

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 of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a | Clause 7.3 | A.8.1 | Clause 5.3

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	Clause 5.1 a
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	A.8.1
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	Clause 7.3
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	Clause 5.3

NEW QUESTION: 223
CMM stands for?
A. Capable Mature Model
B. Capability Maturity Model
C. Capacity Maturity Matrix
D. Capability Maturity Matrix
Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
You are the audit team leader conducting a third-party audit of an online insurance organisation. During Stage
1, you found that the organisation took a very cautious risk approach and included all the information security controls in ISO/IEC 27001:2022 Appendix A in their Statement of Applicability.
During the Stage 2 audit, your audit team found that there was no evidence of the implementation of the three controls (5.3 Segregation of duties, 6.1 Screening, 7.12 Cabling security) shown in the extract from the Statement of Applicability. No risk treatment plan was found.

Control Reference	Objective	Control driven by			Applicable	Last Assessed	Justification if not applicable
		Business Risk	Legal requirement	Customer Contract			
5.3	Avoid conflicts of interest	Yes	No	No	Yes	02/202X	None
6.1	Screen personnel	Yes	No	Yes	Yes	02/202X	None
7.12	Cable protection	Yes	Yes	No	Yes	02/202X	None

Select three options for the actions you would expect the auditee to take in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:2022.
A. Allocate responsibility for producing evidence to prove to auditors that the controls are implemented.
B. Compile plans for the periodic assessment of the risks associated with the controls.
C. Implement the appropriate risk treatment for each of the applicable controls.
D. Incorporate written procedures for the controls into the organisation's Security Manual.
E. Remove the three controls from the Statement of Applicability.
F. Revise the relevant content in the Statement of Applicability to justify their exclusion.
G. Revisit the risk assessment process relating to the three controls.
H. Undertake a survey of customers to find out if the controls are needed by them.
Answer: C,F,G (LEAVE A REPLY)

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the auditee should take the following actions in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:20221:
* Implement the appropriate risk treatment for each of the applicable controls, as this is the main requirement of clause 6.1.3.e and the objective of the risk treatment process2.
* Revise the relevant content in the Statement of Applicability to justify their exclusion, as this is the expected output of the risk treatment process and the evidence of the risk-based decisions3.
* Revisit the risk assessment process relating to the three controls, as this is the input for the risk treatment process and the source of identifying the risks and the controls4.
The other options are not correct because:
* Allocating responsibility for producing evidence to prove to auditors that the controls are implemented is not a valid action, as the audit team already found that there was no evidence of the implementation of the three controls.
* Compiling plans for the periodic assessment of the risks associated with the controls is not a valid action, as this is part of the risk monitoring and review process, not the risk treatment process5.
* Incorporating written procedures for the controls into the organisation's Security Manual is not a valid action, as this is part of the documentation and operation of the ISMS, not the risk treatment process.
* Removing the three controls from the Statement of Applicability is not a valid action, as this is not a sufficient justification for their exclusion and does not reflect the risk treatment process.
* Undertaking a survey of customers to find out if the controls are needed by them is not a valid action, as this is not a relevant criterion for the risk assessment and treatment process, which should be based on the organisation's own context and objectives.
References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 36, section 4.5.22:
ISO/IEC 27001:2022, clause 6.1.3.e3: ISO/IEC 27001:2022, clause 6.1.3.f4: ISO/IEC 27001:2022, clause
6.1.25: ISO/IEC 27001:2022, clause 6.2. : ISO/IEC 27001:2022, clause 7.5 and 8. : ISO/IEC 27001:2022, clause 6.1.3.d. : ISO/IEC 27001:2022, clause 4.1 and 4.2.

NEW QUESTION: 225
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: 226
We can leave laptops during weekdays or weekends in locked bins.
A. True
B. False
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, clause A.11.2.9, the organization should protect mobile devices and media containing sensitive information from unauthorized access, loss or theft. The organization should also implement appropriate encryption techniques and backup procedures for such devices and media. Therefore, leaving laptops in locked bins during weekdays or weekends is not a secure practice, as it exposes them to potential theft or damage. Laptops should be stored in a safe location when not in use, such as a locked cabinet or drawer, and should be protected by passwords or biometric authentication. Reference: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course Handbook, page 58; [ISO/IEC 27001:2022], clause A.11.2.9.

NEW QUESTION: 227
----------is an asset like other important business assets has value to an organization and consequently needs to be protected.
A. Infrastructure
B. Data
C. Information

D. Security

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 228

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

A. Analysis

B. Sampling

C. Observation

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 229

What is a reason for the classification of information?

A. To provide clear identification tags

B. To structure the information according to its sensitivity

C. Creating a manual describing the BYOD policy

Answer: (SHOW ANSWER)

Explanation

The reason for the classification of information is to structure the information according to its sensitivity.

Information classification is a process of assigning categories or labels to information based on its value, sensitivity, criticality and legal requirements. Information classification helps to determine the appropriate level of security controls and handling procedures for different types of information. Information classification also facilitates the communication of information security requirements and expectations among internal and external parties. ISO/IEC 27001:2022 requires the organization to classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification (see clause A.8.2.1).

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 Data Classification?

NEW QUESTION: 230
Which of the options below presents a minor nonconformity?
A. The risk assessment methodology prevents evaluation of information security risks
B. The contract of the company with its supplier does not have the appropriate document version control
C. The backup of data is performed once a month, while the company's procedure requires daily backups
Answer: C (LEAVE A REPLY)
This is a minor nonconformity. The backup frequency not adhering to the company's procedure of daily backups but occurring once a month represents a deviation from established processes, yet it might not immediately impact the effectiveness of the information security management system.
References: ISO/IEC 27001:2013, Clause A.12.3 (Backup)

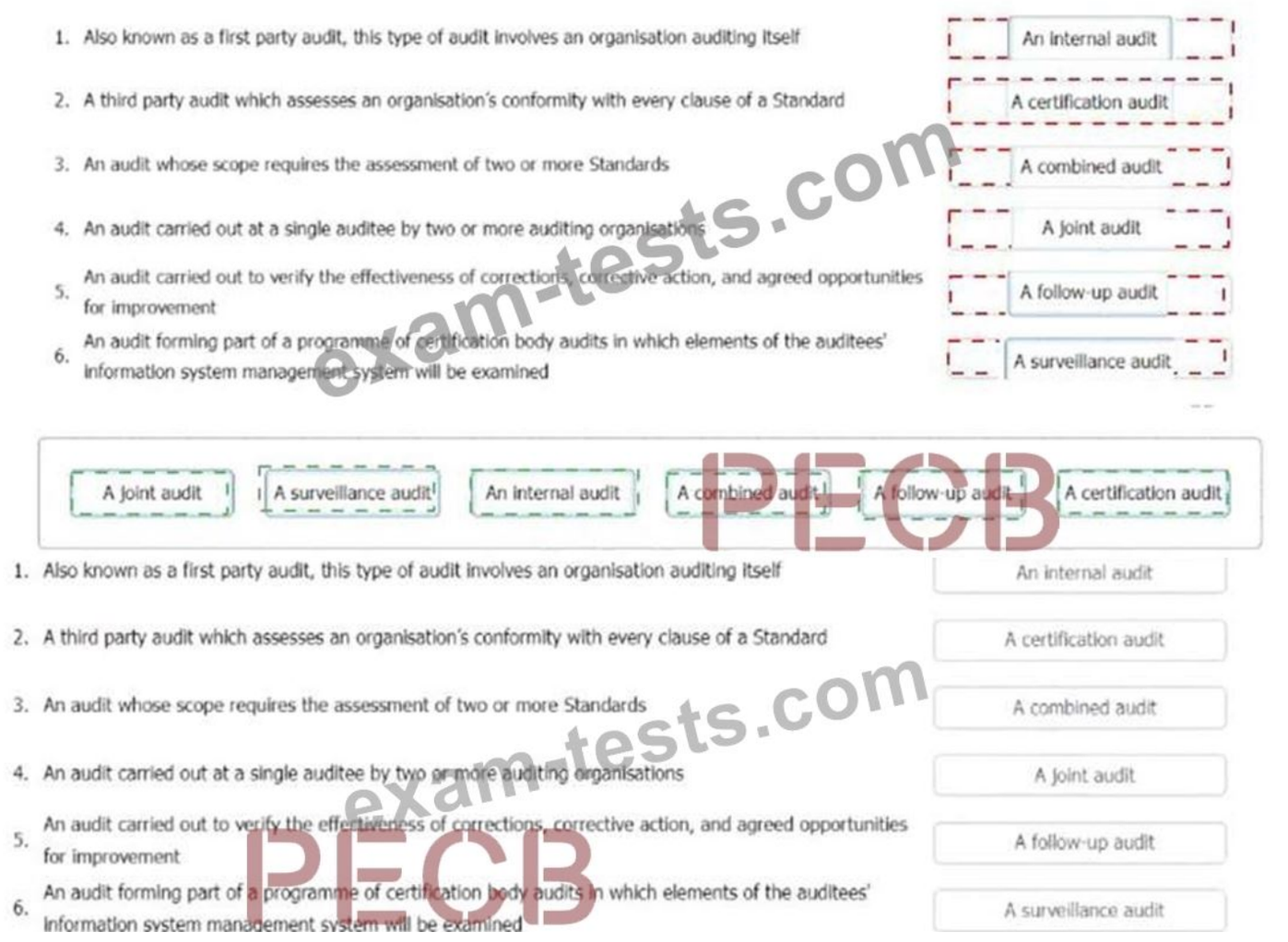
NEW QUESTION: 231
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.
You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.
To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.
Select three options for the audit evidence you need to find to verify the scope of the ISMS.
A. The auditee has identified the resident's needs and expectations on the facility and environmental safety
B. The auditee has ISO 9001 certification
C. The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling
D. The auditee has identified the resident's needs and expectations on how they should protect the resident's personal data
E. The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment
F. The auditee has identified the resident's needs and expectations on healthcare medical treatment services
G. The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located
H. The auditee is considering the purchase of a healthcare monitoring app from an external software company
Answer: C,D,G (LEAVE A REPLY)
According to ISO 27001:2022 clause 4.3, the organisation shall determine the scope of the information security management system (ISMS) by considering the internal and external issues,

the requirements of interested parties, and the interfaces and dependencies with other organisations12 In this case, the ISMS scope covers an outsourced data center that hosts the artificial intelligence (AI) cloud server for healthcare monitoring and analysis of the residents' data. Therefore, the audit evidence you need to find to verify the scope of the ISMS should include:
The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to comply with the relevant laws and regulations regarding the quality, safety, and privacy of healthcare services and patient data12 The auditee has identified the resident's needs and expectations on how they should protect the resident's personal data. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to ensure the confidentiality, integrity, and availability of the resident's personal data that is collected, processed, and stored by the electronic wristband and the AI cloud server12 The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located. This is an interface and dependency with another organisation that affects the ISMS scope, as the auditee has to control the externally provided processes, products, and services that are relevant to the ISMS, and to implement appropriate contractual requirements related to information security12 The following options are not relevant or sufficient for verifying the scope of the ISMS:
The auditee has identified the resident's needs and expectations on the facility and environmental safety.
This is an external issue and an interested party requirement, but it does not affect the ISMS scope, as it is not related to information security12 The auditee has ISO 9001 certification. This is an indication of the auditee's quality management system, but it does not verify the scope of the ISMS, as it is not related to information security12 The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment. These are external issues and interested party requirements, but they do not affect the ISMS scope, as they are not related to information security12 The auditee has identified the resident's needs and expectations on healthcare medical treatment services. These are external issues and interested party requirements, but they do not verify the scope of the ISMS, as they are not specific to information security12 The auditee is considering the purchase of a healthcare monitoring app from an external software company. This is a potential change that may affect the ISMS scope in the future, but it does not verify the current scope of the ISMS, as it is not yet implemented or controlled12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 232
You are an experienced ISMS audit team leader. An auditor in training has approached you to ask you to clarify the different types of audits she may be required to undertake.
Match the following audit types to the descriptions.

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

Answer:



NEW QUESTION: 233
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. Set up an access control procedure
B. Formulate a policy
C. Encrypt all sensitive information
D. Appoint security staff
Answer: B (LEAVE A REPLY)

NEW QUESTION: 234
Scenario 6: Sinvestment is an insurance company that offers home, commercial, and life insurance. The company was founded in North Carolina, but have recently expanded in other locations, including Europe and Africa.
Sinvestment is committed to complying with laws and regulations applicable to their industry and preventing any information security incident. They have implemented an ISMS based on ISO/IEC 27001 and have applied for ISO/IEC 27001 certification.
Two auditors were assigned by the certification body to conduct the audit. After signing a confidentiality agreement with Sinvestment. they started the audit activities. First, they reviewed the documentation required by the standard, including the declaration of the ISMS scope, information security policies, and internal audits reports. The review process was not easy because, although Sinvestment stated that they had a documentation procedure in place, not all documents had the same format.
Then, the audit team conducted several interviews with Sinvestment's top management to understand their role in the ISMS implementation. All activities of the stage 1 audit were performed remotely, except the review of documented information, which took place on-site, as requested by Sinvestment.
During this stage, the auditors found out that there was no documentation related to information security training and awareness program. When asked, Sinvestment's representatives stated that the company has provided information security training sessions to all employees. Stage 1 audit gave the audit team a general understanding of Sinvestment's operations and ISMS.
The stage 2 audit was conducted three weeks after stage 1 audit. The audit team observed that the marketing department (which was not included in the audit scope) had no procedures in place to control employees' access rights. Since controlling employees' access rights is one of the ISO/IEC 27001 requirements and was included in the information security policy of the company, the issue was included in the audit report. In addition, during stage 2 audit, the audit team observed that Sinvestment did not record logs of user activities.

The procedures of the company stated that "Logs recording user activities should be retained and regularly reviewed," yet the company did not present any evidence of the implementation of such procedure.

During all audit activities, the auditors used observation, interviews, documented information review, analysis, and technical verification to collect information and evidence. All the audit findings during stages 1 and 2 were analyzed and the audit team decided to issue a positive recommendation for certification.

Based on scenario 6, during stage 1 audit, the auditor found out that some documents regarding the ISMS had different format. What should the auditor do in this case?

A. Verify if the documented information has the appropriate format and is in accordance with the company's documentation procedure since this is a requirement of the standard

B. Verify only if the information required by the standard is documented without taking into account the format since this is not a requirement of the standard

C. Document this observation as an issue that should be verified during stage 2 audit

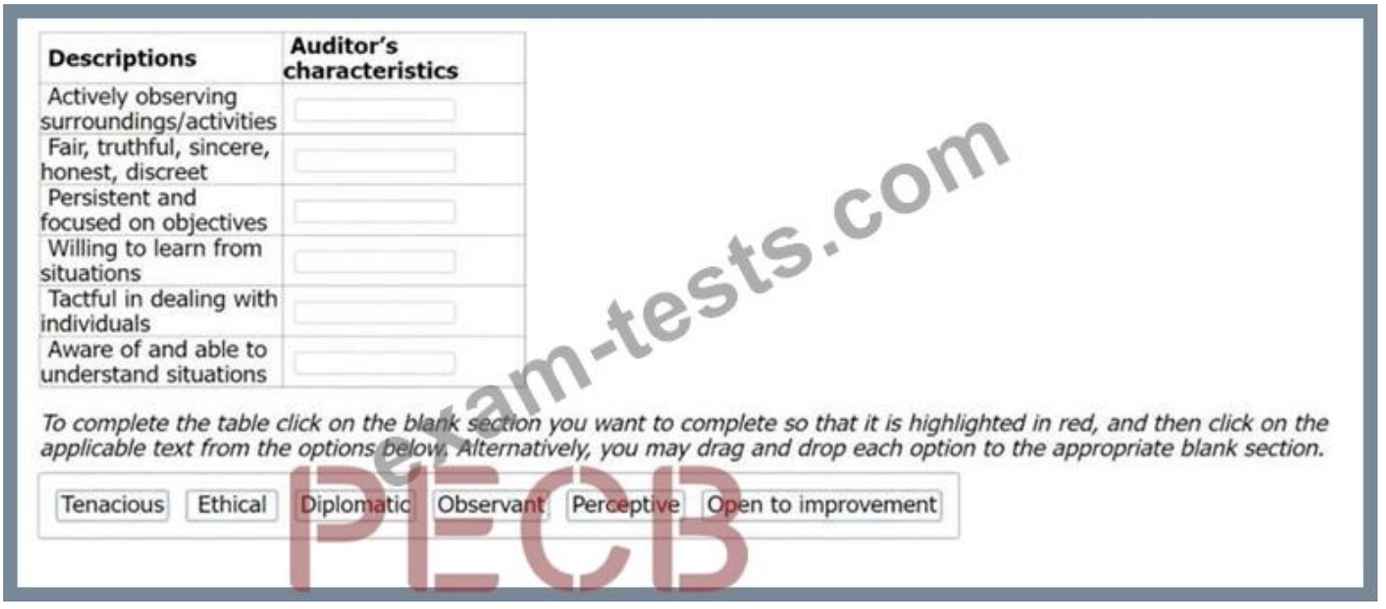
Answer: (SHOW ANSWER)

The auditor should verify if the information required by the standard is documented, without necessarily focusing on the format, as long as the content meets the requirements of the standard. ISO/IEC 27001 does not mandate a specific format for documentation, only that necessary information is appropriately documented, maintained, and controlled.

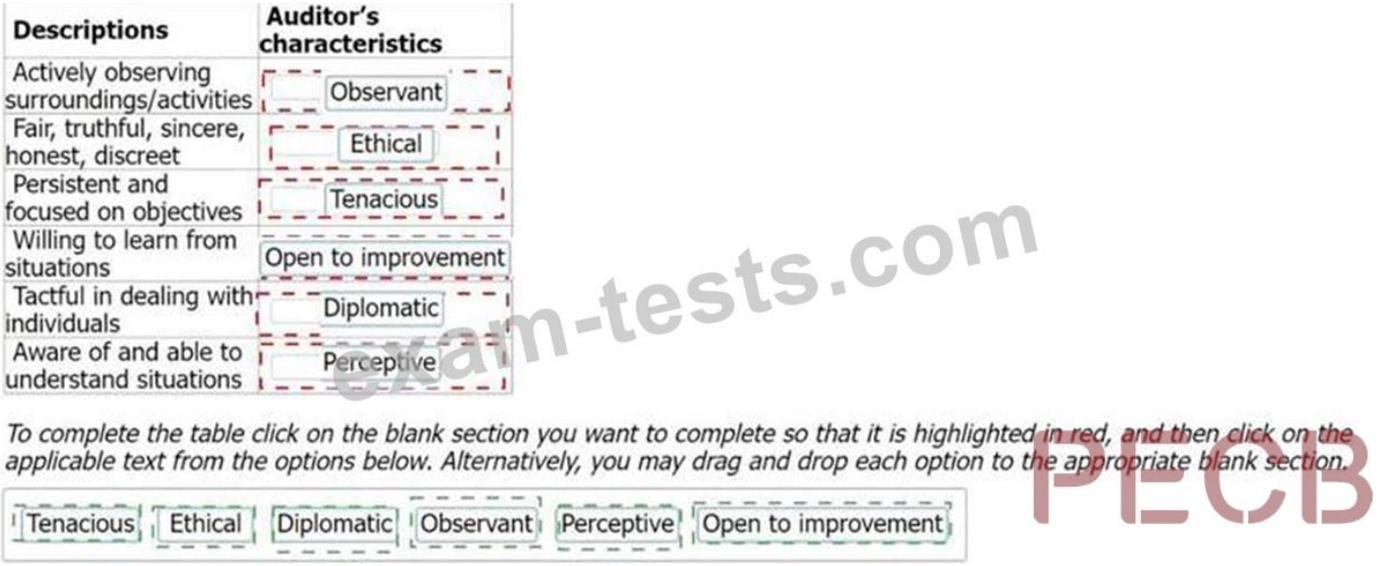
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

NEW QUESTION: 235

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.



Answer:



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: 236
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: (SHOW ANSWER)
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: 237
The following are purposes of Information Security, except:
A. Minimize Business Risk
B. Ensure Business Continuity
C. Maximize Return on Investment
D. Increase Business Assets
Answer: D (LEAVE A REPLY)

NEW QUESTION: 238

Which two activities align with the "Check" stage of the Plan-Do-Check-Act cycle when applied to the process of managing an internal audit program as described in ISO 19011?

A. Retains records of internal audits

B. Define audit criteria and scope for each internal audit

C. Update the internal audit programme

D. Establish a risk-based internal audit programme

E. Conduct internal audits

F. Verify effectiveness of the internal audit programme

G. Review trends in internal audit result

Answer: F,G (LEAVE A REPLY)

The Check stage of the PDCA cycle involves monitoring and measuring the performance of the process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines1. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer feedback1.
Reference: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 239

Below is Purpose of "Integrity", which is one of the Basic Components of Information Security

A. the property that information is not made available or disclosed to unauthorized individuals

B. the property of safeguarding the accuracy and completeness of assets.

C. the property that information is not made available or disclosed to unauthorized individuals

D. the property of being accessible and usable upon demand by an authorized entity.

Answer: (SHOW ANSWER)

NEW QUESTION: 240

In which order is an Information Security Management System set up?

A. Implementation, operation, maintenance, establishment

B. Implementation, operation, improvement, maintenance

C. Establishment, implementation, operation, maintenance

D. Establishment, operation, monitoring, improvement

Answer: C (LEAVE A REPLY)

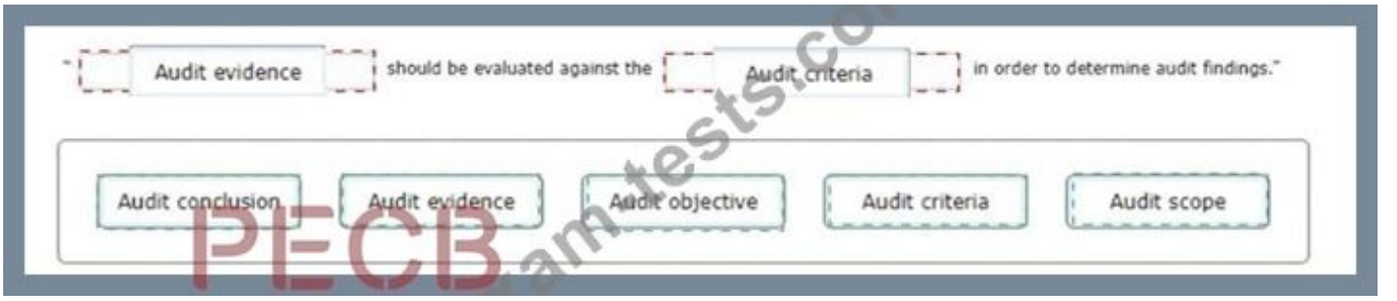
The establishment phase of an ISMS involves defining the scope, context, objectives, and leadership commitment for information security management within an organization. It also involves identifying and assessing the risks and opportunities related to information security and selecting the appropriate controls to treat them. The implementation phase of an ISMS involves executing the plans and actions to achieve the information security objectives and implement the selected controls. It also involves ensuring the availability of resources and competencies for information security management. The operation phase of an ISMS involves monitoring and

measuring the performance and effectiveness of the ISMS and reporting on the results. It also involves addressing nonconformities and taking corrective actions to prevent recurrence. The maintenance phase of an ISMS involves reviewing and evaluating the ISMS at planned intervals and identifying opportunities for improvement. It also involves updating the ISMS as necessary to reflect changes in the internal and external context of the organization. Therefore, an ISMS is set up in the following order: establishment, implementation, operation, maintenance. Reference: ISO/IEC 27001:2022, clauses 6-10; ISO/IEC 27000:2022, clause 4.

NEW QUESTION: 241
Integrity of data means
A. Accuracy and completeness of the data
B. Data should be viewable at all times
C. Data should be accessed by only the right people
Answer: (SHOW ANSWER)
Explanation
Integrity of data means accuracy and completeness of the data. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Data should be viewable at all times is not related to integrity, but to availability. Data should be accessed by only the right people is not related to integrity, but to confidentiality. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4.

NEW QUESTION: 242
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: 243

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: A,C,F,G (LEAVE A REPLY)
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: 244
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)
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. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 26. : ISO/IEC 27001 LEAD AUDITOR - PECB, page 13.

NEW QUESTION: 245
Four types of Data Classification (Choose two)
A. Restricted Data, Confidential Data
B. Project Data, Highly Confidential Data
C. Financial Data, Highly Confidential Data
D. Unrestricted Data, Highly Confidential Data
Answer: A,D (LEAVE A REPLY)
Explanation
Two types of data classification are restricted data and unrestricted data. Restricted data is data that has a high level of sensitivity or confidentiality, and requires strict protection from unauthorized access, disclosure, modification or destruction. Examples of restricted data include personal data, financial data, trade secrets, intellectual property, etc. Unrestricted data is data that has a low level of sensitivity or confidentiality, and can be freely accessed, disclosed, modified or destroyed without significant consequences. Examples of unrestricted data include public information, marketing materials, general news, etc. Data classification is a process of assigning categories or labels to data based on its value, sensitivity, criticality and legal requirements. Data classification helps to determine the appropriate level of security controls and handling procedures for different types of data. ISO/IEC 27001:2022 requires the organization to classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification (see clause A.8.2.1). 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 Data Classification?

NEW QUESTION: 246
Integrity of data means
A. Data should be accessed by only the right people

B. Data should be viewable at all times
C. Accuracy and completeness of the data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 247
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.
Your colleague seems unsure as to the difference between an information security event and an information security incident. You attempt to explain the difference by providing examples.
Which three of the following scenarios can be defined as information security incidents?
A. The organisation's malware protection software prevents a virus
B. A hard drive is used after its recommended replacement date
C. The organisation receives a phishing email
D. An employee fails to clear their desk at the end of their shift
E. A contractor who has not been paid deletes top management ICT accounts
F. An unhappy employee changes payroll records without permission
G. The organisation fails a third-party penetration test
H. The organisation's marketing data is copied by hackers and sold to a competitor
Answer: (SHOW ANSWER)
According to ISO/IEC 27000:2018, which provides an overview and vocabulary of information security management systems, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant1. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security1. Therefore, based on this definition, three examples of information security incidents are:
A contractor who has not been paid deletes top management ICT accounts: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of access, data, or functionality for the top management.
An unhappy employee changes payroll records without permission: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in financial fraud, legal liability, or reputational damage for the organization.
The organisation's marketing data is copied by hackers and sold to a competitor: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of confidentiality, competitive advantage, or customer trust for the organization.

The other options are not examples of information security incidents, but rather information security events that may or may not lead to incidents depending on their impact and severity. For example:
The organisation's malware protection software prevents a virus: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, as it is prevented by the malware protection software.
A hard drive is used after its recommended replacement date: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it fails or causes other problems.
The organisation receives a phishing email: This is an example of an identified occurrence of a network state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it is opened or responded to by the recipient.
An employee fails to clear their desk at the end of their shift: This is an example of an identified occurrence of a service state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the desk contains sensitive or confidential information that is accessed by unauthorized persons.
The organisation fails a third-party penetration test: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the penetration test reveals serious vulnerabilities that are exploited by malicious actors.

NEW QUESTION: 248
You are performing an ISMS audit at a residential nursing home that provides healthcare services and are reviewing the Software Code Management (SCM) system. You found a total of 10 user accounts on the SCM.
You confirm that one of the users, Scott, resigned 9-months
ago. The SCM System Administrator confirmed Scott's last check-out of the source code was found 1 month ago. He was using one of the uthorized desktops from the local network in a secure area.
You check with the user de-registration procedure which states "Managers have to make sure of deregistration of the user account and authorisation immediately from the relevant ICT system and/or equipment after resignation approval." There was no deregistration record for user Scott.
The IT Security Manager explains that Scott still comes back to the office every month after he resigned to provide support on source code maintenance. That's why his account on SCM still exists.

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 access controls are periodically reviewed to maintain security (Relevant to control A.5.35)
B. Collect more evidence on how the transition of Scott from full-time to part-time employment was managed (relevant to control A.6.5)
C. Collect more evidence from Scott's background verification checks performed by the human resource department under the new employment relationship. (Relevant to control A.6.1)
D. Collect more evidence of why Scott resigned and whether his re-engagement represents a conflict of interest. (relevant to control A.5.3)
E. Collect more evidence on how Scott can access the employee's desktop and local network. (Relevant to control A.5.15)
F. Collect more evidence on how Scott can access the secure area. (Relevant to control A.8.4)
G. Collect more evidence on how the organization pays for Scott's source code maintenance support service. (Relevant to control A.6.2)
H. Collect more evidence on where Scott kept the source code that he checked out and how it was secured.
(Relevant to control A.8.4)
Answer: B,D,G (LEAVE A REPLY)
Explanation
The options B, D, and G are not valid audit trails because they are not directly related to the ISMS requirements or the audit criteria. They are more relevant to the human resource management or the contractual arrangements of the organization, which are outside the scope of the ISMS audit. The other options are valid audit trails because they can provide evidence of how the organization implements and maintains the ISMS controls related to access control, secure areas, and information security aspects of business continuity management. References:
PECB Candidate Handbook ISO/IEC 27001 Lead Auditor, page 16, section 4.2.1 ISO/IEC 27001:2013, clauses A.5.3, A.5.15, A.5.35, A.6.1, A.6.2, A.6.5, A.8.4, A.17.1 ISO 19011:2018, clause 6.2.2

NEW QUESTION: 249
We can leave laptops during weekdays or weekends in locked bins.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation
According to ISO/IEC 27001:2022, clause A.11.2.9, the organization should protect mobile devices and media containing sensitive information from unauthorized access, loss or theft. The organization should also implement appropriate encryption techniques and backup procedures for such devices and media. Therefore, leaving laptops in locked bins during weekdays or weekends is not a secure practice, as it exposes them to potential theft or damage. Laptops should be

stored in a safe location when not in use, such as a locked cabinet or drawer, and should be protected by passwords or biometric authentication. References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course Handbook, page 58; [ISO/IEC 27001:2022], clause A.11.2.9.

NEW QUESTION: 250
Which of the following does a lack of adequate security controls represent?
A. Asset
B. Vulnerability
C. Impact
D. Threat
Answer: B (LEAVE A REPLY)
Explanation
A lack of adequate security controls represents a vulnerability, which is a weakness or flaw in an asset or its protection that can be exploited by a threat. A vulnerability can increase the likelihood or impact of a security incident, and therefore should be identified and treated as part of the risk management process. ISO/IEC
27001:2022 defines vulnerability as "the absence or weakness of a safeguard that could be exploited by a threat source" (see clause 3.49). 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: 251
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.
You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that he electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.
To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.
Select four options for the clauses and/or controls of ISO/IEC 27001:2022 that are directly relevant to the verification of the scope of the ISMS.
A. Control 5.3 Organizational roles, responsibilites and authorities
B. Clause 4.2 Understanding the needs and expectations of interested parties
C. Control 5.3 Legal, statutory, regulatory and contractual requirements
D. Control 6.3 Information security awareness, education, and training
E. Clause 5.2 Policy
F. Clause 4.1 Understanding the organization and its context
G. Control 7.6 Working in secure areas
H. Clause 4.3 Determining the scope of the information security management system

Answer: (SHOW ANSWER)

B. This clause requires the organisation to determine the interested parties that are relevant to the ISMS, and the requirements of these interested parties12. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to identify the stakeholders that have an influence or an interest in the information security of the organisation, such as customers, suppliers, regulators, employees, etc. The organisation should also consider the needs and expectations of these interested parties when defining the scope of the ISMS, and ensure that they are met and communicated.

E. This clause requires the organisation to establish an information security policy that provides the framework for setting the information security objectives and guiding the information security activities13. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to define the direction and principles of the ISMS, and to align them with the strategic goals and context of the organisation. The information security policy should also be consistent with the scope of the ISMS, and should be communicated and understood within the organisation and by relevant interested parties.

F. This clause requires the organisation to determine the internal and external issues that are relevant to the purpose and the context of the organisation, and that affect its ability to achieve the intended outcomes of the ISMS14. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to understand the factors and conditions that influence the information security of the organisation, such as the legal, technological, social, economic, environmental, etc. The organisation should also monitor and review these issues, and consider them when defining the scope of the ISMS.

H. This clause requires the organisation to determine the boundaries and applicability of the ISMS to establish its scope15. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to describe the information and processes that are included in the ISMS, and to document the scope in a clear and concise manner. The organisation should also consider the issues, requirements, and interfaces identified in clauses 4.1, 4.2, and 4.3 when determining the scope of the ISMS, and ensure that the scope is appropriate to the nature and scale of the organisation.

References:

1: PECB Candidate Handbook - ISO 27001 Lead Auditor, page 17 2: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause

4.2 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 5.2 4: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.1 5: ISO/IEC

27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.3

NEW QUESTION: 252

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.

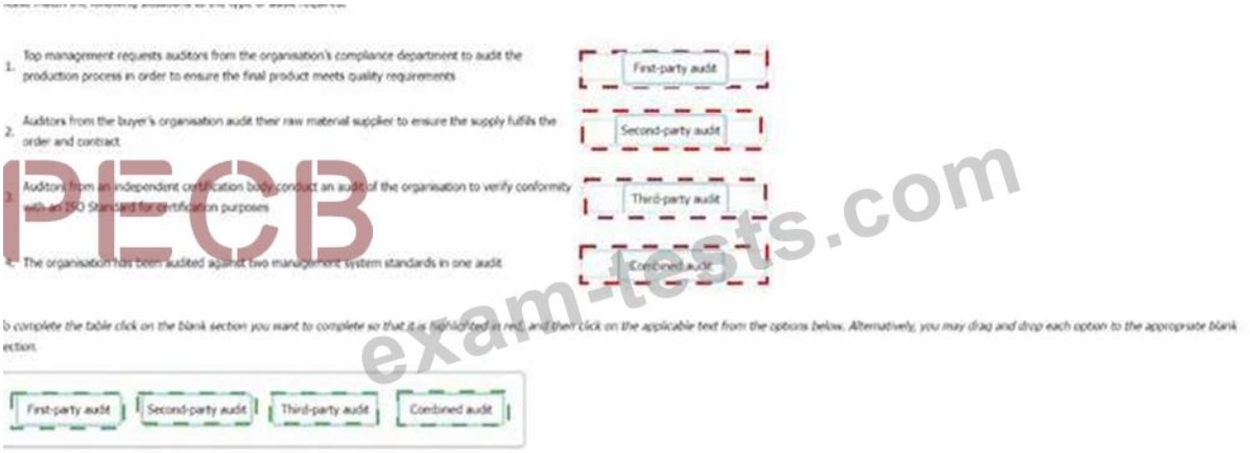
Answer:

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: 253

Please match the following situations to the type of audit required.

Answer:



Explanation:

* Top management requests auditors from the organisation's compliance department to audit the production process in order to ensure the final product meets quality requirements = First-party audit
* Auditors from the buyer's organisation audit their raw material supplier to ensure the supply fulfils the order and contract = Second-party audit
* Auditors from an independent certification body conduct an audit of the organisation to verify conformity with an ISO Standard for certification purposes = Third-party audit
* The organisation has been audited against two management system standards in one audit = Combined audit Explanation: According to the ISO/IEC 27001 standard, there are three main categories of audits: internal, external, and certification1. An internal audit, also known as a first-party audit, is an audit conducted by the organisation itself, or by an external party on its behalf, for management review and other internal purposes12. An external audit, also known as a second-party audit, is an audit conducted by a customer or other interested party on a supplier or contractor to verify compliance with contractual or other requirements12. A certification audit, also known as a third-party audit, is an audit conducted by an independent certification body to verify

conformity with an ISO standard for certification purposes12. A combined audit is an audit where two or more management system standards are audited together3.
References: 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, page 192: ISO 27001 Audit Types and How They are Conducted23: The Four ISO 27001 Audit Categories, Explained4

NEW QUESTION: 254
What type of system ensures a coherent Information Security organisation?
A. Federal Information Security Management Act (FISMA)
B. Information Technology Service Management System (ITSM)
C. Information Security Management System (ISMS)
D. Information Exchange Data System (IEDS)
Answer: C (LEAVE A REPLY)
Explanation
An Information Security Management System (ISMS) is a systematic approach to managing the security of information assets within an organization. It includes the policies, processes, and controls that address the risks and opportunities related to information security. An ISMS is based on the Plan-Do-Check-Act (PDCA) cycle, which consists of four phases: establishment, implementation, operation, and maintenance. Therefore, an ISMS is set up in the following order: establishment, implementation, operation, maintenance. References: ISO/IEC 27000:2022, clause 3.24; ISO/IEC 27001:2022, clause 4.

NEW QUESTION: 255
You are conducting a third-party surveillance audit when another member of the audit team approaches you seeking clarification. They have been asked to assess the organisation's application of control 5.7 - Threat Intelligence. They are aware that this is one of the new controls introduced in the 2022 edition of ISO/IEC
27001, and they want to make sure they audit the control correctly.
They have prepared a checklist to assist them with their audit and want you to confirm that their planned activities are aligned with the control's requirements.
Which three of the following options represent valid audit trails?
A. I will ensure that the task of producing threat intelligence is assigned to the organisation's internal audit team
B. I will ensure that the organisation's risk assessment process begins with effective threat intelligence
C. I will speak to top management to make sure all staff are aware of the importance of reporting threats
D. I will ensure that appropriate measures have been introduced to inform top management as to the effectiveness of current threat intelligence arrangements
E. I will check that the organisation has a fully documented threat intelligence process
F. I will check that threat intelligence is actively used to protect the confidentiality, integrity and availability of the organisation's information assets

G. I will review how information relating to information security threats is collected and evaluated to produce threat intelligence
H. I will determine whether internal and external sources of information are used in the production of threat intelligence
Answer: (SHOW ANSWER)
These three options represent valid audit trails for control 5.7, as they are aligned with the control's requirements and objectives. According to the web search results from my predefined tool, control 5.7 requires organisations to collect and analyse information relating to information security threats and use that information to take mitigation actions12. The control also specifies that threat intelligence should be relevant, perceptive, contextual, and actionable, and that it should be used to prevent, detect, or respond to threats34.
Therefore, the auditor should verify how the organisation collects, analyses, and produces threat intelligence, how it uses threat intelligence to protect its information assets, and how it monitors and evaluates the effectiveness of its threat intelligence arrangements. The other options are not valid audit trails, as they are either irrelevant, incorrect, or incomplete. For example:
*The task of producing threat intelligence is not assigned to the organisation's internal audit team, but to the person or team responsible for the ISMS, such as the information security manager or the information security committee5 .
*The organisation's risk assessment process does not begin with effective threat intelligence, but with the identification of the context, scope, and objectives of the ISMS . Threat intelligence is an input for the risk identification and analysis, but not the starting point of the risk assessment process.
*Speaking to top management to make sure all staff are aware of the importance of reporting threats is not sufficient to audit the control, as it does not address how the organisation collects, analyses, and produces threat intelligence, nor how it uses it to take mitigation actions. The auditor should also speak to the staff involved in the threat intelligence process, and review the relevant documents and records.
*Checking that the organisation has a fully documented threat intelligence process is not enough to audit the control, as it does not verify the implementation and effectiveness of the process. The auditor should also observe the process in action, and examine the outputs and outcomes of the process.
*Determining whether internal and external sources of information are used in the production of threat intelligence is a partial audit trail, as it only covers one aspect of the control. The auditor should also assess the quality, reliability, and relevance of the sources, and how the information is analysed and used.
References: = 1: ISO 27001:2022 Annex A 5.7 - Threat Intelligence - ISMS.online12: ISO 27001 Annex A
5.7 Threat Intelligence - High Table23: ISO/IEC 27001:2022 Information technology - Security techniques
- Information security management systems - Requirements, clause A.5.74: ISO 27002 Emphasizes Need For Threat Intelligence - Rapid745: ISO/IEC 27007:2011 Information

technology - Security techniques - Guidelines for information security management systems auditing, clause 6.3.2. : ISO 27001 Statement of Applicability [Updated 2024] - Sprinto3 : ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, clause 6.1.1. : ISO 27001 Requirement 6.1.1 - Actions to address risks and opportunities | ISMS.online1

NEW QUESTION: 256
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: (SHOW ANSWER)
Explanation
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: 257
Changes on project-managed applications or database should undergo the change control process as documented.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 258
All are prohibited in acceptable use of information assets, except:
A. Company-wide e-mails with supervisor/TL permission.
B. Messages with very large attachments or to a large number ofrecipients.

C. Electronic chain letters
D. E-mail copies to non-essential readers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
How is the purpose of information security policy best described?
A. An information security policy provides direction and support to the management regarding information security.
B. An information security policy provides insight into threats and the possible consequences.
C. An information security policy documents the analysis of risks and the search for countermeasures.
D. An information security policy makes the security plan concrete by providing it with the necessary details.
Answer: (SHOW ANSWER)

NEW QUESTION: 260
You are an ISMS auditor conducting a third-party surveillance audit of a telecom's provider. You are in the equipment staging room where network switches are pre-programmed before being despatched to clients. You note that recently there has been a significant increase in the number of switches failing their initial configuration test and being returned for reprogramming.
You ask the Chief Tester why and she says, 'It's a result of the recent ISMS upgrade'. Before the upgrade each technician had their own hard copy work instructions. Now, the eight members of my team have to share two laptops to access the clients' configuration instructions online. These delays put pressure on the technicians, resulting in more mistakes being made'.
Based solely on the information above, which clause of ISO/IEC 27001:2022 would be the most appropriate to raise a nonconformity against? Select one.
A. Clause 7.2 - Competence
B. Clause 8.1 - Operational planning and control
C. Clause 7.5 - Documented information
D. Clause 10.2 - Nonconformity and corrective action
Answer: B (LEAVE A REPLY)

NEW QUESTION: 261
What type of compliancy standard, regulation or legislation provides a code of practice for information security?
A. IT Service Management
B. Computer criminality act
C. Personal data protection act
D. ISO/IEC 27002
Answer: D (LEAVE A REPLY)

NEW QUESTION: 262
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits. Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.
The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.
Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months. Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.
Based on the scenario above, answer the following question:
The audit team photocopied the examined employee training records to support their conclusion. Should the audit team obtain an approval from Lawsy before taking this action? Refer to scenario 7.
A. Yes. the audit team should obtain the approval of the auditee when verifying the existence of a process in all cases, including when taking notes and photocopying documents

B. Yes, the audit team can photocopy documents observed during the audit if the auditee agrees to it
C. No, the audit team has the authority to photocopy documents in order to verify the conformity of a certain document to the audit criteria
Answer: B (LEAVE A REPLY)
Yes, the audit team should obtain approval from Lawsy before photocopying documents. This is a best practice to ensure that the auditee agrees to the duplication of documents, which might contain sensitive or confidential information. Although auditors can observe and note down information, copying documents typically requires explicit permission to maintain trust and ensure compliance with confidentiality agreements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 263
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: D (LEAVE A REPLY)
Explanation
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). 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 Identification?]

NEW QUESTION: 264
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: C,D (LEAVE A REPLY)

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:

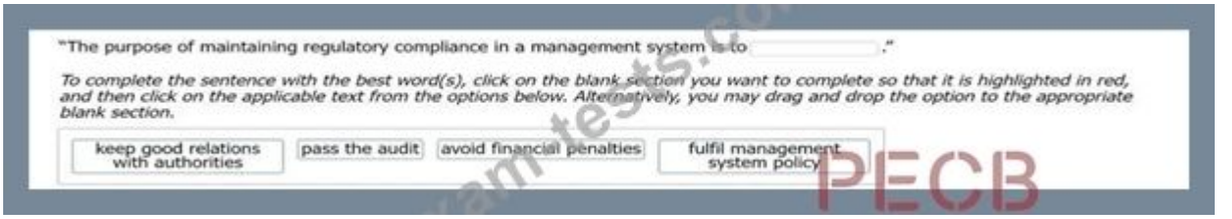
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 265

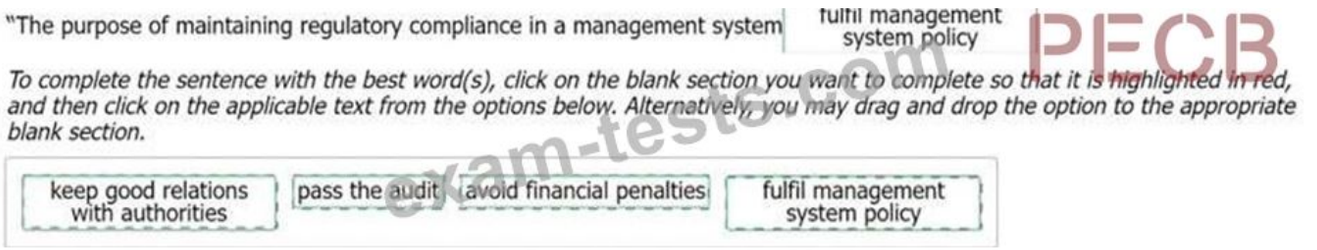
You are an experienced audit team leader conducting a third-party surveillance audit of an organisation that designs websites for its clients. You are currently reviewing the organisation's Statement of Applicability.
Based on the requirements of ISO/IEC 27001, which two of the following observations about the Statement of Applicability are true?
A. The Statement of Applicability is owned and amended by the organisation's top management
B. The Statement of Applicability must be reviewed at Management Review
C. Justification is only required for any controls that the organisations choses to exclude
D. Justification for both the inclusion and exclusion of Annex A controls in the Statement of Applicability is required
E. A Statement of Applicability must be produced by organisations seeking ISO/IEC 27001 conformity
F. The Statement of Applicability must be reviewed at least annually
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 266
The responsibilities of a---------- include facilitating audit activities, maintaining logistics, ensuring that health and safety policies are observed, and witnessing the audit process on behalf of the auditee.
A. Internal auditor
B. Observer
C. Guide
Answer: C (LEAVE A REPLY)
The responsibilities described fit those of a "guide." A guide in an audit context is typically someone from the auditee's organization who facilitates audit activities, manages logistics, ensures compliance with health and safety policies, and may also witness the audit process, assisting the audit team.
References: ISO 19011:2018, Guidelines for auditing management systems

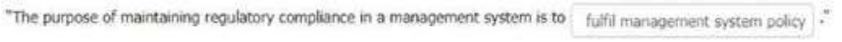
NEW QUESTION: 267
Select the words that best complete the sentence:
"The purpose of maintaining regulatory compliance in a management system is to To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.



Answer:



Explanation:



According to ISO 27001:2013, clause 5.2, the top management of an organization must establish, implement and maintain an information security policy that is appropriate to the purpose of the organization and provides a framework for setting information security objectives. The information security policy must also include a commitment to comply with the applicable legal, regulatory and contractual requirements, as well as any other requirements that the organization subscribes to. Therefore, maintaining regulatory compliance is part of fulfilling the management system policy and ensuring its effectiveness and suitability. References:

* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 5.2
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* ISO 27001 Policy: How to write it according to ISO 27001

NEW QUESTION: 268

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: 269
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. Appoint security staff
B. Encrypt all sensitive information
C. Formulate a policy
D. Set up an access control procedure
Answer: C (LEAVE A REPLY)
Explanation
An organisational measure is a measure that involves the establishment of policies, procedures, roles, responsibilities, and structures to manage information security within an organization. Examples of organisational measures include security policies, awareness programs, risk assessments, audits, and incident response plans. A policy is a statement of intent or direction that provides guidance for decision making and actions within an organization. A policy defines the scope, objectives, principles, and roles for information security management. Therefore, formulating a policy is the first step in a structured approach to come up with an organisational measure to protect laptop computers. References: ISO/IEC 27000:2022, clause 3.47; ISO/IEC 27001:2022, clause 5.2.

NEW QUESTION: 270
Which one of the following options best describes the main purpose of a Stage 1 third-party audit?
A. To introduce the audit team to the client
B. To learn about the organisation's procurement
C. To determine redness for a stage 2 audit
D. To check for legal compliance by the organisation
E. To prepare an independent audit report
F. To get to know the organisation's customers
Answer: (SHOW ANSWER)
The main purpose of a Stage 1 third-party audit is to determine readiness for a Stage 2 audit. A Stage 1 audit is a preliminary assessment that evaluates the organization's ISMS documentation, scope, context, and objectives, and identifies any major gaps or nonconformities that need to be addressed before the Stage 2 audit. A Stage 1 audit does not introduce the audit team to the client, as this is done during the audit planning phase. A Stage 1 audit does not check for legal compliance by the organization, as this is done during the Stage 2 audit. A Stage 1 audit does not

prepare an independent audit report, as this is done after the Stage 2 audit. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 70. : ISO/IEC 27001 LEAD AUDITOR - PECB, page 23.

NEW QUESTION: 271
Which four of the following statements about audit reports are true?
A. Audit reports should be produced by the audit team leader with input from the audit team
B. Audit reports should include or refer to the audit plan
C. Audit reports should be sent to the organisation's top management first because their contents could be embarrassing
D. Audit reports should be assumed suitable for general circulation unless they are specifically marked confidential
E. Audit reports should only evidence nonconformity
F. Audit reports should be produced within an agreed timescale
G. Audit reports that are no longer required can be destroyed as part of the organisation's general waste
H. Audit reports should always be reviewed by the client, dated, and signed as 'accepted'
Answer: A,B,F,H (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the audit reports should be produced by the audit team leader with input from the audit team, as they are responsible for collecting and analysing the audit evidence1. The audit reports should also include or refer to the audit plan, as it provides the basis for the audit objectives, scope, criteria, and methodology2. Furthermore, the audit reports should be produced within an agreed timescale, as it is part of the audit programme management and ensures timely communication of the audit results3. Additionally, the audit reports should always be reviewed by the client, dated, and signed as 'accepted', as it confirms the audit completion and the formal agreement on the audit findings and conclusions4.
The other statements are false because:
* Audit reports should not be sent to the organisation's top management first because their contents could be embarrassing, as this would compromise the audit impartiality and confidentiality5. Audit reports should be distributed according to the audit programme procedures and the audit plan.
* Audit reports should not be assumed suitable for general circulation unless they are specifically marked confidential, as this would violate the audit confidentiality and the protection of personal information.
Audit reports should be treated as confidential documents and only shared with the authorised parties.
* Audit reports should not only evidence nonconformity, as this would limit the audit scope and value.
Audit reports should also evidence conformity, improvement opportunities, good practices, and audit observations.

* Audit reports that are no longer required should not be destroyed as part of the organisation's general waste, as this would pose a risk to the audit confidentiality and the information security. Audit reports
* should be retained, disposed, or destroyed according to the audit programme procedures and the applicable legal requirements.
References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 32, section 4.4.32: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.43: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 31, section 4.4.14: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 34, section 4.4.55: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 32, section 4.4.3. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 33, section 4.4.4. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 24, section 4.3.1. : PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 34, section 4.4.5.

NEW QUESTION: 272
Which two of the following phrases would apply to "plan" in relation to the Plan-Do-Check-Act cycle for a business process?
A. Retaining documentation
B. Retaining documentation
C. Organising changes
D. Setting objectives
E. Training staff
F. Providing ICT assets
Answer: D,E (LEAVE A REPLY)
The Plan-Do-Check-Act (PDCA) cycle is a four-step method for implementing and improving processes, products, or services. The "plan" phase involves establishing the objectives and processes necessary to deliver the desired results. This may include setting SMART goals,

identifying resources, defining roles and responsibilities, conducting risk assessments, and developing plans for training, communication, and monitoring.
References:
* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB
* ISO 19011:2018 Guidelines for auditing management systems [Section 5.3.1]

NEW QUESTION: 273
Which option below about the ISMS scope is correct?
A. ISMS scope should be available as documented information
B. ISMS scope should ensure continual improvement
C. ISMS scope should be compatible with the strategic orientation of the organization
Answer: A (LEAVE A REPLY)
According to ISO/IEC 27001, the scope of an ISMS must be defined and documented. This documentation should include the boundaries and applicability of the information security management system, which helps in defining what information, locations, and assets are covered under the ISMS.
References: ISO/IEC 27001:2013 Standard, Clause 4.3 (Determining the scope of the information security management system)

NEW QUESTION: 274
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.
A. Confidentiality and nondisclosure agreements
B. How access to source code and development tools are managed
C. How power and data cables enter the building
D. How protection against malware is implemented
E. How the organisation evaluates its exposure to technical vulnerabilities
F. Information security awareness, education and training
G. The organisation's arrangements for information deletion
H. The organisation's business continuity arrangements
Answer: (SHOW ANSWER)
The four controls from the list that the auditor in training should review are:
*B. How access to source code and development tools are managed: This control requires the organisation to restrict and monitor the access to the source code and development tools that are used to create, modify, or maintain the software applications and systems that process or store the data of external clients. This is important for ensuring the integrity, confidentiality, and

availability of the software and the data, as well as for preventing unauthorized changes, errors, or malicious code injection.
*D. How protection against malware is implemented: This control requires the organisation to implement appropriate measures to detect, prevent, and remove malware from the IT systems and devices that process or store the data of external clients. This includes using antivirus software, firewalls, email filtering, web filtering, and other tools to protect against viruses, worms, ransomware, spyware, and other malicious software. This is essential for safeguarding the data and the systems from corruption, theft, or damage caused by malware.
*E. How the organisation evaluates its exposure to technical vulnerabilities: This control requires the organisation to identify and assess the technical vulnerabilities that may affect the IT systems and devices that process or store the data of external clients. This includes using vulnerability scanning tools, penetration testing tools, threat intelligence sources, and other methods to discover and evaluate the weaknesses and gaps in the security of the systems and the devices. This is necessary for prioritizing and implementing the appropriate corrective actions and controls to mitigate the risks posed by the vulnerabilities.
*G. The organisation's arrangements for information deletion: This control requires the organisation to establish and implement policies and procedures for deleting the data of external clients from the IT systems and devices when it is no longer needed or required. This includes defining the criteria and methods for data deletion, such as secure erasure, encryption, or physical destruction. This is important for complying with the contractual obligations and the legal and regulatory requirements regarding the retention and disposal of the data, as well as for protecting the confidentiality and integrity of the data.
References: = ISO/IEC 27001:2022, Annex A, clauses A.8.9, A.8.10, A.8.11, and A.8.28; Understanding ISO
27001:2022: People, process, and technology, pages 6-7; What are the 11 new security controls in ISO
27001:2022? - Advisera.

NEW QUESTION: 275
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.
Your colleague seems unsure as to the difference between an information security event and an information security incident. You attempt to explain the difference by providing examples.
Which three of the following scenarios can be defined as information security incidents?
A. The organisation's malware protection software prevents a virus
B. A hard drive is used after its recommended replacement date
C. The organisation receives a phishing email
D. An employee fails to clear their desk at the end of their shift
E. A contractor who has not been paid deletes top management ICT accounts
F. An unhappy employee changes payroll records without permission
G. The organisation fails a third-party penetration test

H. The organisation's marketing data is copied by hackers and sold to a competitor

Answer: E,F,H (LEAVE A REPLY)

According to ISO/IEC 27000:2018, which provides an overview and vocabulary of information security management systems, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant1. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security1. Therefore, based on this definition, three examples of information security incidents are:

* A contractor who has not been paid deletes top management ICT accounts: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of access, data, or functionality for the top management.
* An unhappy employee changes payroll records without permission: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in financial fraud, legal liability, or reputational damage for the organization.
* The organisation's marketing data is copied by hackers and sold to a competitor: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of confidentiality, competitive advantage, or customer trust for the organization.

The other options are not examples of information security incidents, but rather information security events that may or may not lead to incidents depending on their impact and severity. For example:

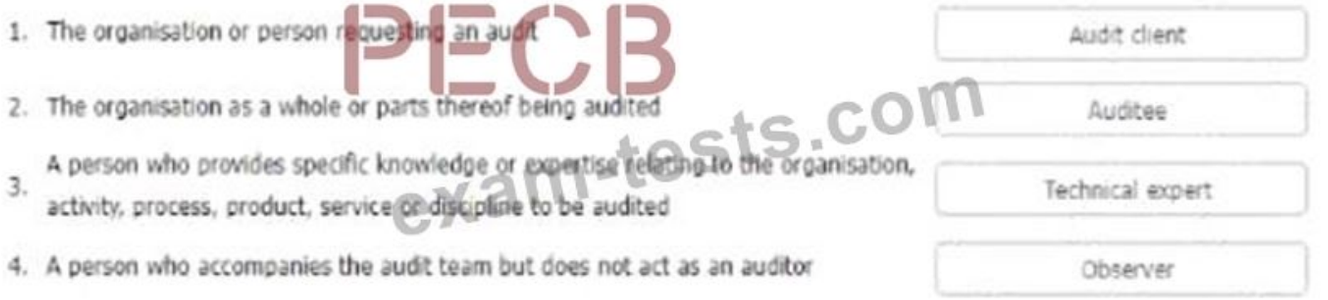
* The organisation's malware protection software prevents a virus: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, as it is prevented by the malware protection software.
* A hard drive is used after its recommended replacement date: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it fails or causes other problems.
* The organisation receives a phishing email: This is an example of an identified occurrence of a network state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it is opened or responded to by the recipient.
* An employee fails to clear their desk at the end of their shift: This is an example of an identified occurrence of a service state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations

and threatening information security, unless the desk contains sensitive or confidential information that is accessed by unauthorized persons.
* The organisation fails a third-party penetration test: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the penetration test reveals serious vulnerabilities that are exploited by malicious actors.
References: ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary

NEW QUESTION: 276
Please match the roles to the following descriptions:

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 test from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.
Answer:

Explanation



* The auditee is the organization or part of it that is subject to the audit. The auditee could be internal or external to the audit client . The auditee should cooperate with the audit team and provide them with access to relevant information, documents, records, personnel, and facilities .
* The audit client is the organization or person that requests an audit. The audit client could be internal or external to the auditee . The audit client should define the audit objectives, scope, criteria, and programme, and appoint the audit team leader .
* The technical expert is a person who provides specific knowledge or expertise relating to the organization, activity, process, product, service, or discipline to be audited. The technical expert could be internal or external to the audit team . The technical expert should support the audit team in collecting and evaluating audit evidence, but should not act as an auditor .
* The observer is a person who accompanies the audit team but does not act as an auditor. The observer could be internal or external to the audit team . The observer should observe the audit activities without interfering or influencing them, unless agreed otherwise by the audit team leader and the auditee .

References :=

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

NEW QUESTION: 277

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. Increase the length of the Stage 2 audit to include the extra sites

B. Obtain information about the additional sites to inform the certification body

C. Arrange to complete a remote Stage 1 audit of the two sites using a video conferencing platform

D. Inform the auditee that the request can be accepted but a full Stage 1 audit must be repeated

Answer: (SHOW ANSWER)

According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, a certification body should establish criteria for determining audit time and audit team composition based on factors such as the scope of certification, size

and complexity of the organization, risks associated with its activities, etc2. Therefore, if an auditee requests to extend the audit scope to include two additional sites after completing Stage 1 of an initial certification audit, the audit team leader should obtain information about the additional sites to inform the certification body, so that they can review and approve the change in scope and adjust the audit time and audit team accordingly2. The other options are not appropriate actions for the audit team leader to take in this situation. For example, increasing the length of the Stage 2 audit to include the extra sites without informing the certification body may violate their procedures and policies; arranging to complete a remote Stage 1 audit of the two sites using a video conferencing platform may not be feasible or effective depending on the nature and location of the sites; and informing the auditee that the request can be accepted but a full Stage 1 audit must be repeated may not be necessary or reasonable if there are no significant changes in the auditee's ISMS since Stage 12. References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

NEW QUESTION: 278
What is an example of a human threat?
A. a lightning strike
B. fire
C. phishing
D. thunderstrom
Answer: C (LEAVE A REPLY)
A human threat is a threat that originates from a person or a group of people who intentionally or unintentionally cause harm to an organization's information assets. Examples of human threats include hackers, insiders, terrorists, criminals, competitors, or disgruntled employees. A human threat can exploit technical, physical, or organizational vulnerabilities to compromise the confidentiality, integrity, or availability of information. Phishing is an example of a human threat that uses social engineering techniques to trick users into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Phishing attacks often involve sending fraudulent emails or messages that appear to be from legitimate sources, such as banks, government agencies, or trusted contacts. The messages may contain links to malicious websites or attachments that contain malware. Therefore, the correct answer is C. Reference: ISO/IEC 27000:2022, clause 3.25; What is Phishing? | How to Identify & Avoid Phishing Scams.

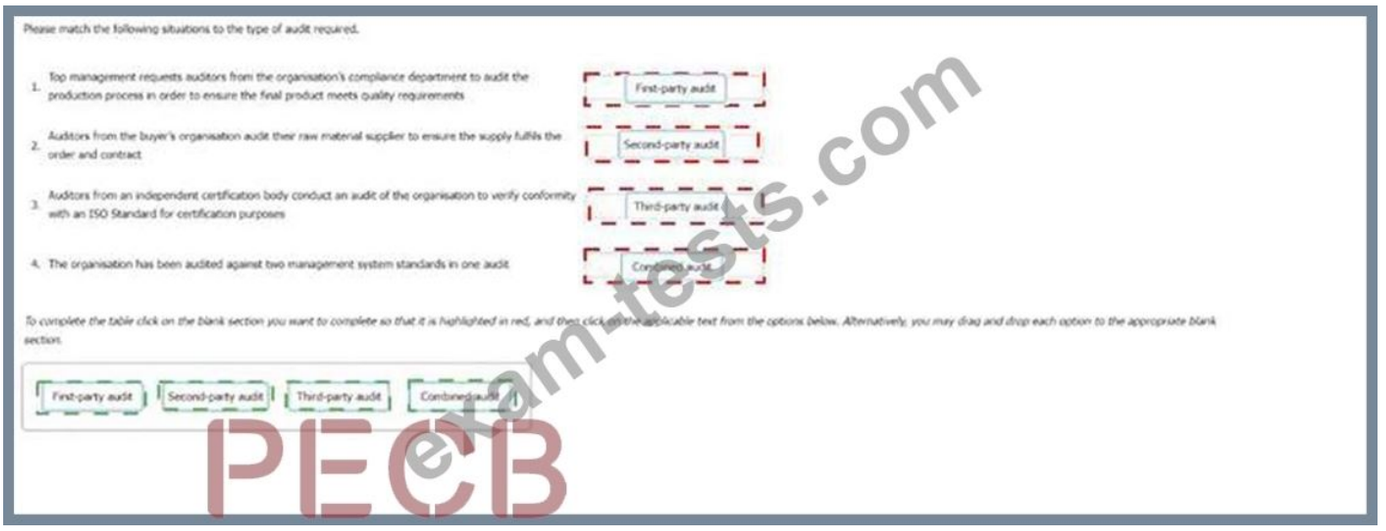
NEW QUESTION: 279
You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymization tests failed. Also, whether the Service Manager is authorized to approve the test.
The IT Manager explains the test results should be approved by him according to 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.
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: 280
Please match the following situations to the type of audit required.

Answer:



Explanation:

Top management requests auditors from the organisation's compliance department to audit the production process in order to ensure the final product meets quality requirements = First-party audit Auditors from the buyer's organisation audit their raw material supplier to ensure the supply fulfils the order and contract = Second-party audit Auditors from an independent certification body conduct an audit of the organisation to verify conformity with an ISO Standard for certification purposes = Third-party audit The organisation has been audited against two management system standards in one audit = Combined audit Explanation: According to the ISO/IEC 27001 standard, there are three main categories of audits: internal, external, and certification1. An internal audit, also known as a first-party audit, is an audit conducted by the organisation itself, or by an external party on its behalf, for management review and other internal purposes12. An external audit, also known as a second-party audit, is an audit conducted by a customer or other interested party on a supplier or contractor to verify compliance with contractual or other requirements12. A certification audit, also known as a third-party audit, is an audit conducted by an independent certification body to verify conformity with an ISO standard for certification purposes12. A combined audit is an audit where two or more management system standards are audited together3.

References: 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, page 192: ISO 27001 Audit Types and How They are Conducted23: The Four ISO 27001 Audit Categories, Explained4