PECB.ISO-IEC-27001-Lead-Auditor.v2024-08-02.q105

Exam Code:	ISO-IEC-27001-Lead-Auditor
Exam Name:	PECB Certified ISO/IEC 27001 Lead Auditor exam
Certification Provider:	PECB
Free Question Number:	105
Version:	v2024-08-02
# of views:	1050
# of Questions views:	1050
https://www.freepdfdumps.com/PECB.ISO-IEC-27001-Lead-Auditor.v2024-08-02.q105.html	

NEW QUESTION: 1
You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre.
Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.
Select four options for the actions you could take.
A. Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared
B. Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit
C. Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity
D. Note the progress made but hold the audit open until all corrective action has been cleared
E. Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified
F. Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity
G. Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale
H. Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised
Answer: (SHOW ANSWER)
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: 2

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)
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: 3
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: (SHOW ANSWER)
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. Reference: : 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: 4
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: 5
In acceptable use of Information Assets, which is the best practice?
A. Access to information and communication systems are provided for business purpose only
B. Interfering with or denying service to any user other than the employee's host
C. Playing any computer games during office hours
D. Accessing phone or network transmissions, including wireless or wifi transmissions
Answer: (SHOW ANSWER)
The best practice in acceptable use of information assets is A: access to information and communication systems are provided for business purpose only. This means that the organization grants access to its information and communication systems only to authorized users who need to use them for legitimate and approved business activities. The organization does not allow or tolerate any unauthorized, inappropriate or personal use of its information and communication systems, as this could compromise information security, violate policies or laws, or cause damage or harm to the organization or its stakeholders. The other options are not best practices in acceptable use of information assets, as they could violate information security policies and

procedures, as well as ethical or legal standards. Interfering with or denying service to any user other than the employee's host (B) is a malicious act that could disrupt the availability or performance of the information systems or services of another user or organization. Playing any computer games during office hours is a personal and unprofessional use of the information and communication systems that could distract the employee from their work duties, waste resources and bandwidth, or expose the systems to malware or other risks. Accessing phone or network transmissions, including wireless or wifi transmissions (D) is a potential breach of confidentiality or privacy that could intercept, monitor or modify the information transmitted by another user or organization without their consent or authorization. ISO/IEC 27001:2022 requires the organization to implement rules for acceptable use of assets (see clause A.8.1.3). 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 Acceptable Use?

NEW QUESTION: 6
You work in the office of a large company. You receive a call from a person claiming to be from the Helpdesk. He asks you for your password.
What kind of threat is this?
A. Natural threat
B. Organizational threat
C. Social Engineering
D. Arason
Answer: C (LEAVE A REPLY)
Explanation
This is an example of a social engineering threat, which is a type of human threat that involves manipulating or deceiving people into revealing confidential information, performing unauthorized actions, or compromising the security of information assets. Social engineering techniques can exploit the psychological, emotional, or behavioral vulnerabilities of people, such as trust, curiosity, fear, or greed. A person claiming to be from the Helpdesk and asking for your password is trying to trick you into giving away your credentials, which can be used to access your account or system without your authorization. Therefore, the correct answer is C. References: ISO/IEC 27000:2022, clause 3.25; What is Social Engineering? | Definition and Examples.

NEW QUESTION: 7
You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

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

Nonconformities (NCs)

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

signed by *Audit Team Leader*

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

A. Recommend certification immediately

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

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

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

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

Answer: D (LEAVE A REPLY)

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

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

Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:

Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO
19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.

Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC
17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.

Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.

Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.
References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 8
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: 9
The computer room is protected by a pass reader. Only the System Management department has a pass.
What type of security measure is this?
A. a corrective security measure
B. a physical security measure

C. a logical security measure
D. a repressive security measure
Answer: B (LEAVE A REPLY)
Explanation
A physical security measure is a measure that protects information and information processing facilities from physical threats and hazards, such as fire, flood, earthquake, theft, vandalism, etc. Physical security measures include locks, alarms, fences, cameras, fire extinguishers, ventilation systems, etc. The computer room is protected by a pass reader that only allows authorized personnel from the System Management department to access it. This is an example of a physical security measure, because it prevents unauthorized physical access to the computer room and its contents. ISO/IEC 27001:2022 requires the organization to implement physical and environmental security controls to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities (see clause A.11). 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 Physical Security?

NEW QUESTION: 10
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. Disagree with the raising of the minor nonconformity as appropriate action was taken at the earliest opportunity. Instead raise an opportunity for improvement.
B. Agree with the raising of a minor non-conformity but against control 5.15, not 5.18.
C. Disagree with the raising of the minor nonconformity, there is sufficient evidence to justify an escalation to a major non-conformity.
D. Agree with the raising of the minor non-conformity against 5.18.
E. Require additional audit evidence to be obtained before determining whether a non-conformity is appropriate.
F. Disagree with the raising of a minor conformity as appropriate action was taken at the earliest opportunity Take no further action.

Answer: (SHOW ANSWER)

NEW QUESTION: 11
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. Spoofing
D. Phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Changes on project-managed applications or database should undergo the change control process as documented.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
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: 14
There was a fire in a branch of the company Midwest Insurance. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost for good.
What is an example of the indirect damage caused by this fire?
A. Melted backup tapes
B. Burned computer systems
C. Burned documents
D. Water damage due to the fire extinguishers
Answer: D (LEAVE A REPLY)
An example of the indirect damage caused by the fire in the branch of Midwest Insurance is water damage due to the fire extinguishers. Indirect damage is the damage that occurs as a consequence of an incident, but not directly caused by it. Indirect damage can include loss of revenue, reputation, customers, market share, etc. In this case, the water damage due to the fire extinguishers is not directly caused by the fire itself, but by the actions taken to stop it. The water damage can affect other assets or information that were not burned by the fire, such as furniture, carpets, documents, etc. ISO/IEC 27001:2022 defines indirect impact as "impact resulting from consequences of an unwanted incident" (see clause 3.26). Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, [What is Indirect Damage?]

NEW QUESTION: 15
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: 16
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: (SHOW ANSWER)
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: 17
Which of the following is not a type of Information Security attack?
A. Legal Incidents
B. Vehicular Incidents
C. Technical Vulnerabilities
D. Privacy Incidents
Answer: B (LEAVE A REPLY)
Vehicular incidents are not a type of information security attack. A vehicular incident is an event that involves a vehicle or its driver causing damage or injury to people or property. A vehicular incident may have an impact on information security if it affects the availability or integrity of information or systems that are transported or accessed by vehicles, but it is not an intentional or malicious attack on information security. Legal incidents are a type of information security attack that involve legal actions or disputes that may compromise the confidentiality or integrity of information or systems. Technical vulnerabilities are a type of information security attack that exploit weaknesses or flaws in software or hardware that may compromise the confidentiality, integrity, or availability of information or systems. Privacy incidents are a type of information security attack that involve unauthorized access or disclosure of personal or sensitive information that may compromise the confidentiality or integrity of information or systems. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 25. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

NEW QUESTION: 18
Match the correct responsibility with each participant of a second-party audit:

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

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

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.

Audit Team Leader | Auditor in training | Auditor | Auditee | Guide | Observer

Answer:

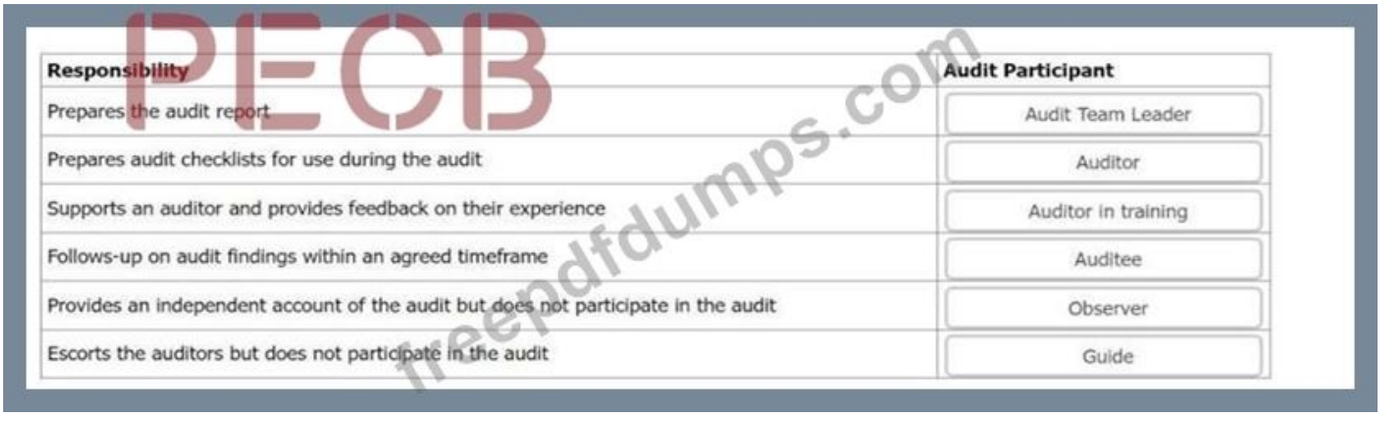
Match the correct responsibility with each participant of a second-party audit:

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

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.

Audit Team Leader | Auditor in training | Auditor | Auditee | Guide | Observer

Explanation:



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: 19
What is a repressive measure in case of a fire?
A. Taking out a fire insurance
B. Putting out a fire after it has been detected by a fire detector
C. Repairing damage caused by the fire
Answer: B (LEAVE A REPLY)
A repressive measure is a measure that aims to reduce or eliminate the impact of an incident after it has occurred. Putting out a fire after it has been detected by a fire detector is an example of a repressive measure, as it reduces the damage caused by the fire. Taking out a fire insurance is not a repressive measure, but a corrective measure, as it compensates for the loss after the incident. Repairing damage caused by the fire is also not a repressive measure, but a recovery measure, as it restores the normal operation after the incident. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 28. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 29. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 30.

NEW QUESTION: 20
Changes on project-managed applications or database should undergo the change control process as documented.
A. True

B. False

Answer: (SHOW ANSWER)

Explanation

Changes on project-managed applications or database should undergo the change control process as documented, because this is a requirement of ISO/IEC 27001:2022 clause 12.1.2, which states that "the organization shall define and apply a change management process for changes to systems and applications within the scope of the information security management system". The change management process should ensure that changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. 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: 21

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: 22
What is the goal of classification of information?
A. To create a manual about how to handle mobile devices
B. Applying labels making the information easier to recognize
C. Structuring information according to its sensitivity
Answer: C (LEAVE A REPLY)
The goal of classification of information is to structure information according to its sensitivity and value for the organization. Classification of information helps to determine the appropriate level of protection and handling for each type of information. Applying labels making the information easier to recognize is not the goal of classification, but a method of implementing classification. Creating a manual about how to handle mobile devices is not related to classification of information, but to information security policies and procedures. Reference: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 33. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 35. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36.

NEW QUESTION: 23
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?
A. Verification should focus on whether any action undertaken taken has been undertaken efficiently
B. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
C. Verification should focus on whether any action undertaken is complete
D. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
E. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
F. Verification should focus on whether any action undertaken has been undertaken effectively
Answer: C,F (LEAVE A REPLY)
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence. The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12

A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12
* Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12
* Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for
* improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 24

Which three of the following phrases are objectives' in relation to an audit?

A. International Standard

B. Identify opportunities for improvement

C. Confirm the scope of the management system

D. Management policy

E. Complete audit on time

F. Regulatory requirements

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

Explanation

According to ISO 19011:2018, which provides guidelines for auditing management systems, the audit objectives are defined by the audit client and may include determining the extent of conformity or nonconformity of the audited management system against the audit criteria, evaluating the ability of the audited management system to ensure that the organization meets applicable statutory, regulatory and contractual requirements, identifying potential improvement opportunities for the audited management system, and facilitating continual improvement of the audited management system1. Therefore, these three phrases are examples of objectives in relation to an audit. The other options are not objectives, but rather elements or factors that may influence or affect an audit. For example, an international standard is a source of audit criteria, a management policy is a part of the audited management system, and completing an audit on time is a requirement for an effective audit. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 25

Changes on project-managed applications or database should undergo the change control process as documented.

A. True

B. False

Answer: A (LEAVE A REPLY)

Changes on project-managed applications or database should undergo the change control process as documented, because this is a requirement of ISO/IEC 27001:2022 clause 12.1.2, which states that "the organization shall define and apply a change management process for changes to systems and applications within the scope of the information security management system". The change management process should ensure that changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. 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]

NEW QUESTION: 26

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)
Explanation
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. 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, ISO/IEC 27000 family - Information security management systems

NEW QUESTION: 27
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. Establish a risk-based internal audit programme
B. Update the internal audit programme
C. Retains records of internal audits
D. Review trends in internal audit result
E. Verify effectiveness of the internal audit programme
F. Define audit criteria and scope for each internal audit
G. Conduct internal audits
Answer: D,E (LEAVE A REPLY)
Explanation
The Check stage of the PDCA cycle involves monitoring and measuring the performance of the process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines1. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer feedback1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 28

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: 29
An administration office is going to determine the dangers to which it is exposed.
What do we call a possible event that can have a disruptive effect on the reliability of information?
A. dependency
B. threat
C. vulnerability
D. risk
Answer: B (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: 30
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: 31

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: (SHOW ANSWER)

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: 32

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)

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. 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. References: ISO/IEC 27000:2022, clause 3.8; Defining Security Principles - Pearson IT Certification.

NEW QUESTION: 33

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: 34
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. System restart
B. accidental alteration of data
C. a loose cable
D. private use of data
Answer: (SHOW ANSWER)

NEW QUESTION: 35
A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives.
What is not one of the four main objectives of a risk analysis?
A. Implementing counter measures
B. Determining relevant vulnerabilities and threats
C. Establishing a balance between the costs of an incident and the costs of a security measure
D. Identifying assets and their value
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
What is the goal of classification of information?
A. To create a manual about how to handle mobile devices
B. Applying labels making the information easier to recognize
C. Structuring information according to its sensitivity
Answer: C (LEAVE A REPLY)
Explanation
The goal of classification of information is to structure information according to its sensitivity and value for the organization. Classification of information helps to determine the appropriate level of protection and handling for each type of information. Applying labels making the information easier to recognize is not the goal of classification, but a method of implementing classification. Creating a manual about how to handle mobile devices is not related to classification of information, but to information security policies and procedures. References: : CQI & IRCA ISO

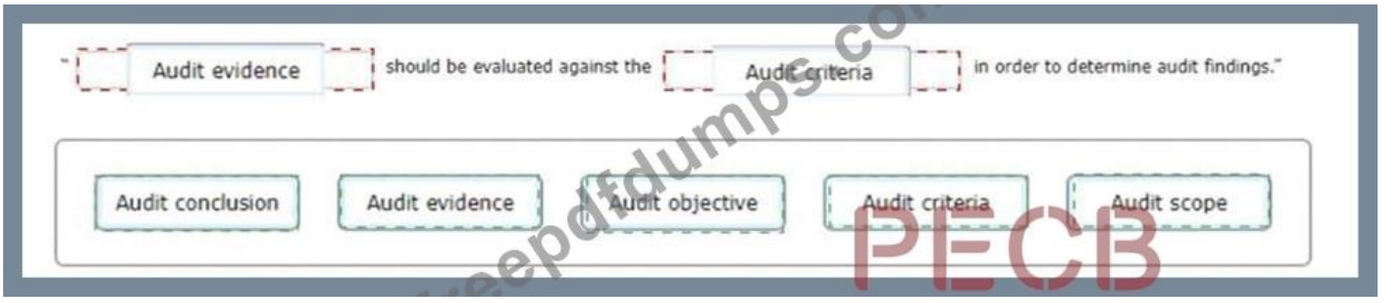
27001:2022 Lead Auditor Course Handbook, page 33. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 35. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36.

NEW QUESTION: 37

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: 38
Four types of Data Classification (Choose two)
A. Unrestricted Data, Highly Confidential Data
B. Project Data, Highly Confidential Data
C. Restricted Data, Confidential Data
D. Financial Data, Highly Confidential Data
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 39
Review the following statements and determine which two are false:
A. Conducting a technology check in advance of a virtual audit can improve the effectiveness and efficiency of the audit
B. During a virtual audit, auditees participating in interviews are strongly recommended to keep their webcam enabled
C. The number of days assigned to a third-party audit is determined by the auditee's availability
D. Due to confidentiality and security concerns, screen sharing during a virtual audit is one method by which the audit team can review the auditee's documentation
E. The selection of onsite, virtual or combination audits should take into consideration historical performance and previous audit results
F. Auditors approved for conducting onsite audits do not require additional training for virtual audits, as there are no significant differences in the skillset required
Answer: C,F (LEAVE A REPLY)
Explanation
The number of days assigned to a third-party audit is not determined by the auditee's availability, but by the audit program, which considers the audit scope, objectives, criteria, risks, and resources12. The auditee's availability is only one factor that affects the audit planning and scheduling, but not the audit duration3.
Auditors approved for conducting onsite audits do require additional training for virtual audits, as there are significant differences in the skillset required. Virtual audits pose different challenges and opportunities than onsite audits, such as communication, technology, security, and evidence collection4 . Auditors need to be familiar with the tools and techniques for conducting remote audits, as well as the ethical and professional behavior expected in a virtual environment .
References:
* PECB Candidate Handbook - ISO 27001 Lead Auditor, page 18
* ISO 19011:2018, Guidelines for auditing management systems, clause 5.3.2
* ISO 19011:2018, Guidelines for auditing management systems, clause 6.3.1
* Deloitte - Conducting a Virtual Internal Audit, page 1

* [A Guide to Conducting Effective and Efficient Remote Audits], page 1
* [ISO 19011:2018, Guidelines for auditing management systems], clause 7.2.3
* [Remote Auditing Best Practices & Checklist for Regulatory Compliance], page 1

NEW QUESTION: 40
You are the lead auditor of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks.
What is this risk strategy called?
A. Risk bearing
B. Risk avoidance
C. Risk neutral
D. Risk skipping
Answer: (SHOW ANSWER)
The risk strategy that involves taking measures for the large risks but not for the small risks is called risk bearing. Risk bearing is a strategy that accepts the existence of risks and their potential consequences without implementing any specific controls to reduce them. Risk bearing is usually applied to risks that have low likelihood and low impact, or when the cost of controls outweighs the benefits. Risk bearing implies that the organization has enough resources and resilience to cope with the risks if they materialize. ISO/IEC 27001:2022 defines risk acceptance as "decision to accept risk" (see clause 3.4). 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 Risk Bearing?]

NEW QUESTION: 41
Cabling Security is associated with Power, telecommunication and network cabling carrying information are protected from interception and damage.
A. True
B. False
Answer: (SHOW ANSWER)
Explanation
Cabling security is associated with power, telecommunication and network cabling carrying information are protected from interception and damage. This statement is true, as cabling security is a part of physical and environmental security that aims to prevent unauthorized physical access, damage and interference to information and information processing facilities. Cabling security involves securing the cables that transmit information from one device or location to another, such as power cables, telephone cables, network cables, etc. Cabling security can prevent eavesdropping, tampering, interruption or destruction of information by physical means, such as cutting, tapping, bending or exposing the cables. ISO/IEC 27001:2022 requires the organization to implement physical and environmental security controls to prevent unauthorized

physical access, damage and interference to the organization's information and information processing facilities (see clause A.11). 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 Cabling Security?

NEW QUESTION: 42
Select the option which best describes how Information Security Management System audits should be conducted:
A. Audit criteria should be used to assess circumstantial evidence in order to generate audit outcomes.
Then, the audit report should be created and presented to the audit team at the audit team meeting.
B. Audit criteria should be used to assess objective evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team leader at the closing meeting.
C. Audit methods should be used to assess audit evidence in order to generate audit recommendations.
Then, the audit recommendations should be created and presented to the auditee at the closing meeting.
D. Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
E. Audit objectives should be used to assess audit evidence in order to generate audit conclusions. Then, the audit findings should be created and presented to the audit client at the closing meeting.
F. Audit objectives should be used to assess objective evidence in order to generate audit conclusions.Then, the audit recommendations should be created and presented to top management at management review.
Answer: D (LEAVE A REPLY)
The option that best describes how Information Security Management System (ISMS) audits should be conducted, aligning with best practices and standards like ISO/IEC 27001:2022, is:
D: Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.

NEW QUESTION: 43
Changes to the information processing facilities shall be done in controlled manner.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
How are data and information related?

A. Data is a collection of structured and unstructured information
B. Information consists of facts and statistics collected together for reference or analysis
C. When meaning and value are assigned to data, it becomes information
Answer: C (LEAVE A REPLY)
Data and information are related concepts, but they are not the same. Data are simply facts or figures that represent raw facts or figures and form the basis of information. Information is data that has been given value through analysis, interpretation, or compilation in a meaningful form. When meaning and value are assigned to data, it becomes information that can be used for decision making, problem solving, or communication. Therefore, the correct answer is C.
Reference: ISO/IEC 27000:2022, clause 3.7; Data vs Information - Difference and Comparison | Diffen.

NEW QUESTION: 45
What type of legislation requires a proper controlled purchase process?
A. Intellectual property rights act
B. Computer criminality act
C. Government information act
D. Personal data protection act
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?
A. Verification should focus on whether any action undertaken taken has been undertaken efficiently
B. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
C. Verification should focus on whether any action undertaken is complete
D. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
E. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
F. Verification should focus on whether any action undertaken has been undertaken effectively
Answer: (SHOW ANSWER)
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and

correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence. The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12 Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12 Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 47
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)
Explanation
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). 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 Integrity?

NEW QUESTION: 48
Finnco, a subsidiary of a certification body, provided ISMS consultancy services to an organization.
Considering this scenario, when can the certification body certify the organization?
A. There is no time constraint in such a situation
B. At no time, since it presents a conflict of interest
C. If a minimum period of two years has passed since the last consulting activities
Answer: (SHOW ANSWER)
A certification body cannot certify an organization if it has provided consultancy services to that organization.
This situation presents a conflict of interest, as the certification body is required to maintain impartiality and objectivity. The ISO/IEC 17021-1 standard, which sets out requirements for

bodies providing audit and certification of management systems, specifies that providing both services to the same client is incompatible.
References: ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems

NEW QUESTION: 49
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)
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). 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

NEW QUESTION: 50
Which reliability aspect of information is compromised when a staff member denies having sent a message?
A. Confidentiality
B. Integrity
C. Availability
D. Correctness
Answer: B (LEAVE A REPLY)
The reliability aspect of information that is compromised when a staff member denies having sent a message is integrity. Integrity is the property of information that ensures its accuracy, completeness, consistency and authenticity. When a staff member denies having sent a message, it implies that the message was either altered, forged, deleted or repudiated by someone else, which violates the integrity of the information. ISO/IEC 27001:2022 defines integrity as "the 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: 51

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

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

The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymisation functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You are preparing the audit findings. Select the correct option.
A. There is a nonconformity (NC). The organisation and developer perform security tests that fail. (Relevant to clause 8.1, control A.8.29)
B. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
C. There is NO nonconformity (NC). The Service Manager makes a good decision to continue the service.
(Relevant to clause 8.1, control A.8.30)

D. There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.
(Relevant to clause 8.1, control A.8.29)
Answer: (SHOW ANSWER)

NEW QUESTION: 52
A management system audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit criteria are a set of requirements that may include policies, procedures, standards, regulations, etc. The purpose of a management system audit is to evaluate the performance of an organisation's management system in terms of its effectiveness, efficiency, compliance, and improvement. A management system audit can also identify strengths, weaknesses, opportunities, and risks of the management system and provide recommendations for improvement.
When preparing for an audit, which of the following statements is false?
A. The audit plan may be changed during the audit
B. The audit plan is shared with the auditee in advance of the audit
C. Each auditor creates their own audit checklist for use during the audit
D. The audit checklists are shared and agreed with the auditee in advance of the audit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?
A. Verification should focus on whether any action undertaken taken has been undertaken efficiently
B. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
C. Verification should focus on whether any action undertaken is complete
D. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
E. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
F. Verification should focus on whether any action undertaken has been undertaken effectively
Answer: (SHOW ANSWER)
Explanation
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the

organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence. The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:

* Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12
* Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes,
* but it is not a requirement of ISO 27001:2022. The auditor should focus on the effectiveness and completeness of the actions, not on the efficiency12
* Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to

review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 54
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: 55
Information or data that are classified as _____ do not require labeling.
A. Public
B. Internal
C. Confidential
D. Highly Confidential
Answer: A (LEAVE A REPLY)
Information or data that are classified as public do not require labeling. Public information or data are those that are intended for general disclosure and have no impact on the organization's operations or reputation if disclosed. Labeling is a method of implementing classification, which is a process of structuring information according to its sensitivity and value for the organization. Labeling helps to identify the level of protection and handling required for each type of information. Information or data that are classified as internal, confidential, or highly confidential require labeling, as they contain information that is not suitable for public disclosure and may cause harm or loss to the organization if disclosed. 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
What is an example of a human threat?

A. fire
B. thunderstrom
C. phishing
D. a lightning strike
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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: 58
You are performing an ISMS audit at a residential nursing home (ABC) that provides healthcare services. The next step in your audit plan is to verify the information security of ABC's healthcare mobile app development, support, and lifecycle process.
During the audit, you learned the
organization outsourced the mobile app development to a professional software development company with CMMI Level 5, ITSM (ISO/IEC
20000-1), BCMS (ISO 22301) and ISMS (ISO/IEC 27001) certified.
The IT Manager presented the software security management procedure and summarised the process as following:
The mobile app development shall adopt "security-by-design" and "security-by-default" principles, as a minimum. The following security functions for personal data protection shall be available: Access control.
Personal data encryption, i.e., Advanced Encryption Standard (AES) algorithm, key lengths: 256 bits; and Personal data pseudonymization.
Vulnerability checked and no security backdoor
You sample the latest Mobile App Test report, details as follows:

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

You ask the IT Manager why the organisation still uses the mobile app while personal data encryption and pseudonymisation tests failed. Also, whether the Service Manager is authorised to approve the test.
The IT Manager explains the test results should be approved by him according to the software security management procedure.
The reason why the encryption and pseudonymisation functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You are preparing the audit findings. Select the correct option.
A. There is NO nonconformity (NC). The Service Manager makes a good decision to continue the service.
(Relevant to clause 8.1, control A.8.30)

B. There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.
(Relevant to clause 8.1, control A.8.29)
C. There is a nonconformity (NC). The organisation and developer perform security tests that fail.
(Relevant to clause 8.1, control A.8.29)
D. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30)
Answer: (SHOW ANSWER)
Explanation
C: This statement is true because the organisation and the developer have not met the requirements of clause 8.1, control A.8.29, which states that the organisation should ensure that information security is an integral part of information systems across the entire lifecycle, and that information security requirements should be identified and agreed prior to the development or acquisition of information systems12. The organisation and the developer have performed security tests that fail to meet the security requirements that were defined in the software security management procedure, such as personal data encryption and pseudonymization. This indicates that the information security controls are not effective and that the information systems are not compliant with the ISMS. The organisation and the developer should take corrective actions to resolve the nonconformity and to prevent its recurrence.
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, Annex A, control A.8.29

NEW QUESTION: 59
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: A,C (LEAVE A REPLY)
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: 60
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: 61
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)

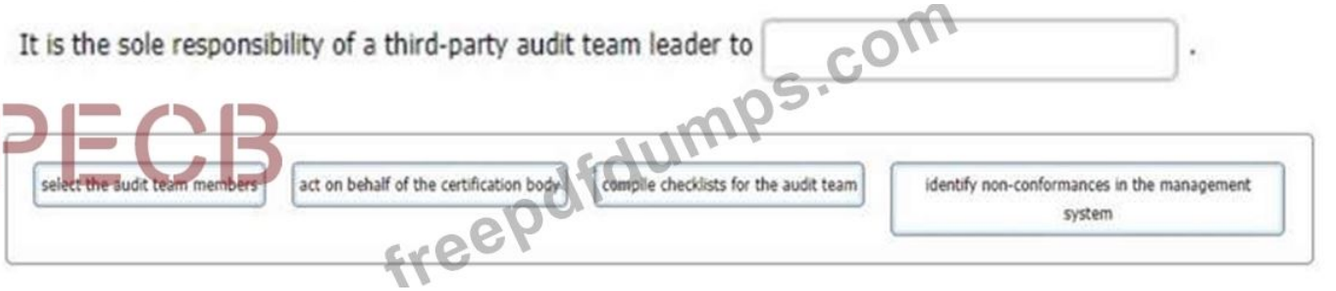
The difference between a restricted and confidential document is that a restricted document is to be shared among named individuals, while a confidential document is to be shared among an authorized group. Restricted and confidential are examples of information classification levels that indicate the 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). 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 Information Classification?

NEW QUESTION: 62
What is a definition of compliance?
A. An official or authoritative instruction
B. A rule or directive made and maintained by an authority.
C. The state or fact of according with or meeting rules or standards
D. Laws, considered collectively or the process of making or enacting laws
Answer: C (LEAVE A REPLY)

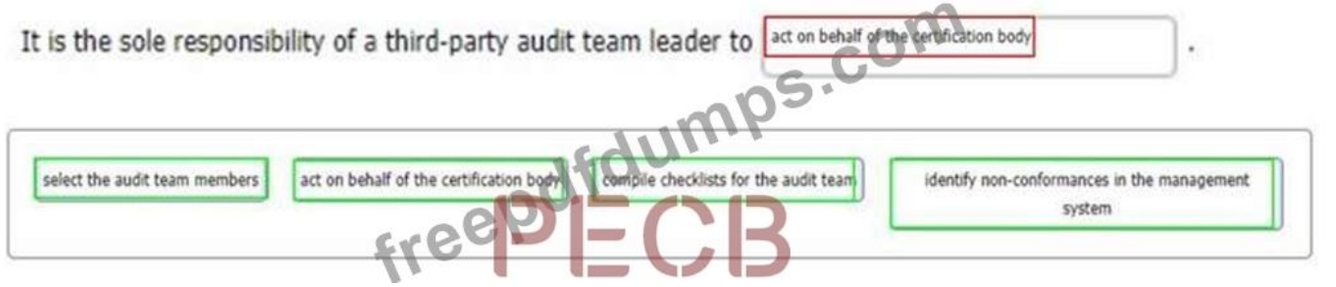
NEW QUESTION: 63
The auditor should consider (1)-------when determining the (2)--------
A. (1) Standard requirements. (2) audit criteria
B. (1) Audit risks, (2) audit objectives
C. (1) Penalties related to legal noncompliance, (2) materiality
Answer: B (LEAVE A REPLY)

The auditor should consider "audit risks" when determining the "audit objectives." Understanding the risks associated with the audit helps define the objectives clearly, ensuring that the audit focuses on the most significant areas of concern, aligns with the audit scope, and adequately addresses the risks identified.
References: ISO 19011:2018, Guidelines for auditing management systems

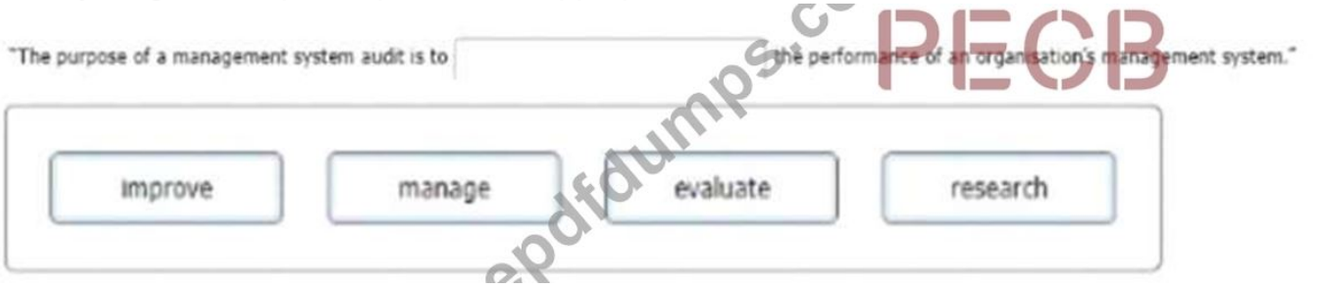
NEW QUESTION: 64
Select the words that best complete the sentence:
To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.



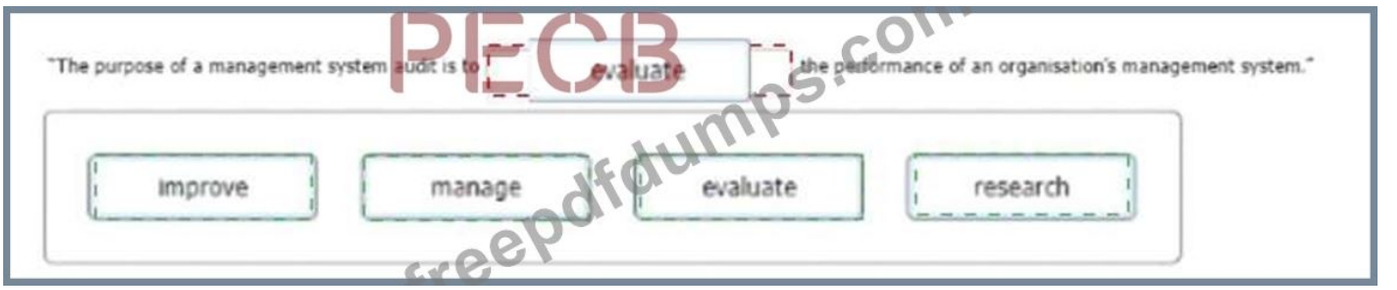
Answer:



NEW QUESTION: 65
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: 66

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: A,C,E,G (LEAVE A REPLY)
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: 67
PayBell, a finance corporation, is using an accounting software to track financial transactions. The software can be accessed from anywhere with an internet connection. It also enables PayBell's employees to easily collaborate with each other to ensure accurate financial reporting. What type of services is PayBell using?
A. Artificial intelligence
B. Cloud computing
C. Machine learning
Answer: (SHOW ANSWER)

NEW QUESTION: 68

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

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

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

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

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

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

*Are firewall-related controls implemented?

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

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

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

Based on this scenario, answer the following question:

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: 69
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. Restricted Mail
C. Public Mail
D. Confidential Mail
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
A property of Information that has the ability to prove occurrence of a claimed event.
A. Electronic chain letters
B. Integrity
C. Availability
D. Accessibility
Answer: B (LEAVE A REPLY)
A property of information that has the ability to prove occurrence of a claimed event is integrity. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events.
Integrity also implies that information and systems can be verified and validated as authentic and accurate.
Electronic chain letters are not a property of information, but a type of spam or hoax message that may contain malicious or misleading content. Availability means that service should be accessible at the required time and usable only by the authorized entity. Accessibility is not a property of information, but a characteristic of usability that refers to how easy it is for users to access and interact with information and systems. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC
27001 Brochures | PECB], page 4. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

NEW QUESTION: 71
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: 72
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: 73

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)

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: 74
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits. Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.
The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.
Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months. Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.

Based on the scenario above, answer the following question:
Based on scenario 7, what should Lawsy do prior to the initiation of stage 2 audit?
A. Perform a quality review of audit findings from stage 1 audit
B. Define which audit test plans can be combined to verify compliance
C. Review and confirm the audit plan with the certification body
Answer: C (LEAVE A REPLY)
Prior to the initiation of stage 2 audit, Lawsy should review and confirm the audit plan with the certification body. This ensures that both parties agree on the objectives, scope, and procedures for the stage 2 audit, thus aligning expectations and facilitating a smoother audit process.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 75
Which six of the following actions are the individual(s) managing the audit programme responsible for?
A. Selecting the audit team
B. Retaining documented information of the audit results
C. Defining the objectives, scope and criteria for an individual audit
D. Defining the plan of an individual audit
E. Establishing the extent of the audit programme
F. Establishing the audit programme
G. Determining the resources necessary for the audit programme
H. Communicating with the auditee during the audit
Answer: A,B,C,D,E,F (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, an audit programme is a set of one or more audits planned for a specific time frame and directed towards a specific purpose1. The individual(s) managing the audit programme are responsible for establishing, implementing and maintaining the audit programme in accordance with the organization's policies and objectives1. This includes defining the extent of the audit programme based on strategic direction, risks and opportunities; establishing the audit programme by defining its objectives, scope and criteria; determining the resources necessary for the audit programme; selecting competent auditors and assigning them to appropriate audits; defining the objectives, scope and criteria for each individual audit; defining the plan of each individual audit; retaining documented information of the audit results; reviewing and improving the performance of the audit programme1. Therefore, these six actions are part of the responsibilities of the individual(s) managing the audit programme. The other option, communicating with the auditee during the audit, is not a responsibility of the individual(s) managing the audit programme, but rather a responsibility of the audit team leader1. Reference: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 76
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: 77
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: 78
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: B,D (LEAVE A REPLY)
Explanation
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: 79
In which order is an Information Security Management System set up?

A. Establishment, operation, monitoring, improvement
B. Implementation, operation, improvement, maintenance
C. Establishment, implementation, operation, maintenance
D. Implementation, operation, maintenance, establishment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
You are preparing the audit findings. Select two options that are correct.
A. There is an opportunity for improvement (OFI). The iLiirmation security incident training effectiveness can be improved. This is relevant to clause 7.2 and control A.6.3.
B. There is no nonconformance. The information security weaknesses, events, and incidents are reported.
This conforms with clause 9.1 and control A.5.24.
C. There is no nonconformance. The information security handling training has performed, and its effectiveness was evaluated. This conforms with clause 7.2 and control A.6.3.
D. There is a nonconformity (NC). Based on sampling interview results, none of the interviewees were able to describe the incident management procedure reporting process including the role and responsibilities of personnel. This is not conforming with clause 9.1 and control A.5.24.
E. There is a nonconformity (NC). The information security incident training has failed. This is not conforming with clause 7.2 and control A.6.3.
F. There is an opportunity for improvement (OFI). The information security weaknesses, events, and madents are reported. This is relevant to clause 9.1 and control A.5.24.
Answer: A,D (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 7.2 requires an organization to determine the necessary competence of persons doing work under its control that affects its ISMS performance, and to provide training or take other actions to acquire or maintain the necessary competence1. Control A.6.3 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 respect2. Therefore, if an ISMS auditor finds that the information security incident training effectiveness can be improved, this indicates an opportunity for improvement (OFI) that is relevant to clause 7.2 and control A.6.3.
According to ISO/IEC 27001:2022, clause 9.1 requires an organization to monitor, measure, analyze and evaluate its ISMS performance and effectiveness1. Control A.5.24 requires an organization to define and apply procedures for reporting information security events and weaknesses2. Therefore, if an ISMS auditor finds that based on sampling interview results, none of the interviewees were able to describe the incident management procedure reporting process including the role and responsibilities of personnel, this indicates a nonconformity (NC) that is not conforming with clause 9.1 and control A.5.24.

The other options are not correct options for preparing the audit findings based on the given information. For example, there is no nonconformance if the information security weaknesses, events, and incidents are reported, as this conforms with clause 9.1 and control A.5.24; there is no nonconformance if the information security handling training has performed, and its effectiveness was evaluated, as this conforms with clause 7.2 and control A.6.3; there is no nonconformity if the information security incident training has failed, as this may not necessarily indicate a lack of conformity with clause 7.2 or control A.6.3; there is no opportunity for improvement if the information security weaknesses, events, and incidents are reported, as this is already conforming with clause 9.1 and control A.5.24. 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: 81
You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

Cosmic Certifications Limited

Summary of audit findings:

Opportunities for Improvement (OI)

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

Nonconformities (NCs)

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

signed by *Audit Team Leader*

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

A. Recommend certification immediately

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

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

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

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

Answer: (SHOW ANSWER)

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

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

* Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:20222. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:

* Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO

19011:20182, which provides guidelines for auditing management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.
* Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC
17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.
* Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.
* Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.
References: ISO/IEC 17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 82
A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.
Where in the incident cycle is moving to a stand-by arrangements found?
A. between threat and incident
B. between recovery and threat
C. between damage and recovery
D. between incident and damage
Answer: (SHOW ANSWER)
Moving to a stand-by arrangement is found between incident and damage in the incident cycle. The incident cycle is a model that describes the phases of an incident from its occurrence to its

resolution. The incident cycle consists of four phases: threat, incident, damage, and recovery1. A threat is a potential cause or source of harm to an organization's information assets or systems. An incident is an event that compromises the confidentiality, integrity, or availability of information assets or systems. Damage is the negative impact or consequence of an incident on the organization's assets, operations, reputation, or legal obligations. Recovery is the process of restoring normal service and operations after an incident and preventing recurrence2. Moving to a stand-by arrangement is a form of contingency plan that enables the organization to continue its critical activities in an alternative location or mode after an incident. This measure is taken before the damage caused by the incident is fully assessed or contained. Therefore, moving to a stand-by arrangement is found between incident and damage in the incident cycle. Reference: [ISO/IEC 27031:2011], clause 4.2; [ISO/IEC 27035:2016], clause 4.

NEW QUESTION: 83
Select two of the following options that are the responsibility of a legal technical expert on the audit team during a certification audit.
A. Evaluating the auditee's legal knowledge
B. Criticising the organisation's legal compliance issues
C. Debating complex legal points with the auditee
D. Advising on legal checkpoints for the audit team
E. Verifying the legal status of the organisation
F. Meeting the organisation's legal representative
Answer: D,E (LEAVE A REPLY)
Explanation
A legal technical expert (LTE) is a person who provides specific knowledge or expertise related to the legal aspects of the information security management system (ISMS) during a certification audit. The LTE is not an auditor, but a member of the audit team who supports the auditors in collecting and evaluating the audit evidence. The LTE is not responsible for evaluating the auditee's legal knowledge, criticising the organisation's legal compliance issues, or debating complex legal points with the auditee, as these tasks may be beyond the scope of the audit, or may compromise the objectivity and impartiality of the audit. The LTE is responsible for advising on legal checkpoints for the audit team, such as the applicable legal, regulatory, and contractual requirements, the relevant sources of information, the methods of verification, and the criteria of evaluation. The LTE is also responsible for verifying the legal status of the organisation, such as the registration, licensing, authorisation, or accreditation of the organisation, and the compliance with the relevant laws and regulations. References:
What is the role of a technical expert in ISO audit?
Roles, Responsibilities & Authorities for ISO 27001 5.3
Guide to Become an ISO 27001 Lead Auditor

NEW QUESTION: 84
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: 85
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)
Explanation
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

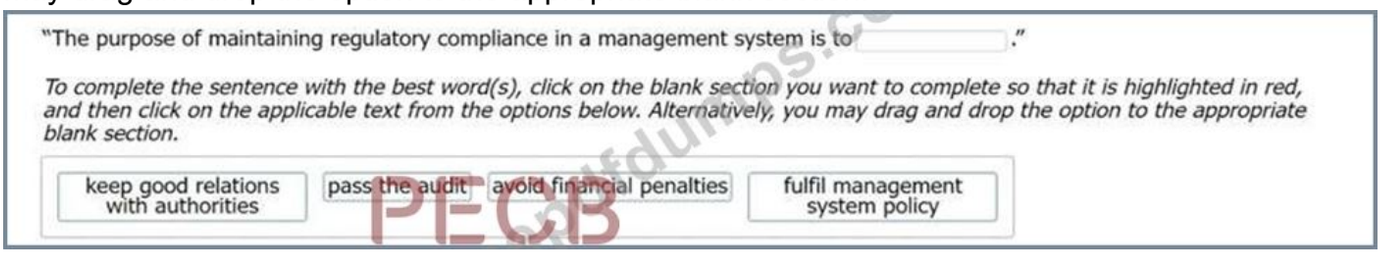
NEW QUESTION: 86
You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.

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 one option of the correct statement which defines the content of the scope of the ISMS.
A. The ISMS scope should not cover external service providers because they can have compliance difficulties with the information security policy and requirements
B. The ISMS scope should take any information security issues that have occurred and any interested parties' requirements into consideration
C. The most likely ISMS scope is to cover the IT department and the outsourced data centre
D. The organisation should only follow the government's recommendation, i.e., legal and legislation to define the ISMS scope
Answer: (SHOW ANSWER)
The correct statement which defines the content of the scope of the ISMS is that the ISMS scope should take any information security issues that have occurred and any interested parties' requirements into consideration.
According to ISO/IEC 27001:2022, the scope of the ISMS should be determined by considering the internal and external issues, the requirements and expectations of interested parties, the interfaces and dependencies between the organisation and other parties, and the information security risks. The scope of the ISMS should also be aligned with the strategic direction of the organisation and be appropriate to its purpose and context.
The scope of the ISMS should not be limited by the government's recommendation, nor exclude external service providers, nor be based on a single department or function, unless these are justified by the risk assessment and the needs and expectations of interested parties.
References: = ISO/IEC 27001:2022, clause
4.3; PECB Candidate Handbook ISO 27001 Lead Auditor, page 15; ISO 27001 scope statement | How to set the scope of your ISMS - Advisera.

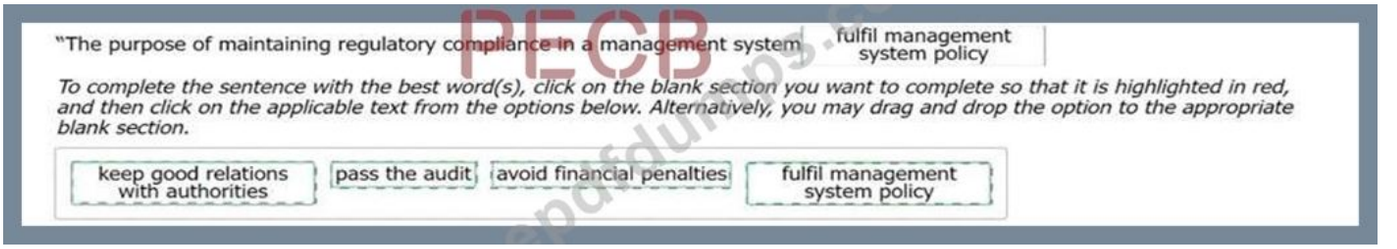
NEW QUESTION: 87
You are an experienced ISMS audit team leader. You are providing an introduction to ISO/IEC 27001:2022 to a class of Quality Management System Auditors who are seeking to retrain to enable them to carry out information security management system audits.
You ask them which of the following characteristics of information does an information security management system seek to preserve?
Which three answers should they provide?
A. Clarity
B. Accessibility
C. Completeness
D. Importance

E. Availability
F. Confidentiality
G. Integrity
H. Efficiency
Answer: (SHOW ANSWER)
Explanation
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

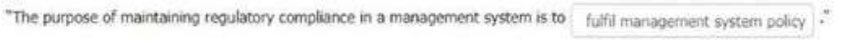
NEW QUESTION: 88
Select the words that best complete the sentence:
"The purpose of maintaining regulatory compliance in a management system is to To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable 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: 89

Why do we need to test a disaster recovery plan regularly, and keep it up to date?

A. Otherwise the measures taken and the incident procedures planned may not be adequate

B. Otherwise it is no longer up to date with the registration of daily occurring faults

C. Otherwise remotely stored backups may no longer be available to the security team

Answer: A (LEAVE A REPLY)

Explanation

Testing a disaster recovery plan regularly and keeping it up to date is essential to ensure that the measures taken and the incident procedures planned are adequate and effective in the event of a disaster6. A disaster recovery plan is a documented set of actions and arrangements to enable an organization to respond to a disaster affecting its information assets and resume its critical activities within a defined time frame7.

However, a disaster recovery plan may become obsolete or ineffective due to changes in the organization's environment, operations, risks, or resources. Therefore, testing the plan periodically and updating it accordingly is necessary to verify its validity, feasibility, completeness, and accuracy6. References: ISO/IEC 27031:2011, clauses 7.4 and 8.3; ISO/IEC 27000:2022, clause 3.11.

NEW QUESTION: 90

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: (SHOW ANSWER)

Explanation

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).

References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Phishing?

NEW QUESTION: 91

You work in the office of a large company. You receive a call from a person claiming to be from the Helpdesk. He asks you for your password.

What kind of threat is this?

A. Arason

B. Organizational threat

C. Natural threat

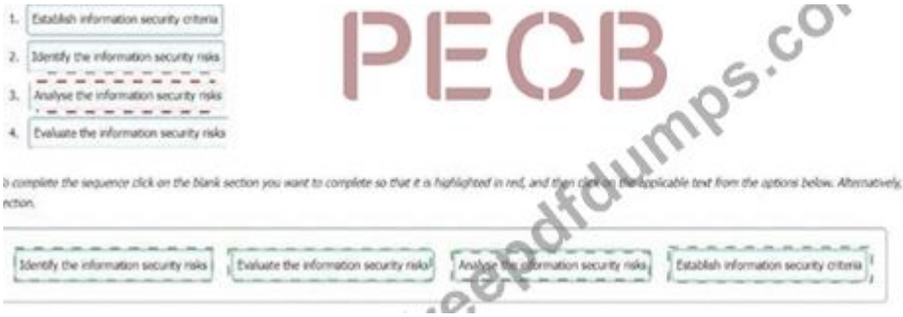
D. Social Engineering

Answer: D (LEAVE A REPLY)

NEW QUESTION: 92

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

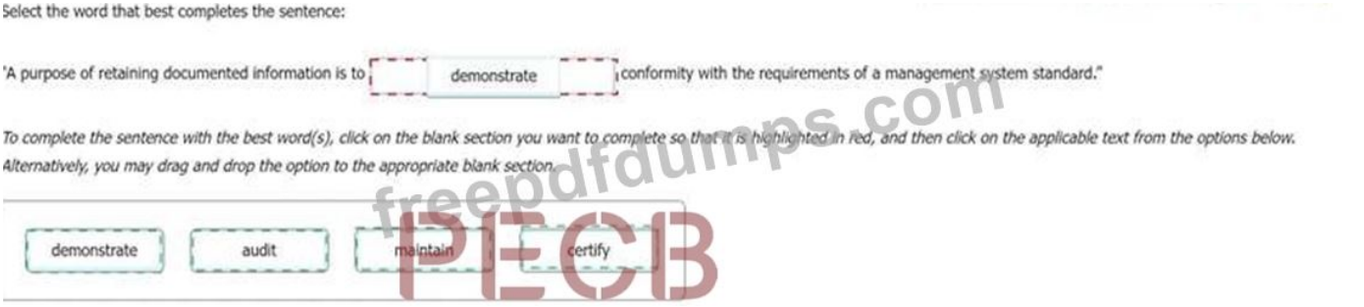
According to ISO 27001:2022, the standard for information security management systems (ISMS), the correct sequence for the information security risk assessment process is as follows:

* 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: 93
Select the word that best completes the sentence:

Answer:



Explanation:

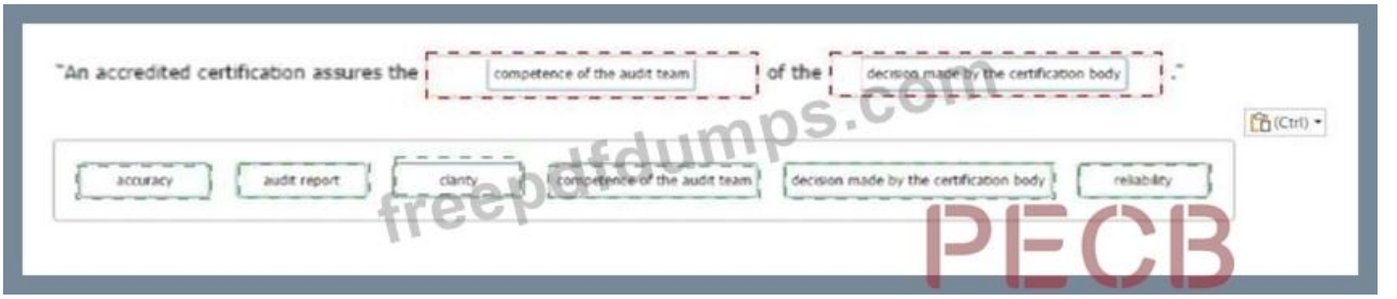
The word that best completes the sentence is "demonstrate". According to ISO/IEC 27001:2022, Clause 7.5, the organization shall retain documented information as evidence of the performance of the processes and the conformity of the products and services with the requirements1. The

purpose of retaining documented information is to demonstrate conformity with the requirements of the management system standard, not to maintain, audit, or certify it. References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 7.5

NEW QUESTION: 94
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)
Explanation
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: 95
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:

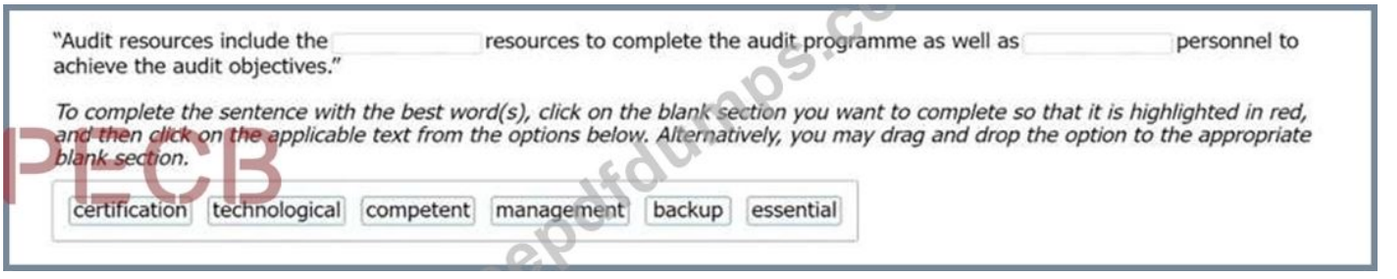


Explanation:
competence of the audit team and decision made by the certification body According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, an accredited certification means that the certification body has been evaluated by 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

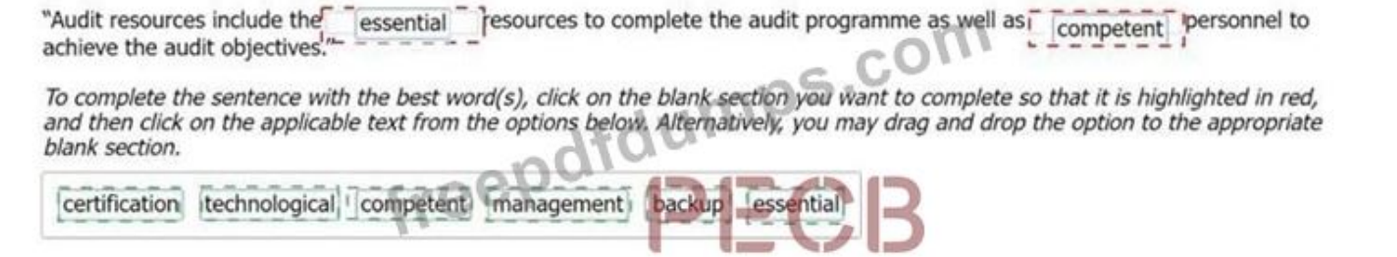
NEW QUESTION: 96
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable 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:
Should the auditor archive the copies of employee training records after the completion of the audit? Refer to scenario 7.
A. No, copies of files are not generally kept as audit records
B. Yes, copies of files are in the auditor's possession, as mentioned in the audit agreement
C. Yes, all the documented information generated during the audit should be kept as audit record
Answer: (SHOW ANSWER)
No, copies of files are not generally kept as audit records unless specifically required and agreed upon in the audit plan. Audit records typically include notes and observations made by auditors, not copies of the auditee's files, unless these are essential and explicitly allowed by the auditee.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 97
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: 98
What is we do in ACT - From PDCA cycle
A. Take actions to continually monitor process performance
B. Take actions to continually improve process performance
C. Take actions to continually monitor process performance
D. Take actions to continually improve people performance
Answer: (SHOW ANSWER)
In the Act phase of the PDCA cycle, the process is reviewed and evaluated based on the results from the Check phase. The actions taken in this phase aim to continually improve the process performance by addressing the root causes of problems, implementing corrective and preventive actions, and updating the process documentation1. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 99
What is the goal of classification of information?
A. To create a manual about how to handle mobile devices
B. Applying labels making the information easier to recognize
C. Structuring information according to its sensitivity

Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
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: 101
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.

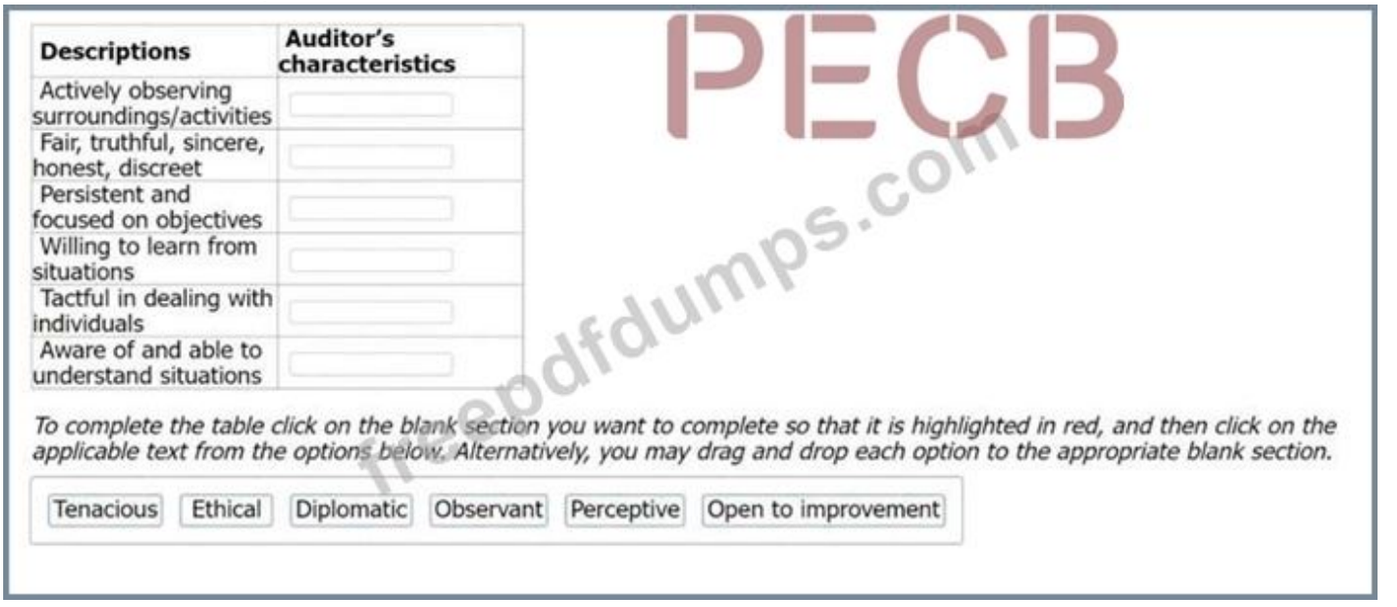
Being one of the top video game console developers in the world, Knight is also often the center of attention for malicious activities. The company has had an operational ISMS for over a year. The ISMS scope includes all departments of Knight, except Finance and HR departments. Recently, a number of 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: 102
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)

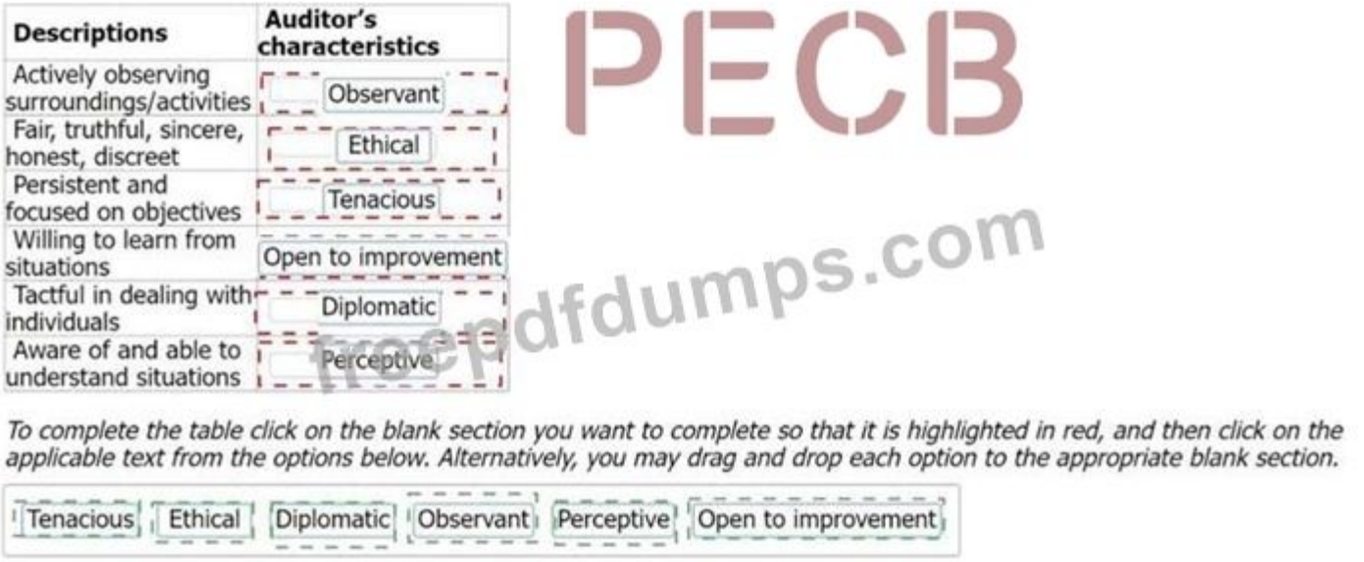
ISO/IEC 27001:2022 is an information security management system standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies the requirements for establishing, implementing, maintaining and continually improving an 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: 103

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:

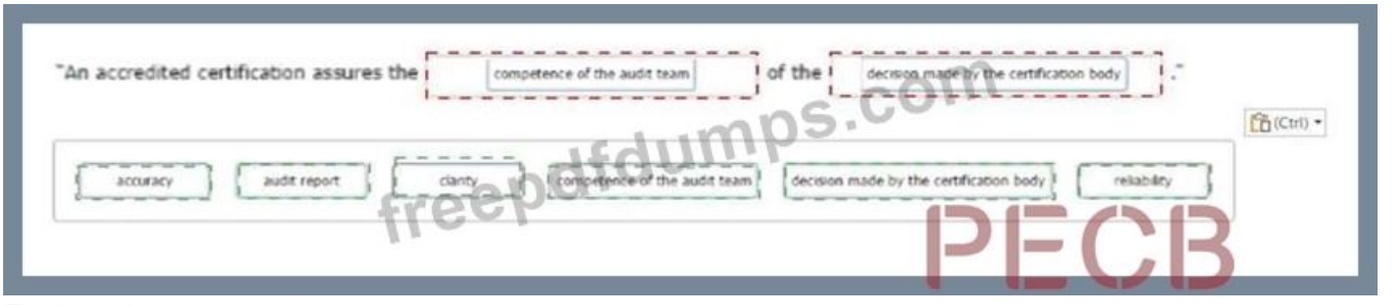
* Tenacious: Persistent and focused on objectives
* Ethical: Fair, truthful, sincere, honest, discreet
* Diplomatic: Tactful in dealing with individuals
* Observant: Actively observing surroundings/activities
* Perceptive: Aware of and able to understand situations
* Open to improvement: Willing to learn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

NEW QUESTION: 104

Select the words that best complete the sentence:

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

Answer:



Explanation

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

NEW QUESTION: 105
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: B,C,E (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 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

Valid ISO-IEC-27001-Lead-Auditor Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Auditor Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Auditor exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Auditor exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Auditor dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Auditor_examcollection.html (**368** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)