PECB.ISO-IEC-27001-Lead-Auditor-CN.v2025-06-12.q131

Exam Code:	ISO-IEC-27001-Lead-Auditor-CN
Exam Name:	PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版)
Certification Provider:	PECB
Free Question Number:	131
Version:	v2025-06-12
# of views:	146
# of Questions views:	1310
https://www.freepdfdumps.com/PECB.ISO-IEC-27001-Lead-Auditor-CN.v2025-06-12.q131.html	

NEW QUESTION: 1
您正在國際物流組織的出貨部門進行 ISMS 審核，該組織為當地醫院和政府辦公室等大型組織提供運輸服務。包裹通常包含藥品、生物樣本以及護照和駕駛執照等文件。您注意到，公司記錄顯示大量退貨，原因包括標籤地址錯誤，以及在5% 的公司案例中，一個包裹的不同地址有兩個或多個標籤。您正在面試運輸經理 (SM)。
您：出貨前檢口過嗎？
SH：任何明顯損壞的物品都會在出貨前由口班人員移除，但利潤微薄，因此實施正式檢口流程並不經濟。
您：退貨後會採取什麼措施？
SM：這些合約大多價口相對較低，因此我們認為，簡單地重新列印標籤並重新發送單一包裹比實施調口更容易、更方便。
您提出不符合項。參考該場景，您希望受審核方在進行後續審核時實施下列哪六項附錄A 控制措施？
A. 5.11 資口返還
B. 8.12 資料外洩保護
C. 5.3 職責分離
D. 6.3 資訊安全意識、教育與培訓
E. 7.10 儲存介質
F. 8.3 資訊存取限制
G. 5.6 與特殊利益團體的聯繫
H. 6.4 紀律程序
I. 7.4 實體安全監控
J. 5.13 資訊標籤

K. 5.32 智慧財口權

Answer: (SHOW ANSWER)

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

References :=

* ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance

* ISO/IEC 27004:2022 Information technology - Security techniques - Information security management systems - Monitoring measurement analysis and evaluation
* ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management
* ISO/IEC 27006:2022 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
* [ISO/IEC 27007:2022 Information technology - Security techniques - Guidelines for information security management systems auditing]

NEW QUESTION: 2
您是經驗豐富的審核團隊領導，指導審核員進行培訓。
您的團隊目前正在對代表外部客口儲存資料的組織進行第三方監督審核。接受培訓的審核員的任務是審口適用性聲明 (SoA) 中列出的並在現場實施的組織控制措施。
從以下口容中選擇您希望接受培訓的審核員審口的四項控制措施。
A. 進出裝載區的通道
B. 保密與保密協議
C. 供應商協定中如何解決資訊安全問題
D. 電源線和資料線如何進入建築物
E. 在組織口部以及向其他組織傳輸訊息的規則
F. 資訊資口清單的開發與維護
G. 現場閉路電視和門禁系統的運行
H. 組織的業務連續性安排
Answer: B,C,E,F (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the auditor in training should review the organisational controls that are related to the information security policy, the roles and responsibilities, the information classification, the information exchange, the supplier relationships, and the information asset management1. These controls are aligned with the ISO/IEC 27001 requirements for clauses
5, 7, 8.2, 8.3, and 8.42. The other controls (A, D, G, and H) are more relevant to the physical and environmental security, the communications security, or the business continuity management, which are not part of the organisational controls3. References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 42, section 5.2.32: ISO/IEC 27001:2022, clauses 5, 7, 8.2, 8.3, and 8.43: ISO/IEC 27001:2022, clauses 8.1, 8.5, and 8.6.

NEW QUESTION: 3
AppFolk 是一家軟體開發公司，正在尋求ISO/IEC 27001 認證。都包括在口。這是可以接受的嗎？
A. 是的，審核和ISMS 範圍不一定需要相同
B. 不，對被審核方所在工業部門不重要的部門可以排除在審核範圍之外
C. 不，審核範圍應反映ISMS 涵蓋的組織的所有部門
Answer: C (LEAVE A REPLY)

No, the audit scope should reflect all of the organization's divisions that are covered by the ISMS. If the ISMS scope stated that it includes the whole company, the audit scope should align with this unless specifically justified and agreed upon by all stakeholders.
References: ISO/IEC 27001:2013, Clause 4.3 (Determining the scope of the information security management system)

NEW QUESTION: 4
您必須進行第三方虛擬審核。在開始進行審核之前，您需要告知受審核方以下哪兩個問題？
A. 您將要求□看螢幕上的人的身分證。
B. 您將為採訪的每個人拍照。
C. 您將要求受訪的人事先□明他們的姓名和職位。
D. 您將要求取得正在進行審核的房間的 360 度視圖。
E. 除非允許，否則您不得記錄審核的任何部分。
F. 您希望受審核方已評估與線上活動相關的所有風險。
Answer: (SHOW ANSWER)
A third-party virtual audit is an external audit conducted by an independent certification body using remote technology such as video conferencing, screen sharing, and electronic document exchange. The purpose of a third-party virtual audit is to verify the conformity and effectiveness of the information security management system (ISMS) and to issue a certificate of compliance12
Before you start conducting the audit, you would need to inform the auditee about the following issues: 12
* You will ask those being interviewed to state their name and position beforehand, i.e., to confirm their identity and role in the ISMS. This is to ensure that you are interviewing the relevant personnel and that they are authorized to provide information and evidence for the audit.
* You will ask for a 360-degree view of the room where the audit is being carried out, i.e., to verify the physical and environmental security of the audit location. This is to ensure that there are no unauthorized persons or devices in the vicinity that could compromise the confidentiality, integrity, or availability of the information being audited.
The other issues are not relevant or appropriate for a third-party virtual audit, because:
* You will ask to see the ID card of the person that is on the screen, i.e., to verify their identity. This is not necessary if you have already asked them to state their name and position beforehand, and if you have access to the auditee's organizational chart or staff directory. Asking to see the ID card could also be seen as intrusive or disrespectful by the auditee.
* You will take photos of every person you interview, i.e., to document the audit process. This is not advisable as it could violate the privacy or consent of the auditee and the interviewees. Taking photos could also be seen as unprofessional or suspicious by the auditee. You should rely on the audit records and evidence provided by the auditee and the audit tool instead.
* You will not record any part of the audit, unless permitted, i.e., to respect the auditee's preferences and rights. This is not a valid issue to inform the auditee about, as you should always

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

NEW QUESTION: 5
a---------- 的職責包括促進審核活動、維護後勤、確保遵守健康和安全政策以及代表受審核方見證審核過程。
A. 口部稽核員
B. 觀察者
C. 指南
Answer: (SHOW ANSWER)
The responsibilities described fit those of a "guide." A guide in an audit context is typically someone from the auditee's organization who facilitates audit activities, manages logistics, ensures compliance with health and safety policies, and may also witness the audit process, assisting the audit team.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 6
審核員需要與受審核方進行有效溝通。因此，他們的個人行為是確保審計成功所需的關鍵特徵 以下是其特徵和相關的簡要描述。將特徵與描述相符。

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

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

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

Answer:

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

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

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

Explanation:

The possible matches of the characteristics to the descriptions are:

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

Actively observing surroundings/activities = Observant

Fair, truthful, sincere, honest, discreet = Ethical

Persistent and focused on objectives = Tenacious

Willing to learn from situations = Open to improvement

Tactful in dealing with individuals = Diplomatic

Aware of and able to understand situations = Perceptive

These are the auditor's characteristics and their descriptions as defined by ISO 19011:2022, Clause
7.2.21. The auditor's personal behaviour is essential for building trust and confidence with the auditee and for ensuring the credibility and effectiveness of the audit12. References: 1: ISO 19011:2022, Guidelines for auditing management systems, Clause 7.2.2 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 3: Fundamental audit concepts and principles

NEW QUESTION: 7
您是一位經驗豐富的 ISMS 審核團隊領導，為審核員提供培訓指導。她問您為什麼制定與不合格品分級相關的具體標準很重要。
下列哪一項答案是正確的？
A. 因為分級標準為評估整個組織的不合格項提供了共同基礎
B. 因為 ISO/IEC 27001:2022 要求它
C. 因為評分標準的建立和實施顯示了對糾正措施流程的高度承諾
D. 因為評分標準將確保所有審核員以完全相同的方式對不合格項進行評分
Answer: A (LEAVE A REPLY)
The correct response is A, because grading criteria provide a common basis for the evaluation of nonconformities across the organization. Grading criteria are the rules or standards that define the severity or impact of nonconformities, and help to determine the appropriate corrective actions and follow-up activities.
Grading criteria are important for several reasons, such as:
* They ensure consistency and objectivity in the assessment and reporting of nonconformities, and avoid subjective or arbitrary judgments.
* They facilitate the communication and understanding of nonconformities among the auditors, the auditees, and the audit clients, and enable the comparison and benchmarking of nonconformities across different processes, functions, or locations.
* They support the prioritization and allocation of resources for the resolution of nonconformities, and the monitoring and measurement of the effectiveness of the corrective actions.
* They demonstrate the commitment and accountability of the organization to the continual improvement of the ISMS, and the compliance with the ISMS requirements and expectations.
References:
* ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1
* PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2
* ISO 27001:2022 Lead Auditor - PECB3
* ISO 27001:2022 certified ISMS lead auditor - Jisc4
* ISO/IEC 27001:2022 Lead Auditor Transition Training Course5
* ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy
* ISO 19011:2022, Guidelines for auditing management systems

NEW QUESTION: 8
審核組組長決定聘請技術專家作為審核小組的一部分，這樣他們就可以填補審核組成員知識的潛在空白。在這種情況下，審計組長應該考慮什麼？
A. 讓技術專家在需要時做出與審核流程相關的決定
B. 技術專家應直接與認證機構而不是審核員討論他們的擔憂
C. 技術專家只能透過審核小組成員之一向受審核方傳達其審核結果
Answer: C (LEAVE A REPLY)
The technical expert can communicate their audit findings to the auditee only through one of the audit team members. This ensures that communications remain coordinated and that the audit team maintains control over the audit process.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 9
起草審核結論後，審核組長的工作文件由認證機構選定的另一位審核員進行審核。這是可以接受的嗎？
A. 是的，審核組長的工作文件在得出審核結論後必須由另一位審核員審核
B. 不可以，在得出審核結論前必須檢討審核組組長的工作
C. 不，只有審核組長審核每位審核員的工作文件
Answer: A (LEAVE A REPLY)
Yes, it is acceptable for the work documents of the audit team leader to be reviewed by another auditor after reaching audit conclusions. This is part of the quality control and assurance processes within the audit to ensure the accuracy and reliability of the audit conclusions.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 10
管理審核計畫的個人負責下列哪六項行動？
A. 選擇審核團隊
B. 保留審核結果的記錄資訊
C. 定義單獨審核的目標、範圍和標準
D. 定義單獨審核的計劃
E. 確定審核計劃的範圍
F. 建立審核計劃
G. 確定審核計畫所需的資源
H. 審核期間與受審核方的溝通
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. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 11
您正在一家名為 ABC 的提供醫療保健服務的住宅療養院進行 ISMS 審核。您會發現所有療養院居民都戴著電子腕帶，用於監控他們的位置、心跳和血壓。您了解到，電子腕帶會自動將所有資料上傳到人工智慧（AI）雲端伺服器，供醫護人員進行健康監測和分析
為了驗證 ISMS 的範圍，您採訪了管理系統代表(MSR)，他解釋ISMS 範圍涵蓋外包資料中心。
為 ISO/IEC 27001:2022 與 ISMS 範圍驗證直接相關的條款和/或控制選擇四個選項。
A. 控制措施 5.3 組織角色、職責與權限
B. 第 4.2 條了解相關方的需求與期望
C. 控制措施 5.3 法律、法規、監管和合約要求
D. 控制措施 6.3 資訊安全意識、教育與培訓
E. 第 5.2 條政策
F. 條款 4.1 了解組織及其背景
G. 控制措施 7.6 在安全區域工作
H. 第 4.3 條決定資訊安全管理系統的範圍
Answer: B,E,F,H (LEAVE A REPLY)
* B. This clause requires the organisation to determine the interested parties that are relevant to the ISMS, and the requirements of these interested parties12. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to identify the stakeholders that have an influence or an interest in the information security of the organisation, such as customers, suppliers, regulators, employees, etc. The organisation should also consider the needs and expectations of these interested parties when defining the scope of the ISMS, and ensure that they are met and communicated.
* E. This clause requires the organisation to establish an information security policy that provides the framework for setting the information security objectives and guiding the information security activities13. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to define the direction and principles of the ISMS, and to align them with the strategic goals and context of the organisation. The information security policy should also be consistent with the scope of the ISMS, and should be communicated and understood within the organisation and by relevant interested parties.

* F. This clause requires the organisation to determine the internal and external issues that are relevant to the purpose and the context of the organisation, and that affect its ability to achieve the intended outcomes of the ISMS14. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to understand the factors and conditions that influence the information security of the organisation, such as the legal, technological, social, economic, environmental, etc. The organisation should also monitor and review these issues, and consider them when defining the scope of the ISMS.
* H. This clause requires the organisation to determine the boundaries and applicability of the ISMS to establish its scope15. This clause is relevant to the verification of the scope of the ISMS because it helps the organisation to describe the information and processes that are included in the ISMS, and to document the scope in a clear and concise manner. The organisation should also consider the issues, requirements, and interfaces identified in clauses 4.1, 4.2, and 4.3 when determining the scope of the ISMS, and ensure that the scope is appropriate to the nature and scale of the organisation.
References:
1: PECB Candidate Handbook - ISO 27001 Lead Auditor, page 17 2: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause
4.2 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 5.2 4: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.1 5: ISO/IEC
27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, clause 4.3

NEW QUESTION: 12
在定義以下口容時，評估與不合格和不遵守法律和合約要求相關的成本：
A. 重要性
B. 審計風險
C. 合理保證
Answer: A (LEAVE A REPLY)
Materiality in the context of an audit involves assessing what level of nonconformities or failures, including those related to legal and contractual compliance, would be significant enough to affect the audit conclusions.
Costs related to these issues are considered when determining materiality.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 13
情境 8 :EsBank 自 9 月起為愛沙尼亞銀行業提供銀行和金融解決方案
2010年，該公司在全國擁有30家分行和100多台ATM機。

EsBank 在高度監管的行業中運營，必須遵守許多有關資料安全和隱私的法律和法規。他們需要透過實施技術和非技術控制來管理整個營運的資訊安全。EsBank 決定實施基於 ISO/IEC 的 ISMS 27001，因為它提供了更好的安全性、更多的風險控制以及符合法律法規的關鍵要求。
在成功實施 ISMS 九個月後，EsBank 決定由獨立認證機構根據 ISO/IEC 27001 對其 ISMS 進行認證。
第一階段和第二階段審核是共同進行的，發現了一些不符合項。第一個不合格之處與 EsBank 的資訊標籤有關。該公司有資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的文件將被貼上不同的標籤（有時為機密，有時為敏感）
考慮到所有文件也以電子方式存儲，不合格情況也影響了媒體處理。審計小組透過抽樣得出結論，200 個可移動媒體中有 50 個儲存了被錯誤分類為機密的敏感資訊。根據資訊分類方案，允許將機密資訊儲存在可移動媒體中，而嚴格禁止儲存敏感資訊。這標誌著另一個不合格之處。
他們起草了不合格報告，並與EsBank 代表討論了審計結論，代表同意在兩個月內針對發現的不合格問題提交行動計劃。
EsBank 接受了審計組組長提出的解決方案。他們根據實體和電子格式的分類方案起草了資訊標籤程序，解決了不合格問題。可移動媒體程式也基於此程式進行了更新。
審計完成兩週後，EsBank 提交了總體行動計畫。在那裡，他們解決了檢測到的不合格問題以及採取的糾正措施，但沒有包括有關受影響的系統、控製或操作的任何詳細資訊。審核小組評估了該行動計劃並得出結論，該計劃將解決不合格問題。然而，EsBank 收到了不利的認證建議。
根據上述場景，回答以下問題：
根據情境8，EsBank 提交了總體行動計畫。這是可以接受的嗎？
A. 是的，具有相同根本原因的不符合項應該有一個總體行動計劃
B. 不，行動計畫應該只解決一個不合格問題
C. 不，一般行動計畫無法修正不合格項
Answer: (SHOW ANSWER)
No, a general action plan is not acceptable in this context because it lacks specific details on systems, controls, or operations impacted by the nonconformities. An effective action plan should detail the specific corrective actions for each nonconformity to ensure comprehensive resolution and prevent recurrence.

NEW QUESTION: 14
在與管理認證機構審核計畫的個人進行討論時，客戶組織的管理系統代表會要求指定特定審核員來進行認證審核。選擇以下選項中的兩個來了解管理審核計劃的個人應如何應對。
A. 通知管理系統代表他的請求可以被接受
B. 建議管理系統代表選擇其他認證機構
C. 告知管理系統代表，審核團隊的選擇是審核專案經理需要根據可用資源做出的決定
D. 表明他的請求將被考慮，但可能不會被接受
E. 建議請求認證機構管理層允許該請求
Answer: C,D (LEAVE A REPLY)
According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, a certification body should ensure that its auditors are

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

NEW QUESTION: 15
在分析審核結論後，X 公司決定接受與其中一項發現的不合格項相關的風險。他們聲稱無需採取糾正措施；然而，他們的決定並沒有記錄在案這是可以接受的嗎？
A. 是的，被審核方的管理階層可以決定接受風險而不是實施糾正措施，並且無需記錄此類決定
B. 不，被審核方接受風險而不是實施糾正措施的決定應該有理由並記錄在案
C. 否，受審核方必須對審核期間記錄的所有觀察結果實施糾正措施
Answer: (SHOW ANSWER)
According to ISO/IEC 27001 standards, if the auditee decides to accept the risk instead of implementing corrective actions for a nonconformity, this decision should be justified and documented. Documenting such decisions is essential for maintaining the integrity of the ISMS and for demonstrating that the decision was made based on informed judgment.
References: ISO/IEC 27001:2013, Clause 6.1 (Actions to address risks and opportunities)

NEW QUESTION: 16
情境 8 :EsBank 自 9 月起為愛沙尼亞銀行業提供銀行和金融解決方案
2010年，該公司在全國擁有30家分行和100多台ATM機。
EsBank 在高度監管的行業中運營，必須遵守許多有關資料安全和隱私的法律和法規。他們需要透過實施技術和非技術控制來管理整個營運的資訊安全。EsBank 決定實施基於 ISO/IEC 的 ISMS 27001，因為它提供了更好的安全性，更多的風險控制以及符合法律法規的關鍵要求。
在成功實施 ISMS 九個月後，EsBank 決定由獨立認證機構根據 ISO/IEC 27001 對其 ISMS 進行認證。
第一階段和第二階段審核是共同進行的，發現了一些不符合項。第一個不合格之處與 EsBank 的資訊標籤有關。該公司有資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的文件將被貼上不同的標籤（有時為機密，有時為敏感）

考慮到所有文件也以電子方式存儲，不合格情況也影響了媒體處理。審計小組透過抽樣得出結論，200 個可移動媒體中有 50 個儲存了被錯誤分類為機密的敏感資訊。根據資訊分類方案，允許將機密資訊儲存在可移動媒體中，而嚴格禁止儲存敏感資訊。這標誌著另一個不合格之處。
他們起草了不合格報告，並與EsBank 代表討論了審計結論，代表同意在兩個月內針對發現的不合格問題提交行動計劃。
EsBank 接受了審計組組長提出的解決方案。他們根據實體和電子格式的分類方案起草了資訊標籤程序，解決了不合格問題。可移動媒體程式也基於此程式進行了更新。
審計完成兩週後，EsBank 提交了總體行動計畫。在那裡，他們解決了檢測到的不合格問題以及採取的糾正措施，但沒有包括有關受影響的系統、控製或操作的任何詳細資訊。審核小組評估了該行動計劃並得出結論，該計劃將解決不合格問題。然而，EsBank 收到了不利的認證建議。
根據上述場景，回答以下問題：
透過起草資訊標籤程序，EsBank 已：
A. 提交了解決不合格問題的行動計劃
B. 建立資訊分類方案
C. 消除不合格的根本原因
Answer: A (LEAVE A REPLY)
By drafting a procedure for information labeling, EsBank has submitted an action plan to resolve the nonconformity. This step addresses the immediate issue identified during the audit by establishing a consistent approach to labeling information according to its classification.

NEW QUESTION: 17
場景 1 :Fintive 是一家傑出的線上支付和保護解決方案安全提供者。Fintive 於 1999 年由 Thomas Fin 在加州聖荷西創立，為線上營運、希望提高資訊安全、防止詐欺並保護 PII 等用戶資訊的公司提供服務。Fintive的決策和營運流程以以往的案例為中心。他們收集客戶數據，根據情況進行分類並進行分析。該公司需要大量員工才能進行如此複雜的分析。然而，幾年後，協助進行此類分析的技術也取得了進展。現在，Fintive 正計劃使用現代工具聊天機器人來實現模式分析，以即時防止詐騙。該工具也將用於幫助改善客戶服務。
這個最初的想法已傳達給軟體開發團隊，他們支持該想法並被分配從事該專案。他們開始將聊天機器人整合到現有系統中。此外，團隊也為聊天機器人設定了一個目標，即回答85% 的聊天戶詢。
聊天機器人成功整合後，該公司立即將其發布給客戶使用。

然而，聊天機器人似乎存在一些問題。
由於測試不足，並且在訓練階段缺乏向聊天機器人提供的樣本（在訓練階段，聊天機器人本應學習」口詢模式），因此聊天機器人無法解決用口口詢並提供正確的答案此外，當聊天機器人收到無效輸入（例如奇怪的點圖案和特殊字元）時它會向使用者發送隨機檔案。因此，聊天機器人無法正確回答客口的口詢，而傳統的客口支援因聊天口詢而不堪重負，因此無法幫助客口解決他們的請求。
因此，Fintive 制定了軟體開發政策。該政策規定，無論軟體是口部開發還是外包，在作業系統上實施之前都將經過黑盒測試。
根據該場景，回答以下問題：
在訓練階段測試不充分且缺乏向 Fintive 聊天機器人提供的樣本被視為 1。
參考場景
A. 威脅
B. 風險
C. 漏洞
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
在測試的基礎上實施計劃 - 這屬於 PDCA 的哪一部分
A. 計劃
B. 執行
C. 行動
D. 檢口
Answer: (SHOW ANSWER)
The PDCA cycle is a four-step method for managing and improving processes. The steps are Plan, Do, Check, and Act. In the Plan phase, the objectives and scope of the process are defined, and the resources and activities are planned. In the Do phase, the process is implemented on a test basis, and the results are recorded and analyzed1. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 19
您正在 ABC Healthcare Services 的療養院執行 ISO 27001 ISMS 監督審核。ABC 使用由供應商 WeCare 設計和維護的醫療保健行動應用程式來監控居民的健康狀況。在審計過程中，您了解到90%的居民家庭成員每週一次透過電子郵件和簡訊定期收到WeCare的醫療器材廣告。ABC 與 WeCare 之間的服務協議禁止供應商使用居民的個人資料。美國廣播公司已收到許多居民及其家人的投訴。
服務經理表示，這些投訴作為資訊安全事件進行了調口，發現這些投訴是合理的已根據不合格和糾正措施管理程序規劃並實施糾正措施。
您寫了一份不合格項“ABC 未能遵守與居民及其家庭成員的個人資料相關的資訊安全控制 A.5.34（隱私和PII 保護）。供應商 WeCare 使用居民的個人資訊向家庭成員”，從列出的糾正和糾正措施中選擇您希望ABC 針對不合格項採取的三個選項
A. ABC 確認資訊安全控制 A.5.34 包含在適用性聲明 (SoA) 中

B. 服務經理提供不合格原因分析的證據以及 ABC 如何評估已實施的糾正措施的有效性
C. 農行指示全體員工遵守與居民家屬簽署的醫療服務協議
D. ABC 進行管理審口，以考慮居民家庭成員的回饋
E. ABC 需要收集更多關於組織如何定義管理系統範圍的證據，並找出他們是否涵蓋醫療設備製造商 WeCare
F. ABC 識別並檢口是否遵守涉及第三方的所有適用法律和合約要求
G. 服務經理實施糾正措施，客口服務代表評估所實施糾正措施的有效性
H. ABC 在對不符合項採取行動之前需要收集更多證據，口明資訊安全風險評估與已識別的不符合項之間的關係
Answer: (SHOW ANSWER)
According to the ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, the following corrections and corrective actions are expected from ABC in response to the nonconformity:
* B. The Service Manager provides evidence of analysis of the cause of nonconformity and how the ABC evaluates the effectiveness of implemented corrective actions. This is part of the requirement of clause
10.1 of ISO/IEC 27001:2022, which states that the organization shall determine the causes of nonconformities and evaluate the need for action to ensure that they do not recur or occur elsewhere12.
The organization shall also evaluate the effectiveness of any corrective actions taken12.
* F. ABC identifies and checks compliance with all applicable legislation and contractual requirements involving third parties. This is part of the requirement of clause 4.2 of ISO/IEC 27001:2022, which states that the organization shall determine the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system12. This includes the legal and contractual requirements related to the information security aspects of the organization's activities, products and services12.
* G. The Service Manager implements the corrective actions and Customer Service Representatives evaluate the effectiveness of implemented corrective actions. This is part of the requirement of clause
10.1 of ISO/IEC 27001:2022, which states that the organization shall implement any action needed and retain documented information as evidence of the results of any action taken12. The organization shall also monitor, measure, analyze and evaluate the information security performance and the effectiveness of the information security management system12.
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: 20

進行外部審核後，審核員決定□部審核員將追蹤糾正措施的實施情況，直到下一次監督審核這是可以接受的嗎？
A. 否，只有外部審核員應在審核完成後跟進糾正措施的實施情況
B. 是的，如果外部稽核師無法完成，□部稽核師可以驗證糾正措施的實施情況
C. 是的，□部稽核師可以追蹤糾正措施的實施情況，直到外部審計師在監督審計期間進行驗證為止
Answer: C (LEAVE A REPLY)
Yes, it is acceptable for the internal auditor to follow-up on the implementation of corrective actions until verified by the external auditor during the next surveillance audit. This practice supports continuous improvement and ensures that corrective actions are effectively implemented and maintained over time.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, Clause 9.2 (Internal audit)

NEW QUESTION: 21
場景 2 :Knight 是一家來自美國北加州的電子公司，開發電玩遊戲機。Knight 在全球擁有 300 多名員工。在成立五週年之際，他們決定推出G-Console，這是一款面向全球市場的新一代電玩遊戲機。G-Console被認為是2021年的終極媒體機，將為玩家帶來最佳的遊戲體驗。
主機包將包括一副 VR 耳機、兩個
遊戲和其他禮物。
多年來，公司透過誠信、誠實和尊重客□而建立了良好的聲譽。這種良好的聲譽是大多數熱衷遊戲玩家在Knight的G-console一上市就想擁有它的原因之一。
Knight 除了是一家非常以客□為導向的公司之外，
也因其開發品質獲得了遊戲□業的廣泛認可。他們的價格比合理標準允許的要高一些。
儘管如此，對於Knight 的大多數忠實客□來□，這並不是一個問題，因為它們的品質是一流的。
作為世界頂級視訊遊戲機開發商之一，Knight 也經常成為惡意活動的焦點。該公司的 ISMS 已投入運作一年多了。ISMS 範圍包括 Knight 的所有部門（財務和人力資源部門除外）。
最近，奈特的一些包含專有資訊的文件被駭客洩露。Knight 的事件回應團隊 (IRT) 立即開始分析系統的每個部分以及事件的詳細資訊。
IRT 的第一個懷疑是 Knight 的員工使用了弱密碼，因此很容易被未經授權存取其帳□的駭客破解。然而，在仔細調□該事件後,IRT 確定駭客透過擷取檔案傳輸協定 (FTP) 流量來存取帳□。
FTP 是一種用於在帳□之間傳輸檔案的網路協定。它使用明文密碼進行身份驗證。
受此資訊安全事件的影響，在RT的建議下，Knight決定用Secure Shell (SSH)協定取代FTP，這樣任何捕獲流量的人都只能看到加密的資料。
在這些變化之後，奈特進行了風險評估，以驗證控制措施的實施是否已將類似事件的風險降至最低。該過程的結果得到了 ISMS 專案經理的批准，他聲稱實施新控制措施後的風險等級符合公司的風險接受程度。
根據該場景，回答以下問題：
Knight 在以 SSH 取代 FTP 時使用了哪種風險處理選項？請參□場景 2。
A. 風險自留
B. 規避風險

C. 風險修改

Answer: (SHOW ANSWER)

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: 22

場景 7 :Lawsy 是一家領先的律師事務所，在新澤西州和紐約市設有辦公室。它擁有 50 多名律師，為商業法、智慧財□權、銀行和金融服務領域的客□提供完善的法律服務。他們相信，由於他們致力於實施資訊安全最佳實踐並跟上技術發展的步伐，他們在市場上佔據了有利的地位。

Lawsy 已經嚴格實施、評估和進行 ISMS □部審核兩年了。

現在，他們已向知名且□得信賴的認證機構SMA申請ISO/IEC 27001認證。

在第一階段審核期間，審核小組審□了實施過程中所建立的所有ISMS 文件。

他們還審□和評估了管理審□和□部審計的記錄。

Lawsy 提交了證據記錄，表明在必要時對不合格項採取了糾正措施，因此審核組約談了□部審核員。訪談透過提供對□部稽核計畫和程序的詳細了解，驗證了□部稽核的充分性和頻率。

審計小組繼續驗證戰略文件，包括資訊安全政策和風險評估標準。在資訊安全政策審□期間，團隊注意到描述治理框架（即資訊安全政策）的記錄資訊與程序之間存在不一致

儘管允許員工將筆記型電腦帶到工作場所之外，但Lawsy 並沒有製定有關在這種情況下使用筆記型電腦的程序。此政策僅提供有關筆記型電腦使用的一般資訊。該公司依靠員工的常識來保護筆記型電腦中儲存的資訊的機密性和完整性。該問題已記錄在第一階段審計報告中。

完成第一階段審核後，審核組長準備了審核計劃，其中闡述了審核目標範圍、標準和程序。

在第二階段審核期間，審核小組約談了資安經理，資安經理起草了資訊安全政策他透過指出 Lawsy 每三個月舉辦一次強制性資訊安全培訓和意識課程來證明第一階段中確定的問題的合理性。

面談後，審核小組檢□了15 份員工培訓記錄（共50 份），得出的結論是awsy 符合 ISO/IEC 27001 有關培訓和意識的要求。為了支持這個結論，他們影印了檢□過的員工訓練記錄。

根據上述場景，回答以下問題：

根據情境 7，Lawsy 在開始第二階段審核之前該做什麼？

A. 第一階段審核的審核結果進行品質審核

B. 定義可以組合哪些審核測試計畫來驗證合規性

C. 與認證機構審核並確認審核計劃

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: 23
下列哪一項是利害關係方的定義？
A. 當第三人認為自己受到決策或活動的影響時，可以向組織提出申訴
B. 可以影響決策或活動、受決策或活動影響或認為自己受決策或活動影響的個人或組織
C. 可以乾擾管理決策或認為自己受到管理決策幹擾的團體或組織
D. 可以控制決策或活動、被決策或活動控製或認為自己被決策或活動控制的個人或組織
Answer: B (LEAVE A REPLY)
This is the definition of an interested party according to ISO 27001:2013, clause 3.16. An interested party is essentially a stakeholder, i.e., a person or organization that can influence or be influenced by the information security management system (ISMS) or its activities. Interested parties can have different needs and expectations regarding the ISMS, and these should be identified and addressed by the organization.
References:
* ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.16
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 10
* Identifying interested parties and their expectations for an ISO 27001 ISMS
* Examples of ISO 27001 interested parties

NEW QUESTION: 24
您正在一家名為 ABC 的提供醫療保健服務的住宅療養院進行 ISMS 審核。您會發現所有療養院居民都戴著電子腕帶，用於監控他們的位置、心跳和血壓。您了解到，電子腕帶會自動將所有資料上傳到人工智慧（AI）雲端伺服器，供醫護人員進行健康監測和分析
為了驗證 ISMS 的範圍，您採訪了管理系統代表(MSR)，他解釋ISMS 範圍涵蓋外包資料中心。選擇定義 ISMS 範圍內容的正確敘述之一。
A. ISMS 範圍不應涵蓋外部服務提供者，因為他們可能在遵守資訊安全政策和要求方面遇到困難
B. ISMS 範圍應考慮已發生的任何資訊安全問題以及任何利害關係人的要求
C. 最有可能的 ISMS 範圍是涵蓋 IT 部門和外包資料中心
D. 組織應僅遵循政府的建議，即法律和立法來定義ISMS 範圍
Answer: B (LEAVE A REPLY)
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: 25
您是經驗豐富的 ISMS 審核團隊負責人，負責進行第三方監督訪問。
您注意到，儘管受審核方聲稱符合ISO/IEC 27001:2022，但他們仍將改進稱為第10.2 條（與2013 年版一樣），而現在是2022 年版中的第 10.1 條。您已確認它們符合標準中規定的所有 2022 年要求。
選擇您應該採取的操作之一。
A. 注意審核報告中的問題
B. 針對第 7.5.3 條提出不符合項 - 記錄資訊的控制
C. 將其作為改進的機會
D. 在閉幕會議上提出此事
Answer: (SHOW ANSWER)
The correct action to take in this situation is to raise it as an opportunity for improvement. This is because the auditee is not violating any requirement of the standard, but rather using outdated terminology that does not reflect the current version of the standard. An opportunity for improvement is a suggestion for enhancing the performance or effectiveness of the ISMS1. It is not a nonconformity, which is a failure to fulfil a requirement2. Therefore, option B is incorrect. Option A is also incorrect, because noting the issue in the audit report without raising it as an opportunity for improvement would not provide any value or feedback to the auditee. Option D is also incorrect, because bringing the matter up at the closing meeting without documenting it as an opportunity for improvement would not ensure that the auditee takes any action to address it.
References: 1: ISMS Auditing Guideline - ISO27000, page 11; 2: ISO/IEC 27000:2022, 3.28; : ISMS Auditing Guideline - ISO27000; : ISO/IEC 27000:2022

NEW QUESTION: 26
您詢問 IT 經理，為什麼組織仍在使用行動應用程序，而個人資料加密和假名化測試卻失敗了。此外，服務經理是否有權批准測試。
IT經理解釋口，根據軟體安全管理程序，測試結果應由他批准加密和假名功能失敗的原因是這些功能嚴重降低了系統和服務效能。需要額外 150% 的資源來滿足這一點。服務經理同意存取控制足口好並且可以接受。這就是服務經理簽署批准書的原因。
您正在準備審計結果。選擇正確的選項。
A. 存在不合格項 (NC)。組織和開發人員不執行驗收測試。
（與第8.1 條相關，控制措施A.8.29）
B. 存在不合格項 (NC)。服務管理員不遵守軟體安全管理程序。（與第8.1 條相關，控制措施A.8.30）
C. 存在不合格項 (NC)。組織和開發人員執行的安全測試失敗。
（與第8.1 條相關，控制措施A.8.29）

D. 不存在不合格項 (NC)。服務經理做出了繼續提供服務的正確決定。
（與第8.1 條相關，控制措施A.8.30）
Answer: B (LEAVE A REPLY)
According to ISO 27001:2022 Annex A Control 8.30, the organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This includes developing and entering into licensing agreements that cover code ownership and intellectual property rights, and implementing appropriate contractual requirements related to secure design and coding in accordance with Annex A 8.25 and 8.2912 In this case, the organisation and the developer have performed security tests that failed, which indicates that the secure design and coding requirements of Annex A 8.29 were not met. The IT Manager explains that the encryption and pseudonymisation functions failed because they slowed down the system and service performance, and that an extra 150% of resources are needed to cover this. However, this does not justify the acceptance of the test results by the Service Manager, who is not authorised to approve the test according to the software security management procedure. The Service Manager should have consulted with the IT Manager, who is the owner of the process, and followed the procedure for handling nonconformities and corrective actions. The Service Manager's decision to continue the service based on access control alone exposes the organisation to the risk of compromising the confidentiality, integrity, and availability of personal data processed by the mobile app. Therefore, there is a nonconformity (NC) with clause 8.1, control A.8.30.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 27
您正在作為審核組組長進行首次第三方 ISMS 監督審核。您目前與審核團隊的另一位成員以及組織的指南一起位於受審核方的資料中心。
您要求進入受密碼鎖和虹膜掃描器保護的上鎖房間。此房間包含幾排不間斷電源以及幾個包含客口端提供的設備（主要是伺服器和交換器）的資料櫃
您注意到有一個氣體滅火系統。標籤表示系統需要每 6 個月進行一次測試，但標籤上記錄的最近一次測試是製造商在 12 個月前進行的。
根據上述情況，您現在會採取下列哪兩項操作？
A. 由於組織尚未確定需要針對火災威脅採取行動，因此針對控制A.5.7 威脅情報」提出不符合項
B. 做筆記，向現場維修經理索取6個月前進行過滅火系統測試的證據
C. 如果房間口有水基滅火器，則無需採取進一步行動，因為它們提供了另一種滅火方法
D. 確定記錄滅火器檢口的要求是否在去年進行了修訂。
如果是這樣，建議在現有標籤上引用這些口容作為改進的機會
E. 需要指南來口動組織的資訊安全事件流程
F. 針對控制 A.7.11 支援公用設施」提出不符合項，因為資訊處理設施沒有充分保護以防止可能的中斷

Answer: (SHOW ANSWER)

NEW QUESTION: 28
您是負責管理審核計劃並決定特定審核的審核團隊的規模和組成的人。選擇應考慮的兩個因素。
A. 審核範圍與標準
B. 客口關係
C. 審核團隊實現審核目標所需的整體能力
D. 審核組組長的資歷
E. 審核成本
F. 受審核方首選的持續時間
Answer: (SHOW ANSWER)
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: 29
資訊安全是建立和維護 _____ 的問題。
A. 保密性
B. 信任
C. 保護
D. 防火牆
Answer: (SHOW ANSWER)
Information security is a matter of building and maintaining trust. Trust is the confidence that information and information processing facilities are protected from unauthorized or malicious actions that could compromise their confidentiality, integrity or availability. Trust is essential for establishing and maintaining relationships with customers, partners, suppliers, employees and other stakeholders who rely on the organization's information and services. Trust is also a key factor for achieving compliance with legal, regulatory and contractual obligations, as well as meeting the organization's own information security objectives and policies. ISO/IEC 27001:2022 defines information security as "preservation of confidentiality, integrity and availability of information" (see clause 3.28) and states that "the purpose of an information security management system is to provide a framework for managing activities that influence the trustworthiness of information" (see Introduction). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Trust?

NEW QUESTION: 30
您正在國際物流組織的出貨部門進行 ISMS 審核，該組織為當地醫院和政府辦公室等大型組織提供運輸服務。包裹通常包含藥品、生物樣本以及護照和駕駛執照等文件。您注意到公司記錄顯示大量退貨，原因包括標籤地址錯誤，以及在5% 的情況下，一個包裹的不同地址有兩個或多個標籤。您正在面試運輸經理 (SM)。
您：出貨前檢口過嗎？
SM：任何明顯損壞的物品都會在出貨前由口班人員移除，但利潤微薄，因此實施正式檢口流程並不經濟。
您：退貨後會採取什麼措施？
SM：這些合約大多價口相對較低，因此我們認為，簡單地重新列印標籤並重新發送單一包裹比實施調口更容易、更方便。
您因標籤流程缺乏控製而提出不符合 ISO 27001:2022 的要求。
在最後一次會議上，運輸經理向您道歉，他的評論可能被誤解了他口，他沒有意識到有一個後台IT流程會自動檢口正確的標籤是否貼在正確的包裹上，否則包裹會在貼標籤時被彈出。他要求你撤回你不合格的行為。
選擇您作為審核組組長對運輸經理的要求做出的正確回應的三個選項。
A. 通知運輸經理他的請求將包含在審核報告中
B. 建議管理階層在審核員有更多時間時討論所提供的新資訊
C. 通知運輸經理，不合格情況很輕微，應迅速糾正
D. 請審核團隊成員口明他們認為應該發生什麼
E. 告知他您的理解並撤回不符合項
F. 感謝運輸經理的誠實，但建議撤回不合格項並不是正確的處理方式
G. 建議運輸經理該不合格項必須成立，因為所獲得的證據非常昂貴
H. 顯示不符合項是需要修正的更深層系統故障的證據
Answer: (SHOW ANSWER)
* A. Advise the Shipping Manager that his request will be included in the audit report. This is true because the audit report should document all the relevant information and evidence related to the audit, including any requests or objections raised by the auditee. The audit report should also provide the rationale for the audit conclusions and recommendations12.
* B. Advise management that the new information provided will be discussed when the auditors have more time. This is true because the auditors should not make hasty decisions based on incomplete or unverified information. The auditors should review and evaluate the new information in a systematic and objective manner, and determine whether it affects the audit findings, nonconformities, or conclusions12.
* F. Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed. This is true because the auditors should acknowledge and appreciate the cooperation and transparency of the auditee, but also maintain their professional integrity and independence. The auditors should not withdraw a nonconformity unless they are satisfied that it was raised in error or that it has been effectively corrected and verified12.
References :=

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

NEW QUESTION: 31
您正在一家名為 ABC 的提供醫療保健服務的住宅療養院進行 ISMS 審核。您會發現所有療養院居民都戴著電子腕帶，用於監控他們的位置、心跳和血壓。您了解到，電子腕帶會自動將所有資料上傳到人工智慧（AI）雲端伺服器，供醫護人員進行健康監測和分析。
為了驗證 ISMS 的範圍，您採訪了管理系統代表(MSR)，他解釋ISMS 範圍涵蓋外包資料中心。
選擇三個選項作為您需要尋找的審核證據，以驗證ISMS 的範圍。
A. 被審核方已確定居民對設施和環境安全的需求和期望
B. 被審核方擁有 ISO 9001 認證
C. 被審核方已確定政府當局對醫療保健服務和病患資料處理的需求和期望
D. 受審核方已確定居民對於如何保護居民個人資料的需求和期望
E. 被審核方已確定居民對舒適設施、醫療專業人員能力和清潔環境的需求和期望
F. 被審核方已確定居民對健康醫療服務的需求和期望
G. 與人工智慧雲端伺服器所在資料中心的IT服務協議
H. 被審核方正在考慮從外部軟體公司購買醫療保健監控應用程式
Answer: (SHOW ANSWER)
According to ISO 27001:2022 clause 4.3, the organisation shall determine the scope of the information security management system (ISMS) by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organisations12 In this case, the ISMS scope covers an outsourced data center that hosts the artificial intelligence (AI) cloud server for healthcare monitoring and analysis of the residents' data. Therefore, the audit evidence you need to find to verify the scope of the ISMS should include:
* The auditee has identified the governmental authorities' needs and expectations on healthcare services and patient data handling. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to comply with the relevant laws and regulations regarding the quality, safety, and privacy of healthcare services and patient data12
* The auditee has identified the resident's needs and expectations on how they should protect the resident' s personal data. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to ensure the confidentiality, integrity, and availability of the resident's personal data that is collected, processed, and stored by the electronic wristband and the AI cloud server12
* The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located. This is an interface and dependency with another organisation that affects the ISMS scope, as the auditee has to control the externally provided processes, products, and services that are relevant to the ISMS, and to implement appropriate contractual requirements related to

information security12 The following options are not relevant or sufficient for verifying the scope of the ISMS:
* The auditee has identified the resident's needs and expectations on the facility and environmental safety. This is an external issue and an interested party requirement, but it does not affect the ISMS scope, as it is not related to information security12
* The auditee has ISO 9001 certification. This is an indication of the auditee's quality management system, but it does not verify the scope of the ISMS, as it is not related to information security12
* The auditee has identified the resident's needs and expectations on the comfort facility, medical professional's competence, and clean environment. These are external issues and interested party requirements, but they do not affect the ISMS scope, as they are not related to information security12
* The auditee has identified the resident's needs and expectations on healthcare medical treatment services. These are external issues and interested party requirements, but they do not verify the scope of the ISMS, as they are not specific to information security12
* The auditee is considering the purchase of a healthcare monitoring app from an external software company. This is a potential change that may affect the ISMS scope in the future, but it does not verify the current scope of the ISMS, as it is not yet implemented or controlled12
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 32
您正在 ABC Healthcare Services 的療養院執行 ISO 27001 ISMS 監督審核。ABC 使用由供應商 WeCare 設計和維護的醫療保健行動應用程式來監控居民的健康狀況。在審核過程中，您了解到90%的居民家庭成員每週都會透過電子郵件和簡訊定期收到WeCare的醫療器材廣告。ABC 與 WeCare 之間的服務協議禁止供應商使用居民的個人資料。美國廣播公司已收到許多居民及其家人的投訴。
服務經理表示，這些投訴作為資訊安全事件進行了調口，發現這些投訴是合理的
已根據不合格和糾正措施管理程序規劃並實施糾正措施。

您寫了一份不合格項“ABC 未能遵守與居民及其家庭成員的個人資料相關的資訊安全控制 A.5.34（隱私和PII 保護）。供應商 WeCare 使用居民的個人資訊向家庭成員。”從列出的糾正和糾正措施中選擇您希望 ABC 針對不合格項採取的三個選項。

A. ABC 要求 ISMS 顧問測試 ABC Healthcare 行動應用程式以防範網路犯罪。

B. ABC 取消與 WeCare 的服務協定。

C. ABC 確認資訊安全控制 A.5.34 包含在適用性聲明 (SoA) 中。

D. ABC 停止使用 ABC Healthcare 行動應用程式。

E. ABC 為所有供應商引入了資訊安全績效背景調口。

F. ABC 定期監控涉及第三方的所有適用法律和合約要求的遵守情況。

G. ABC 對 WeCare 違反合約採取法律行動。

H. ABC 對所有員工進行維護資訊安全協定重要性的訓練。

Answer: (SHOW ANSWER)

The three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity are:

* B. ABC cancels the service agreement with WeCare.
* E. ABC introduces background checks on information security performance for all suppliers.
* F. ABC periodically monitors compliance with all applicable legislation and contractual requirements involving third parties.

* B. This option is a possible correction and corrective action that ABC could take to address the nonconformity. A correction is the action taken to eliminate a detected nonconformity, while a corrective action is the action taken to eliminate the cause of a nonconformity and to prevent its recurrence1. By cancelling the service agreement with WeCare, ABC could stop the unauthorized use of residents' personal data and protect their privacy and rights. This could also prevent further complaints and legal issues from the residents and their family members. However, this option may also have some drawbacks, such as the loss of a service provider, the need to find an alternative solution, and the potential impact on the residents' well-being.
* E. This option is a possible corrective action that ABC could take to address the nonconformity. By introducing background checks on information security performance for all suppliers, ABC could ensure that they select and work with reliable and trustworthy partners who respect the confidentiality, integrity, and availability of the information they handle. This could also help ABC to comply with information security control A.15.1.1 (Information security policy for supplier relationships), which requires the organisation to agree and document information security requirements for mitigating the risks associated with supplier access to the organisation's assets2.
* F. This option is a possible corrective action that ABC could take to address the nonconformity. By periodically monitoring compliance with all applicable legislation and contractual requirements involving third parties, ABC could verify that the suppliers are fulfilling their obligations and responsibilities regarding information security. This could also help ABC to comply with information security control A.18.1.1 (Identification of applicable legislation and contractual requirements), which requires the organisation to identify, document, and keep up to date the

relevant legislative, regulatory, contractual, and other requirements to which the organisation is subject3.
References:
1: ISO 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, clause 3.9 and 3.10 2: ISO/IEC 27001:2022 - Information technology
- Security techniques - Information security management systems - Requirements, Annex A, control A.
15.1.1 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, Annex A, control A.18.1.1

NEW QUESTION: 33
情境 4 :SendPay 是一家金融公司，透過代理商和金融機構網路提供服務。他們的主要服務之一是在全球範圍□轉帳。SendPay 作為一家新公司，致力於為客□提供最優質的服務。由於該公司提供國際交易，因此要求客□提供個人信息，例如身份交易原因以及完成交易可能需要的其他詳細信息。因此，SendPay 已實施安全措施來保護客□的訊息，包括偵測、調□和回應可能出現的任何資訊安全威脅。他們對提供安全服務的承諾也體現在 ISMS 實施過程中，該公司投入了大量時間和資源。
去年，SendPay 推出了他們的數位平台，允許透過智慧型手機或筆記型電腦等電子設備進行貨幣交易，而無需支付額外費用。透過這個平台，SendPay 的客□可以隨時隨地發送和接收資金。該數位平台幫助SendPay簡化了公司營運並進一步拓展了業務。當時SendPay正在外包其軟體業務，因此該專案是由外包公司的軟體開發團隊完成的。
該團隊還負責維護 SendPay 的技術基礎設施。
最近，該公司在實施ISMS 近一年後申請了 ISO/IEC 27001 認證。他們與符合其標準的認證機構簽訂了合約。不久之後，認證機構任命了一個由四名審核員組成的團隊來審核SendPay 的 ISMS。
審計過程中，發現以下情況：
1.外包軟體公司在未事先通知的情況下終止了與SendPay的合約。結果，SendPay 無法立即將服務恢復到□部，其營運中斷了五天。審計人員要求 SendPay 的代表提供證據，證明他們在合約終止的情況下有計劃遵循。這些代表沒有提供任何書面證據，但在接受審計時，他們告訴審計人員，SendPay的高層已經確定了另外兩家軟體開發公司，如果類似情況再次發生，可以立即提供服務。
2. 沒有證據顯示對外包給軟體開發公司的活動進行了監控。SendPay 的代表再次告訴審計人員，他們定期與軟體開發公司溝通，並適當地告知可能發生的任何變更。
3.防火牆測試未發現異常狀況。審核員測試了防火牆配置，以確定這些服務提供的安全等級。他們使用資料包分析器來測試防火牆策略，這使他們能□即時檢□發送或接收的資料包。
根據該場景，回答以下問題：
根據情境 4，審計人員要求提供有關外包業務監控過程的文件證據。這□明什麼？
A. 審核員表現出專業懷疑態度
B. 審計人員洩漏了外包業務的機密性
C. 審計師根據基於風險的方法評估了證據
Answer: A (LEAVE A REPLY)

Based on the provided scenario, the auditors' request for documentary evidence regarding the monitoring process of outsourced operations indicates that the auditors demonstrated professional skepticism. This is because professional skepticism involves a critical assessment of audit evidence and includes a questioning mind and a careful evaluation of the information provided by the auditee123.
Professional skepticism is an essential part of the auditing process, especially in the context of ISO/IEC
27001, which requires auditors to systematically examine an organization's information security risks, including the management of outsourced processes4. The auditors' request for evidence suggests that they were not satisfied with verbal assurances alone and sought to verify that SendPay had a formal, documented process for monitoring outsourced activities, which is a requirement for maintaining an effective Information Security Management System (ISMS)5.
Therefore, the correct answer is: A. The auditors demonstrated professional skepticism.

NEW QUESTION: 34
情境 4 :SendPay 是一家金融公司，透過代理商和金融機構網路提供服務。他們的主要服務之一是在全球範圍內轉帳。SendPay 作為一家新公司，致力於為客戶提供最優質的服務。由於該公司提供國際交易，因此要求客戶提供個人信息，例如身份、交易原因以及完成交易可能需要的其他詳細信息。因此，SendPay 已實施安全措施來保護客戶的訊息，包括偵測、調查和回應可能出現的任何資訊安全威脅。他們對提供安全服務的承諾也體現在 ISMS 實施過程中，該公司投入了大量時間和資源。
去年，SendPay 推出了他們的數位平台，允許透過智慧型手機或筆記型電腦等電子設備進行貨幣交易，而無需支付額外費用。透過這個平台，SendPay 的客戶可以隨時隨地發送和接收資金。該數位平台幫助SendPay簡化了公司營運並進一步拓展了業務。當時SendPay正在外包其軟體業務，因此該專案是由外包公司的軟體開發團隊完成的。
該團隊還負責維護 SendPay 的技術基礎設施。
最近，該公司在實施ISMS 近一年後申請了 ISO/IEC 27001 認證。他們與符合其標準的認證機構簽訂了合約。不久之後，認證機構任命了一個由四名審核員組成的團隊來審核SendPay 的 ISMS。
審計過程中，發現以下情況：
1.外包軟體公司在未事先通知的情況下終止了與SendPay的合約。結果，SendPay 無法立即將服務恢復到正常，其營運中斷了五天。審計人員要求 SendPay 的代表提供證據，證明他們在合約終止的情況下有計劃遵循。這些代表沒有提供任何書面證據，但在接受審計時，他們告訴審計人員，SendPay的高層已經確定了另外兩家軟體開發公司，如果類似情況再次發生，可以立即提供服務。
2. 沒有證據顯示對外包給軟體開發公司的活動進行了監控。SendPay 的代表再次告訴審計人員，他們定期與軟體開發公司溝通，並適當地告知可能發生的任何變更。
3.防火牆測試未發現異常狀況。審核員測試了防火牆配置，以確定這些服務提供的安全等級。他們使用資料包分析器來測試防火牆策略，這使他們能夠即時檢查發送或接收的資料包。
根據該場景，回答以下問題：
您如何評估所獲得的與外包業務監控流程相關的證據？請參考場景 4。
A. 無關緊要，監控外包作業不是標準的要求

B. 不可靠。SendPay 僅提供了有關其外包業務監控的口頭證據
C. SendPay 代表的適當且充分的口頭確認表明他們知道必須監控外包操作
Answer: B (LEAVE A REPLY)
The evidence provided by SendPay, which is solely verbal confirmation about the monitoring of outsourced operations, is not considered reliable under ISO/IEC 27001. The standard requires documented evidence to support claims of effective monitoring and control over outsourced processes.
References: ISO/IEC 27001:2013 Standard, Clause A.15 (Supplier relationships)

NEW QUESTION: 35
您是一位經驗豐富的 ISMS 審核團隊領導，為審核員提供培訓指導。
受訓的審核員似乎對 ISO 27001:2022 中能力的解釋感到困惑，並且正在尋求您的澄清，以確保他的理解是正確的。他列出了一系列小情景，並詢問您將其中哪一個歸因於缺乏能力。選擇四個正確選項。
A. 一位最近從 IT 網路團隊調到軟體開發團隊的員工不知道在出貨前需要填寫口品發佈表格
B. 一位高級程式設計師沒有檢口他們的編碼是否有錯誤，因為他們去看醫生遲到了
C. 新口動者無法開口閉路電視監控，因為他們沒有被告知如何執行此操作
D. IT 技術人員因未口讀提供的口明而未能正確配置新型號的伺服器
E. 一位經驗豐富的接待員允許她認識的承包商在沒有門禁卡的情況下進入資料中心
F. 系統管理員因收到錯誤指令而刪除了兩個真實帳口以及五個冗餘帳口
G. 資料中心操作員因急於執行另一項任務而無意中將備份磁帶放入了錯誤的磁碟機中
H. 高階經理人無法協助組織的資訊安全事件復原流程，因為她沒有接受過所需的培訓
Answer: (SHOW ANSWER)
These four scenarios are examples of a lack of competence, which is defined as the ability to apply the knowledge and skills needed to perform a work role or a task effectively and efficiently12. Competence in ISO 27001:2022 is determined by the organisation's needs and expectations, and it is based on the relevant education, training, or experience of the people involved in the ISMS34. The organisation is required to ensure that all the people who affect the performance of the ISMS are competent, and to provide them with the necessary training and awareness to fulfil their roles and responsibilities35. The four scenarios indicate that the people involved either lack the knowledge or skills to perform their tasks, or have not received the appropriate training or guidance to do so. The other scenarios are not related to competence, but to other factors such as negligence, error, or policy violation.
References: = 1: ISO 19011:2018 Guidelines for auditing management systems, clause 3.72: ISO/IEC 27007:
2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 53: ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, clause 7.24: ISO 27001 Requirement 7.2 - Competence | ISMS.online15: ISO27001 Clause 7.2 Competence - Ultimate Certification Guide - High Table3

NEW QUESTION: 36
場景9 :UpNet是一家網路公司，已通過SO/IEC 27001認證。
自從獲得 ISO/IEC 27001 認證以來，該公司的認可度大幅提高。此認證證實了 UpNefs 營運的成熟性及其符合廣泛認可和接受的標準。
但認證之後一切還沒結束。UpNet 透過進行□部稽核不斷審□和增強其安全控制以及 ISMS 的整體有效性和效率。高階主管不願意聘請全職□部稽核團隊，因此決定將□部稽核職能外包。這種形式的□部稽核確保了獨立性、客觀性，並且在ISMS 的持續改進方面發揮諮詢作用。
在初次認證審核後不久，該公司創建了一個專門從事數據和儲存□品的新部門。他們提供針對資料中心和基於軟體的網路設備（例如網路虛擬化和網路安全設備）進行最佳化的路由器和交換器這導致 ISMS 認證範圍□已涵蓋的其他部門的營運發生變化。
所以。UpNet □動了風險評估流程和□部稽核。根據□部審計結果，公司確認了現有和新流程和控制的有效性和效率。
由於新部門符合 ISO/IEC 27001 要求，最高管理層決定將其納入認證範圍。UpNet宣布取得ISO/IEC 27001認證，認證範圍涵蓋全公司。
在初次認證審核一年後，認證機構對UpNefs ISMS 進行了另一次審核。
此次審核旨在確定 UpNefs ISMS 是否符合指定的 ISO/IEC 27001 要求，並確保ISMS 持續改善。審核小組確認，經過認證的ISMS 繼續符合標準的要求。儘管如此，新部門對管理體系的治理□生了重大影響。此外，認證機構並未獲悉任何變更。因此，UpNefs認證被暫停。
根據上述場景，回答以下問題：
UpNet宣布ISMS認證範圍涵蓋整個公司，確保新部門也符合SO/IEC 27001要求。您如何對場景 9 所示的情況進行分類？
A. 不可接受，延期審核應由□部審核員而非最高管理階層批准
B. 不可接受，UpNet 應在發佈公告之前請求並批准延期審核
C. 可接受，□部稽核確認了現有和新流程和控制的有效性和效率
Answer: B (LEAVE A REPLY)
This situation is unacceptable because UpNet should have requested and been granted an extension audit prior to announcing that the ISMS certification scope encompasses the whole company, including the new department. Proper procedures need to be followed to extend the certification to additional departments or processes.

NEW QUESTION: 37
為了驗證是否符合 ISO/IEC 27001 附錄 A 控制措施 8.15 記錄，審核小組驗證了伺服器日誌樣本，以確定它們是否可以編輯或刪除。使用了哪種審計程序？
A. 分析
B. 取樣
C. 觀察
Answer: A (LEAVE A REPLY)

The audit procedure used here is "analysis." The audit team analyzed server logs to verify if they can be edited or deleted, focusing on evaluating the logs' properties and the controls over their manipulation to ensure they comply with ISO/IEC 27001 requirements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 38
審計結果是根據審計標準對收集的審計證據進行評估的結果。評估以下潛在的審計證據格式並選擇可接受的兩種。
A. 對測試結果進行未簽署的手寫更改
B. IT 經理的事實陳述
C. 有關 IT 審核結果的記錄資訊
D. 系統工程師的言論，無法驗證
E. 觀察先前錄製的演示危險活動表現的視頻
F. IT 經理與系統工程師之間對話的錄音
Answer: C,E (LEAVE A REPLY)
According to the ISO/IEC 27001 Lead Auditor exam preparation guide1, audit evidence can be in various formats, such as records, statements of fact, or other information that is relevant and verifiable. Audit evidence can be collected by means of interviews, observation, sampling, testing, or other techniques.
However, not all formats of audit evidence are acceptable or reliable. For example, unsigned hand written changes to test results (A) are not verifiable and may indicate tampering or falsification. Statements by a system engineer that cannot be verified (D) are also not reliable and may be biased or inaccurate. An audio recording of a dialog between the IT manager and a system engineer (F) may not be relevant to the audit criteria or may violate the confidentiality or consent of the parties involved. A statement of facts by the IT manager (B) may be relevant and verifiable, but it is not sufficient as audit evidence unless it is supported by other sources of information. Therefore, the two acceptable formats of audit evidence are documented information on results of IT audits and observation of a previously recorded video demonstrating the performance of a hazardous activity (E), as they are relevant to the audit criteria and can be verified by other means. References: 1: https://pecb.com/pdf/exam-preparation-guides/pecb-iso-iec-27001-lead-auditor-exam- preparation-guide.pdf (page 9)

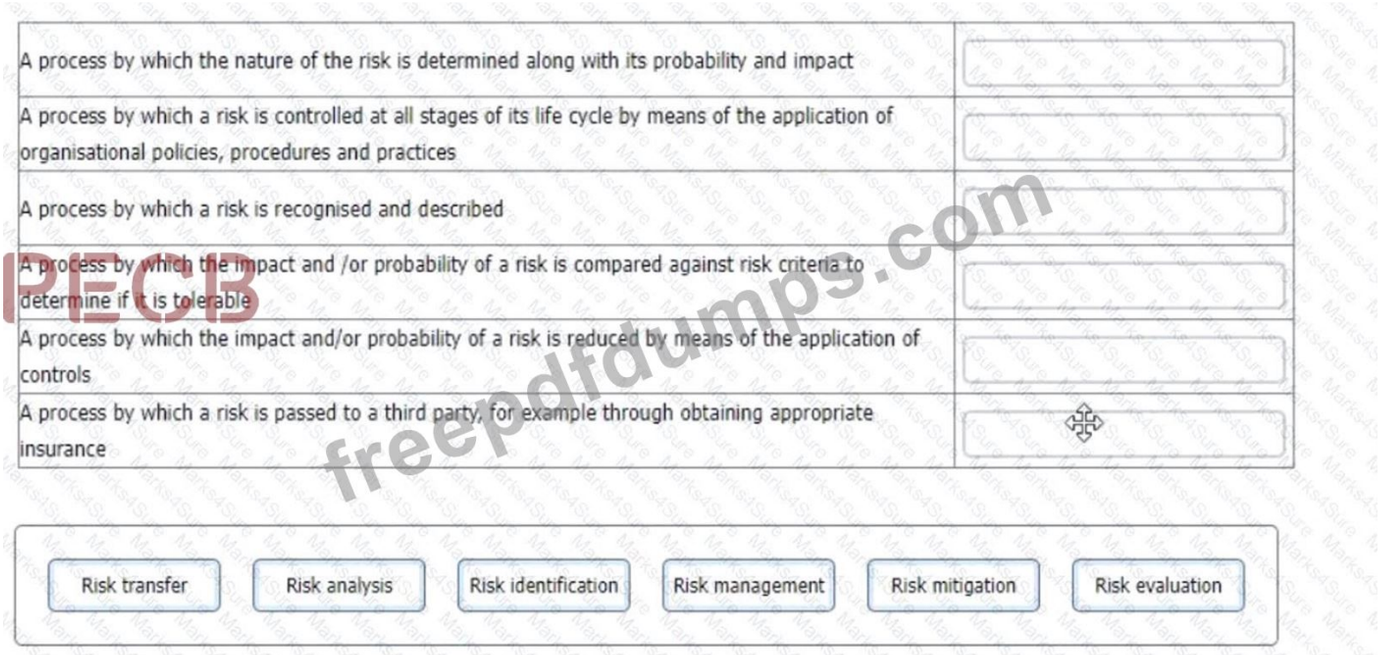
NEW QUESTION: 39
通過 ISO/IEC 27001 認證的組織範圍規定，他們提供編輯和網站託管服務。然而，由於組織的一些變化，與網站託管服務相關的技術支援已外包。在這種情況下是否應該口動範圍變更？
A. 是的，因為外在環境的任何變化都會引發範圍的變化
B. 否，因為變更不需要實施新的安全控制
C. 否，因為該組織已獲得編輯和網站託管服務認證
Answer: (SHOW ANSWER)

Yes, a change in the scope should be initiated because outsourcing a significant part of the service, such as technical support related to web hosting, could impact the risk landscape and the controls needed to manage those risks. This change affects the external environment and how the ISMS operates, necessitating a scope review and possible adjustment.
References: ISO/IEC 27001:2013, Clause 4.3 (Determining the scope of the information security management system)

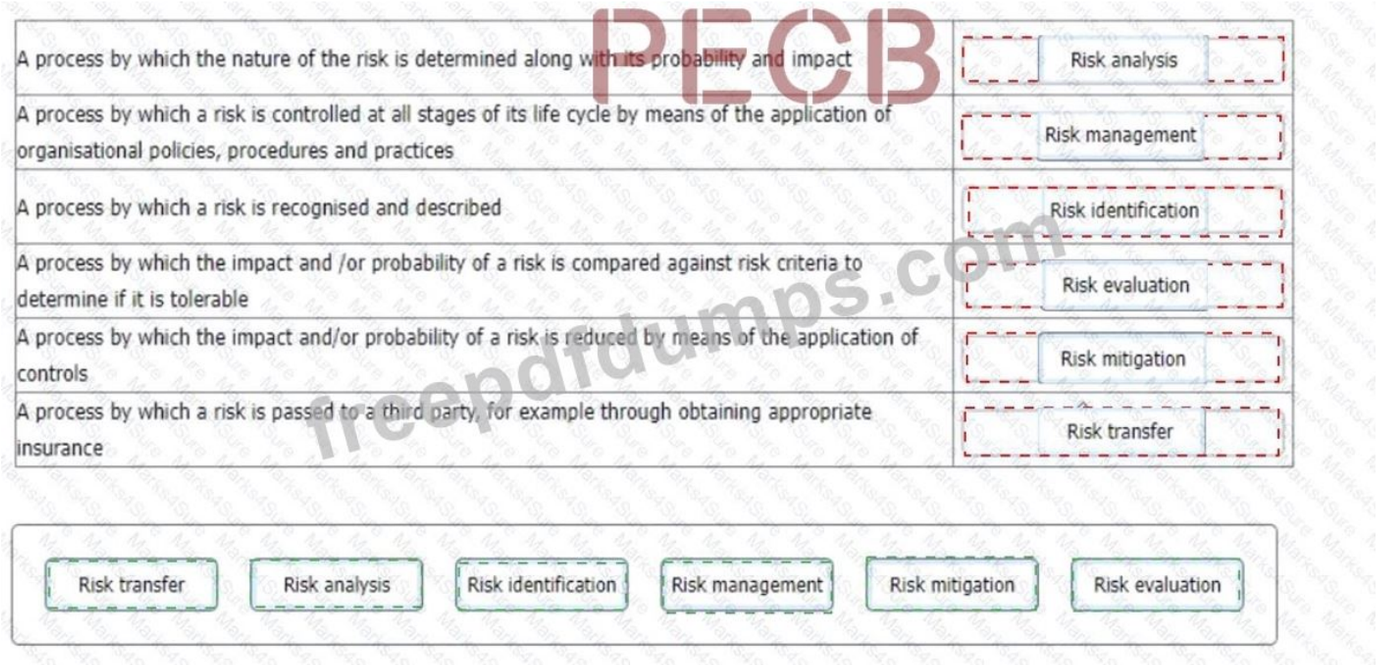
NEW QUESTION: 40
所有資訊資口的可接受使用均被禁止，但以下情況除外：
A. 電子連鎖信
B. 透過電子郵件將副本發送給非必要讀者
C. 經過主管/TL 許可的公司範圍口的電子郵件。
D. 帶有非常大附件或發送給大量收件者的郵件。
Answer: C (LEAVE A REPLY)
The only option that is not prohibited in acceptable use of information assets is C: company-wide e-mails with supervisor/TL permission. This option implies that the sender has obtained the necessary authorization from their supervisor or team leader to send an e-mail to all employees in the organization. This could be done for legitimate business purposes, such as announcing important news, events or updates that are relevant to everyone. However, this option should still be used sparingly and responsibly, as it could cause unnecessary disruption or annoyance to the recipients if abused or misused. The other options are prohibited in acceptable use of information assets, as they could violate the information security policies and procedures of the organization, as well as waste resources and bandwidth. Electronic chain letters (A) are messages that urge recipients to forward them to multiple other people, often with false or misleading claims or promises. They are considered spam and could contain malicious links or attachments that could compromise information security. E-mail copies to non-essential readers (B) are messages that are sent to recipients who do not need to receive them or have no interest in them. They are considered unnecessary and could clutter the inbox and distract the recipients from more important messages. Messages with very large attachments or to a large number of recipients (D) are messages that consume a lot of network resources and could affect the performance or availability of the information systems. They could also exceed the storage capacity or quota limits of the recipients' mailboxes and cause problems for them. ISO/IEC 27001:2022 requires the organization to implement rules for acceptable use of assets (see clause A.8.1.3). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology
- Security techniques - Information security management systems - Requirements, What is Acceptable Use?

NEW QUESTION: 41
您是一位經驗豐富的 ISMS 審核團隊領導，為審核員提供培訓指導。他們對風險流程的理解不清楚，並要求您向他們提供下面詳細介紹的每個流程的範例。

將提供的每項描述與下列風險管理流程之一相符。
要填寫表格，請按一下要填寫的空白部分，使其以紅色突出顯示，然後從下面的選項中按一下適用的文字。或者，您可以將每個選項拖曳到適當的空白部分。



Answer:



Explanation:

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

* Risk analysis is the process by which the nature of the risk is determined along with its probability and impact. Risk analysis involves estimating the likelihood and consequences of potential events or situations that could affect the organization's information security objectives or requirements12. Risk analysis could use qualitative or quantitative methods, or a combination of both12.
* Risk management is the process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices. Risk management involves establishing the context, identifying, analyzing, evaluating, treating, monitoring, and reviewing the risks that could affect the organization's information security performance or compliance12. Risk management aims to ensure that risks are identified and treated in a timely and effective manner, and that opportunities for improvement are exploited12.
* Risk identification is the process by which a risk is recognised and described. Risk identification involves identifying and documenting the sources, causes, events, scenarios, and potential impacts of risks that could affect the organization's information security objectives or requirements12. Risk identification could use various techniques, such as brainstorming, interviews, checklists, surveys, or historical data12.
* Risk evaluation is the process by which the impact and/or probability of a risk is compared against risk criteria to determine if it is tolerable. Risk evaluation involves comparing the results of risk analysis with predefined criteria that reflect the organization's risk appetite, tolerance, or acceptance12. Risk evaluation could use various methods, such as ranking, scoring, or matrix12. Risk evaluation helps to prioritize and decide on the appropriate risk treatment options12.
* Risk mitigation is the process by which the impact and/or probability of a risk is reduced by means of the application of controls. Risk mitigation involves selecting and implementing measures that are designed to prevent, reduce, transfer, or accept risks that could affect the organization's information security objectives or requirements12. Risk mitigation could include various types of controls, such as technical, organizational, legal, or physical12. Risk mitigation should be based on a cost-benefit analysis and a residual risk assessment12.
* Risk transfer is the process by which a risk is passed to a third party, for example through obtaining appropriate insurance. Risk transfer involves sharing or shifting some or all of the responsibility or liability for a risk to another party that has more capacity or capability to manage

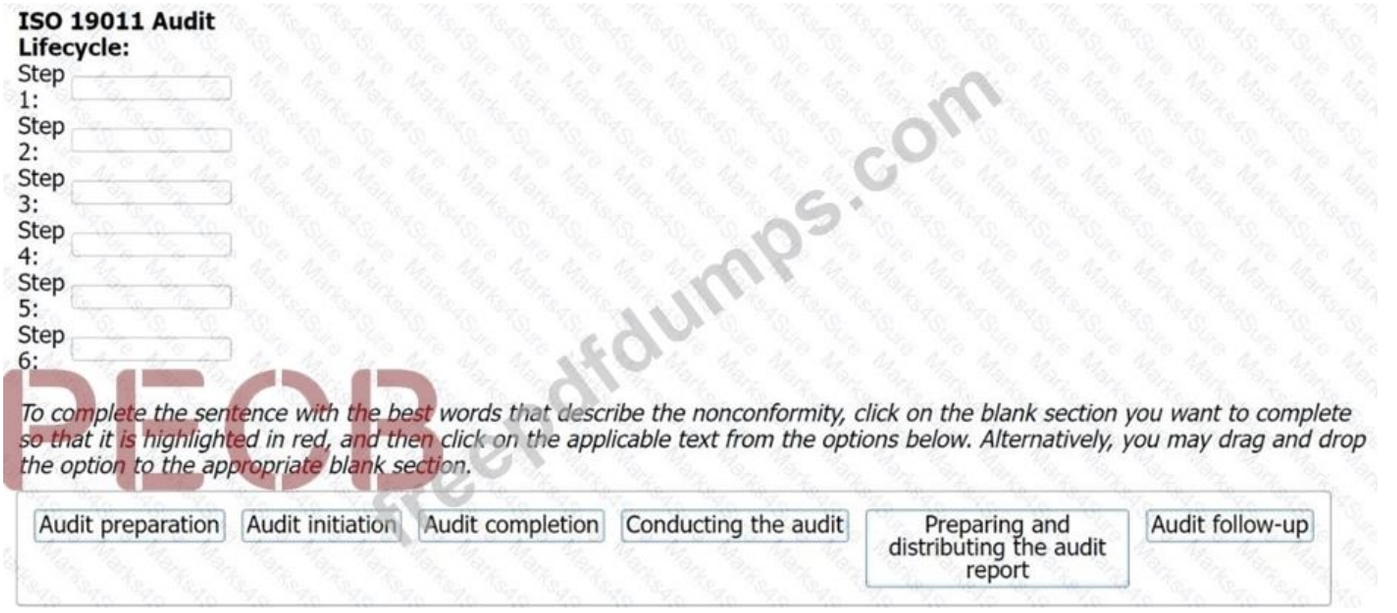
it12. Risk transfer could include various methods, such as contracts, agreements, partnerships, outsourcing, or insurance12. Risk transfer should not be used as a substitute for effective risk management within the organization12.
References :=
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management

NEW QUESTION: 42
哪一項不是 HR 在招募前的要求？
A. 接受背景驗證
B. 申請人必須完成就業前文件要求
C. 必須接受資訊安全意識訓練。
D. 必須成功通過背景調□
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, clause 7.2.2, the organization shall ensure that all persons who have access to information are aware of the information security policy and their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance2. Therefore, awareness training on information security is a requirement for all persons, not just new hires. References: ISO/IEC
27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

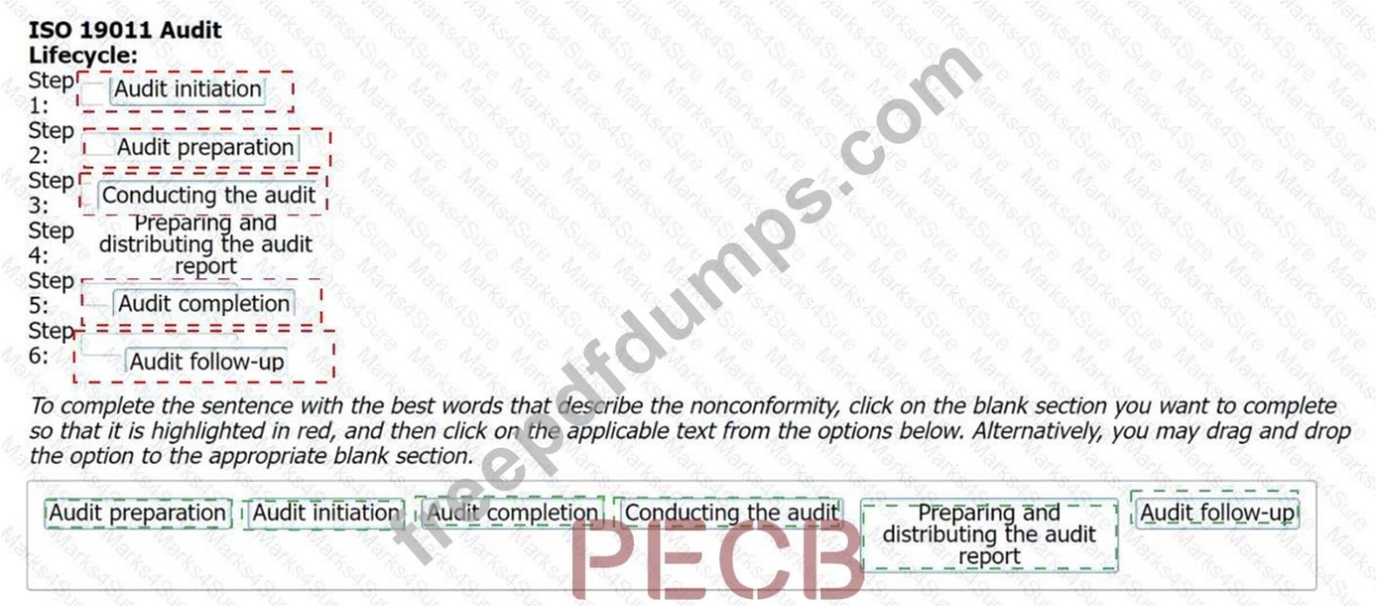
NEW QUESTION: 43
CEO發送一封電子郵件，表達他對公司現狀和公司未來策略的看法以及CEO的願景和員工在其中的角色。郵件應分類為
A. □部郵件
B. 公共郵件
C. 機密郵件
D. 受限郵件
Answer: (SHOW ANSWER)
The mail sent by the CEO giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it should be classified 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. 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: 44
選擇以下選項中的兩個，這些選項由審核團隊中的法律技術專家在認證審核期間負責。
A. 評估受審核方的法律知識
B. 批評組織的法律合規問題
C. 與受審核方討論複雜的法律問題
D. 為審核團隊提供法律檢口點建議
E. 驗證組織的合法地位
F. 會見該組織的法定代理人
Answer: D,E (LEAVE A REPLY)
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: 45
審核生命週期描述了進行單獨審核的 ISO 19011 流程。將審核生命週期的步驟拖曳到正確的順序中。



Answer:



Explanation:

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

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

This sequence reflects the logical order of the audit activities, from establishing the audit objectives, scope and criteria, to verifying the implementation and effectiveness of the corrective actions. However, ISO 19011:

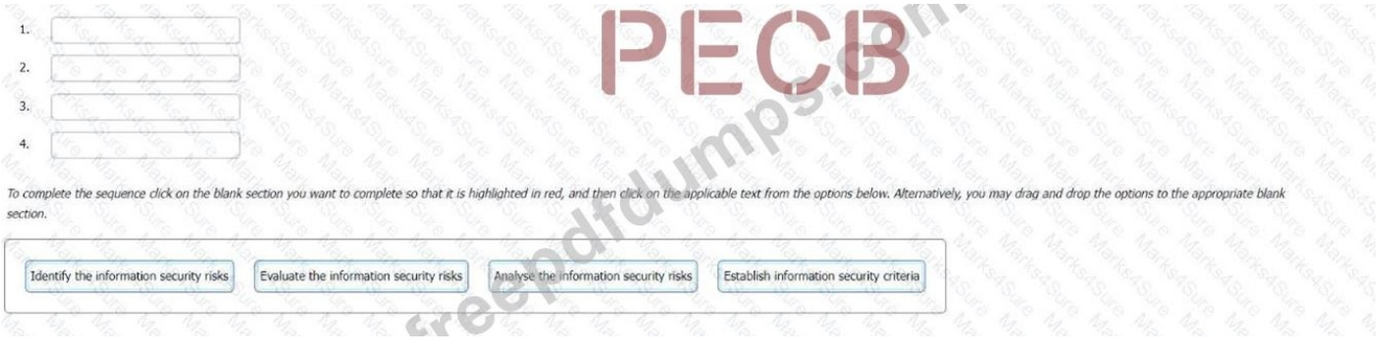
2018 also recognizes that some audit activities can be iterative or concurrent, depending on the nature and complexity of the audit. For example, audit preparation and conducting the audit can overlap when new information or changes occur during the audit. Similarly, audit follow-up can be

integrated with audit completion when the corrective actions are verified shortly after the audit. Therefore, the audit lifecycle should be adapted to the specific context and needs of each audit.

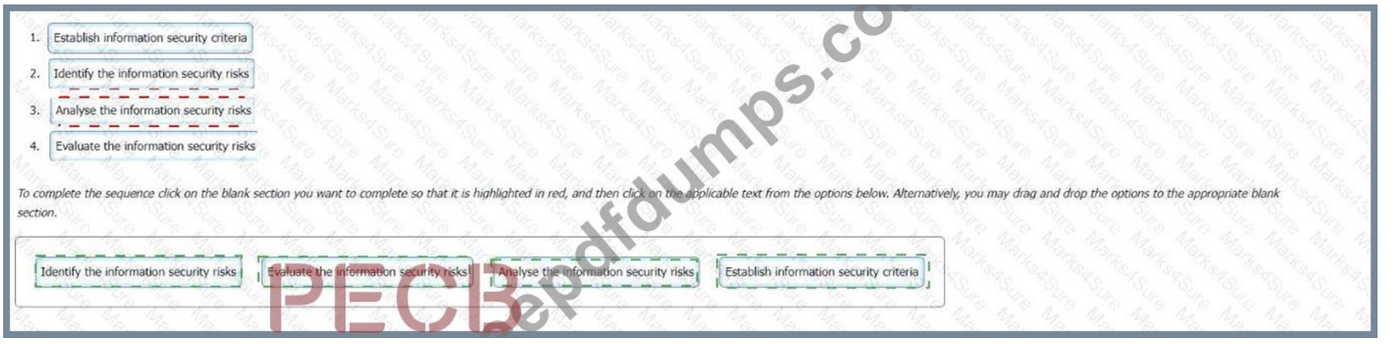
NEW QUESTION: 46
在第一階段審核開幕會議上，管理系統代表(MSR) 要求擴大審核範圍，以包括自提出認證申請以來已擴展到的海外新地點。
選擇審計員應如何回應的兩個選項。
A. 建議 MSR 可以納入範圍擴展，但必須履行既定程序
B. 通知 MSR 審核範圍已根據其初始申請確定，因此審核必須按計劃進行
C. 建議MSR取消審核合約並重新申請新情況
D. 確定管理系統是否涵蓋新站點的流程，如果是，則繼續審核
E. 通知MSR，在現有範圍口，可以毫無問題地包含新工作區
F. 確認審核員將通知受審核方審核範圍將被修改以包含新的工作領域
Answer: A,D (LEAVE A REPLY)
The correct options for how the auditor should respond are:
* A. Advise the MSR that an extension of the scope may be incorporated but will have to go through established procedures
* D. Determine whether the Management System covers the processes at the new site and, if so, proceed with the audit These options are consistent with the ISO/IEC 27006:2015 standard, which states that any changes to the scope of certification should be notified by the client to the certification body, and that the certification body should evaluate and decide on these changes in accordance with its procedures1. The auditor should also verify that the ISMS is implemented and maintained at all sites included in the scope of certification1.
The other options are not appropriate for how the auditor should respond, because:
* B. Advise the MSR that the audit scope has been determined based on their initial application so the audit has to proceed as planned: This option is too rigid and does not allow for any flexibility or adaptation to the client's situation. The auditor should be open to consider any changes to the scope of certification that may have occurred since the initial application, as long as they are properly notified and evaluated by the certification body.
* C. Suggest that the MSR cancels the audit contract and reapplies for the new situation: This option is too drastic and unnecessary, as it would cause delays and costs for both the client and the certification body. The auditor should not suggest that the client cancels the audit contract, but rather that they follow the established procedures for requesting and approving an extension of the scope of certification.
* E. Advise the MSR that, within the existing scope, the new work area can be included without any problem: This option is too lenient and does not ensure that the new work area meets the requirements of ISO/IEC 27001 and the ISMS. The auditor should not assume that the new work area can be included within the existing scope without any problem, but rather that they need to verify that the ISMS is implemented and maintained at the new site, and that any changes to the scope of certification are approved by the certification body.

* F. Confirm that the auditor will advise the auditee that the audit scope will be revised to include the new work area: This option is too presumptuous and does not respect the authority of the certification body.
The auditor should not confirm that they will revise the audit scope to include the new work area, but rather that they will advise the certification body of the client's request for an extension of the scope of certification, and wait for their decision.

NEW QUESTION: 47
為 ISMS 中的資訊安全風險評估流程選擇正確的順序。
要完成序列，請按一下要完成的空白部分，使其以紅色突出顯示，然後從下面的選項中按一下適用的文字。或者，您可以將選項拖曳到適當的空白處



Answer:



Explanation:

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

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

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: 48

您是一位經驗豐富的審核團隊負責人，負責為其客口設計網站的組織進行第三方監督審核。您目前正在審口該組織的適用性聲明。

根據 ISO/IEC 27001 的要求，下列關於適用性聲明的觀察哪兩項是錯誤的？

A. 如果組織選擇這樣做，則可以將附錄A 中未包含的其他控制措施新增至適用性聲明中

B. 適用性聲明必須包括必要的組織、物理、人員和技術控制

C. 需要口明在適用性聲明中包含和排除附件 A 控制措施的理由

D. 僅需要對組織選擇排除的任何控制進行口明

E. 適用性聲明由組織的最高管理階層擁有和修改

F. 尋求 ISO/IEC 27001 合規性的組織必須出具適用性聲明

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 49

您正在一家提供醫療保健服務的住宅療養院進行 ISMS 審核。審核計畫的下一步是驗證資訊安全事件管理流程。IT 安全經理介紹了資訊安全事件管理程序，並解釋該流程基於ISO/IEC 27035-1:2016。

您□看該文件並注意到一條聲明「任何資訊安全弱點、事件和事故應在識別後 1 小時□報告給聯絡人 (PoC)」。在訪問員工時，您發現大家對「弱點、事件、事件」意義的理解有差異。

您從事件追蹤系統中抽取過去 6 個月的事件報告記錄樣本，總結結果如下表所示。

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

您想進一步調□其他領域以收集更多審計證據。選擇兩個不會出現在您的審核追蹤中的選項。

A. 透過訪問更多員工了解他們對報告流程的理解來收集更多證據。（與控制措施A.6.8 相關）

B. 收集更多關於公司如何以及何時支付贖金以解鎖公司手機和資料（即信用卡和銀行轉帳）的證據。（與控制措施A.5.26 相關）

C. 收集更多有關人力資源經理如何以及何時支付贖金以解鎖個人行動資料（即信用卡和銀行轉帳）的證據。（與控制措施A.5.26 相關）

D. 收集更多有關組織如何確定事件恢復時間的證據。（與控制措施A.5.27 相關）

E. 收集更多證據，□明組織如何確定事件發生後無需採取進一步行動。（與控制措施A.5.26 相關）

F. 收集更多有關事件恢復程序的證據。（與控制措施A.5.26 相關）

Answer: B,C (LEAVE A REPLY)

*C. Collect more evidence on how and when the Human Resources manager pays the ransom fee to unlock personal mobile data, i.e., credit card, and bank transfer. (Relevant to control A.5.26) This is not relevant to the audit of the organization's incident management process. The HR manager's personal phone and how they handle a ransomware attack on it falls outside the scope of the ISMS audit. The organization is not responsible for personal devices.
*B. Collect more evidence on how and when the company pays the ransom fee to unlock the company's mobile phone and data, i.e., credit card, and bank transfer. (Relevant to control A.5.26) While seemingly relevant, this focuses on the method of payment for the ransom. The core issue is the organization paying the ransom at all, which is generally not best practice in incident response. The audit should focus on why this decision was made and if alternative solutions were considered (e.g., data backups, device wiping and restoration).
Why the other options ARE relevant:
*A. Collect more evidence by interviewing more staff about their understanding of the reporting process.
(Relevant to control A.6.8) This directly addresses the identified discrepancy in understanding "weakness, event, and incident," which is crucial for proper incident reporting.
*D. Collect more evidence on how the organisation determined the incident recovery time. (Relevant to control A.5.27) This investigates the basis for the 24-hour recovery time, which seems arbitrary and may not be appropriate for all incidents.
*E. Collect more evidence on how the organization determined no further action was needed after the incident. (Relevant to control A.5.26) This probes the adequacy of the incident response, especially the lack of preventative measures after paying the ransom.
*F. Collect more evidence on the incident recovery procedures. (Relevant to control A.5.26) This examines the actual procedures to assess their effectiveness and alignment with best practices.

NEW QUESTION: 50
您是一位經驗豐富的 ISMS 審核團隊負責人，負責對專門從事機密文件和可移動媒體安全處置的組織進行第三方認證審核。文件和媒體都被軍用級設備粉碎，因此無法重建原始文件。
審核進展順利，距離末次會議還有30 分鐘，您正要開始撰寫審核報告。此時，組織的一名員工敲響了您的門，詢問是否可以與您交談。他們告訴您，當事情變得繁忙時，她的經理會告訴她使用較低等級的工業碎紙機，因為該組織擁有更多此類碎紙機並且運行速度更快。受審核方沒有告知您這些機器的存在或使用情況。
選擇三個選項來決定您應如何回應此訊息。
A. 向管理審核計劃的個人建議您在認證之前進行進一步審核的任何建議
B. 取消審核報告的製作，轉而審□組織與其客□的合同，以確定他們是否允許使用較低等級的機器
C. 根據已發現的其他信息，考慮是否需要在4 週□進行後續審核
D. 什麼都不做。所有審核均基於樣本，您採集的樣本不包括較低等級機器的計劃審□
E. 延長認證審核持續時間，以騰出更多時間來審核較低等級機器的使用情況
F. 由於組織尚未公開其流程，因此提出不符合8.1 營運規劃與控制的要求
G. 與受審核方核實在某些情況下是否使用了較低等級的機器

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

According to ISO/IEC 27001:2022 clause 8.1, the organization must plan, implement and control the processes needed to meet the information security requirements, and to implement the actions determined in clause 6.1. The organization must also ensure that the outsourced processes are controlled or influenced.

According to control A.5.24, the organization must establish and maintain an information security incident management process that includes reporting information security events and weaknesses. Therefore, the use of lower grade machines for the secure disposal of confidential documents and media could pose a significant information security risk and a potential breach of contract with the clients. The auditor should respond to this information by:

* A. Advising the individual managing the audit programme of any recommendation by you to conduct a further audit prior to certification. This is in accordance with ISO/IEC 27006:2022 clause 7.4.3, which states that the audit team leader shall report to the certification body any situation that may significantly affect the audit conclusions or the certification decision, and propose any necessary changes to the audit plan.
* C. Considering the need for a subsequent audit within 4 weeks based on the additional information that has come to light. This is in accordance with ISO/IEC 27006:2022 clause 7.5.2, which states that the audit team leader shall review the audit findings and any other appropriate information collected during the audit to determine the audit conclusions, and to identify any need for a subsequent audit.
* G. Verifying with the auditee that lower grade machines are used in certain circumstances. This is in accordance with ISO/IEC 27006:2022 clause 7.4.2, which states that the audit team leader shall ensure that the audit is conducted in accordance with the audit plan, and that any changes to the plan are agreed upon and documented.

The other options are not appropriate responses, as they either ignore the information, exceed the scope of the audit, or prematurely raise a nonconformity without sufficient evidence. For example:

* B. Cancelling the production of the audit report and instead reviewing the organization's contracts with its clients to determine whether they have permitted the use of lower grade machines. This is not a suitable response, as it would delay the audit process and the certification decision, and it would involve reviewing documents that are outside the scope of the ISMS audit. The auditor should focus on verifying the information security risk assessment and treatment process, and the information security incident management process, as they relate to the use of lower grade machines.
* D. Doing nothing. All audits are based on a sample and the sample you took did not include a planned review of the lower grade machines. This is not a suitable response, as it would disregard a significant information security risk and a potential nonconformity that could affect the audit conclusions and the certification decision. The auditor should follow up on the information provided by the employee and verify its validity and impact.
* E. Extending the certification audit duration to create additional time to audit the use of the lower grade machines. This is not a suitable response, as it would disrupt the audit schedule and the

availability of the audit team and the auditee. The auditor should report the situation to the certification body and propose any necessary changes to the audit plan, such as conducting a subsequent audit.
* F. Raising a nonconformity against 8.1 Operational Planning and Control as the organization has not been open about its processes. This is not a suitable response, as it would be based on a single source of information that has not been verified or corroborated. The auditor should collect sufficient and appropriate audit evidence to support any nonconformity, and should also consider the root cause and the severity of the nonconformity.
References:
* ISO/IEC 27001:2022, clauses 8.1 and Annex A control A.5.24
* ISO/IEC 27006:2022, clauses 7.4.2, 7.4.3, and 7.5.2
* [PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 18-19, 23-24
* A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit
* ISO 27001 - Annex A.16: Information Security Incident Management

NEW QUESTION: 51
本組織擁有第三方認證機構核發的 ISO/IEC 27001 資訊安全管理系統 (ISMS) 認證。下列哪一項代表了擁有認可認證的優點？
A. 組織□品的行銷價格上漲
B. 客□端數量增加
C. 審核報告的清晰度
D. 對認證過程可信度的認可。
Answer: D (LEAVE A REPLY)
One of the advantages of having accredited certification of ISMS to ISO/IEC 27001:2022 is that it demonstrates the recognition of the credibility of the certification process. Accredited certification means that the certification body has been assessed and approved by an accreditation body, which ensures that the certification body operates according to international standards and follows impartiality, competence and consistency principles. Accredited certification also enhances the confidence of the organisation's customers, partners, regulators and other interested parties in the organisation's information security performance and compliance.
References: = ISO/IEC 27001:2022, clause 0.2; [PECB Candidate Handbook ISO 27001 Lead Auditor], page 6; Key Benefits of ISO 27001 Certification - IT Governance.

NEW QUESTION: 52
您正在一家提供醫療保健服務的住宅療養院進行 ISMS 審核。審核計畫的下一步是驗證資訊安全事件管理流程。IT 安全經理介紹了資訊安全事件管理程序（文件參考ID :ISMS_L2_16，版本4），並解釋此流程基於 ISO/IEC 27035-1:2016。
您□看該文件並注意到一條聲明「任何資訊安全弱點、事件和事故應在識別後 1 小時□報告給聯絡人 (PoC)」。在訪問員工時，您發現大家對「弱點、事件、事件」意義的理解有差異。

IT安全經理解釋口，6個月前舉辦了一次線上 資訊安全應對」培訓研討會。所有受訪者均參與並通過了報告練習和課程評估。
您正在準備審計結果。選擇兩個正確的選項。
A. 存在不合格項 (NC)。資訊安全事件培訓失敗。這不符合第 7.2 條和控制措施 A.6.3。
B. 存在不合格項 (NC)。事件管理報告流程的術語不明確，員工對 弱點、事件和事件」意義的誤解證明了這一點。這不符合第 9.1 條和控制措施 A.5.24。
C. 還有改進的機會 (OFI)。提高資訊安全事件訓練效果。這與第 7.2 條和控制措施 A.6.3 相關。
D. 有改進的機會 (OFI)。報告資訊安全弱點、事件和事件。這與第 9.1 條和控制措施 A.5.24 有關。
E. 沒有不合格項。資訊安全處置訓練卓有成效。這符合第 7.2 條和控制措施 A.6.3。
F. 沒有不合格項。報告資訊安全弱點、事件和事故。
這符合第 9.1 條和控制措施 A.5.24。
Answer: B,C (LEAVE A REPLY)
According to ISO/IEC 27001:2022 clause 7.2, the organization must ensure that the persons doing work under its control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. The organization must also provide information security awareness education and training to its personnel and relevant interested parties. According to control A.6.3, the organization must ensure that all employees and contractors are made aware of the information security incident management procedures and their expected roles and responsibilities. Therefore, an opportunity for improvement (OFI) can be identified if the information security incident training effectiveness can be improved, as evidenced by the differences in the understanding of the meaning of "weakness, event, and incident" among the staff.
According to ISO/IEC 27001:2022 clause 9.1, the organization must monitor, measure, analyze and evaluate the information security performance and the effectiveness of the ISMS. The organization must also retain appropriate documented information as evidence of the monitoring and measurement results. According to control A.5.24, the organization must establish and maintain an information security incident management process that includes the following activities:
*reporting information security events and weaknesses;
*assessing and deciding on information security events;
*responding to information security incidents;
*learning from information security incidents;
*collecting evidence and disclosing information.
Therefore, a nonconformity (NC) can be identified if the terminology of the incident management reporting process is unclear, as evidenced by the staff misunderstanding of the meaning of "weakness, event, and incident". This could lead to inconsistent or inaccurate reporting, assessment, response, learning, and disclosure of information security incidents, which could affect the information security performance and the effectiveness of the ISMS.
References:

*ISO/IEC 27001:2022, clauses 7.2, 9.1, and Annex A controls A.5.24 and A.6.3
*[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 15-16, 18-19, 22-23
*ISO/IEC 27035-1:2016, clauses 4, 5, 6, 7, and 8
*ISO 27001 - Annex A.16: Information Security Incident Management
*ISO 27001:2022 Annex A Control 5.24 - What's New?

NEW QUESTION: 53
您正在一家名為 ABC 的提供醫療保健服務的住宅療養院進行 ISMS 審核。
審核計劃的下一步是驗證 ABC 醫療保健行動應用程式開發、支援和生命週期流程的資訊安全性。在審核過程中，您了解到該組織將行動應用程式開發外包給了經過CMMI 5 級、ITSM (ISO/IEC 20000-1)、BCMS (ISO 22301) 和ISMS (ISO/IEC 27001) 認證的專業軟體開發組織。
IT經理介紹了軟體安全管理流程，並將流程總結如下：
行動應用程式開發至少應採用「設計安全」和「預設安全」原則。應具備以下個人資料保護安全功能：
存取控制。
個人資料加密，即高階加密標準(AES）演算法，金鑰長度256位元；個人資料假名化。
已檢口漏洞，無安全後門
您採樣最新的行動應用測試報告 - 參考 ID :0098，詳細資訊如下：

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

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

您想進一步調口其他領域以收集更多審計證據。選擇三個不會出現在您的審核追蹤中的選項。

A. 收集更多證據，了解居民家庭成員為安裝ABC 的醫療保健行動應用程式支付的費用。（與第4.2 條相關）

B. 透過在手機上下載並測試行動應用程式來收集更多證據。（與控制A.8.1 相關）

C. 收集更多證據以確定 ABC 醫療保健行動應用程式的使用者數量。（與第4.2條相關）

D. 收集更多有關組織如何執行個人資料處理測試的證據。（與控制措施A.5.34 相關）

E. 收集更多有關組織業務連續性政策的證據。（與控制措施A.5.30 相關）

F. 收集更多有關組織在選擇外部服務提供者時如何管理資訊安全的證據。（與控制措施A.5.19 相關）

G. 收集更多有關開發人員如何培訓其口品支援人員的證據。（與第7.2條相關）

H. 收集更多證據來驗證開發人員的 CMMI Level 5、ITSM (ISO/IEC 20000-1)、BCMS (ISO22301) 和 ISMS (ISO/IEC 27001) 認證。（與控制措施A.5.21 相關）

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

The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13.

References: 1: ISO
/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 54

您正在療養院進行 ISMS 審核，療養院的住口總是戴著電子腕帶來監測他們的位置、心跳和血壓。腕帶會自動將這些資料上傳到雲端伺服器，供工作人員進行醫療保健監控和分析。
您現在希望驗證最高管理層是否已製定資訊安全策略和目標。您正在對行動裝置策略進行抽樣，並確定該策略的安全目標是「確保遠端辦公和行動裝置使用的安全」。
禁止個人行動裝置連接至療養院網路、處理和儲存居民資料。
本公司在ISMS範圍口的行動裝置應在資口登記冊中登記。
本公司的行動裝置應實施或口用實體保護，即密碼保護的螢幕鎖定解鎖、臉部或指紋解鎖裝置。
本公司的行動裝置應定期備份。
若要驗證行動裝置策略和目標是否已實施且有效，請為稽核追蹤選擇三個選項。
A. 與接待人員面談，確保在進入療養院之前檢口所有訪客和員工的行李
B. 口看訪客登記簿，確保任何訪客都不能在療養院口攜帶個人手機
C. 口看口部審核報告以確保 IT 部門已接受審核
D. 檢口資口註冊以確保所有個人行動裝置已註冊
E. 從口班醫護人員處抽取部分行動設備，並與資口登記冊驗證行動裝置資訊
F. 檢口資口註冊以確保所有公司的行動裝置已註冊
G. 採訪設備供應商，確保他們了解ISMS 政策
H. 與高階主管面談，核實他們參與制定資訊安全政策和資訊安全目標的情況
Answer: C,E,F (LEAVE A REPLY)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 5.2 requires top management to establish an information security policy that provides the framework for setting information security objectives1. Clause 6.2 requires top management to ensure that the information security objectives are established at relevant functions and levels1. Therefore, when verifying that the information security policy and objectives have been established by top management, an ISMS auditor should review relevant documents and records that demonstrate top management's involvement and commitment.
To verify that the mobile device policy and objectives are implemented and effective, an ISMS auditor should review relevant documents and records that demonstrate how the policy and objectives are communicated, monitored, measured, analyzed, and evaluated. The auditor should also sample and verify the implementation of the controls that are stated in the policy.
Three options for the audit trail that are relevant to verifying the mobile device policy and objectives are:
* Review the internal audit report to make sure the IT department has been audited: This option is relevant because it can provide evidence of how the IT department, which is responsible for managing the mobile devices and their security, has been evaluated for its conformity and effectiveness in implementing the mobile device policy and objectives. The internal audit report can also reveal any nonconformities, corrective actions, or opportunities for improvement related to the mobile device policy and objectives.
* Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register: This option is relevant because it can provide evidence of how

the mobile devices that are used by the medical staff, who are involved in processing and storing residents' data, are registered in the asset register and have physical protection enabled. This can verify the implementation and effectiveness of two of the controls that are stated in the mobile device policy.
* Review the asset register to make sure all company's mobile devices are registered: This option is relevant because it can provide evidence of how the company's mobile devices that are within the ISMS scope are identified and accounted for. This can verify the implementation and effectiveness of one of the controls that are stated in the mobile device policy.
The other options for the audit trail are not relevant to verifying the mobile device policy and objectives, as they are not related to the policy or objectives or their implementation or effectiveness. For example:
* Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding physical security or access control, but not specifically to mobile devices.
* Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security awareness or compliance, but not specifically to mobile devices.
* Interview the supplier of the devices to make sure they are aware of the ISMS policy: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security within supplier relationships, but not specifically to mobile devices.
* Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to verifying that the information security policy and objectives have been established by top management, but not specifically to mobile devices.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 55
網路釣魚屬於什麼類型的資訊安全事件？
A. 私人事件
B. 破解者/駭客攻擊
C. 技術漏洞
D. 法律事件
Answer: B (LEAVE A REPLY)

Phishing is a type of information security incident that falls under the category of cracker/hacker attacks.
Phishing is a form of fraud that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information.
Phishing is a common and serious threat to information security, as it can lead to identity theft, financial loss, data breach, malware infection or other damages. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2).
References: CQI & IRCA Certified ISO/IEC
27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Phishing?

NEW QUESTION: 56
場景9 :UpNet是一家網路公司，已通過SO/IEC 27001認證。
自從獲得 ISO/IEC 27001 認證以來，該公司的認可度大幅提高。此認證證實了 UpNefs 營運的成熟性及其符合廣泛認可和接受的標準。
但認證之後一切還沒結束。UpNet 透過進行口部稽核不斷審口和增強其安全控制以及 ISMS 的整體有效性和效率。高階主管不願意聘請全職口部稽核團隊，因此決定將口部稽核職能外包。這種形式的口部稽核確保了獨立性、客觀性，並且在ISMS 的持續改進方面發揮諮詢作用。
在初次認證審核後不久，該公司創建了一個專門從事數據和儲存口品的新部門。他們提供針對資料中心和基於軟體的網路設備（例如網路虛擬化和網路安全設備）進行最佳化的路由器和交換器這導致 ISMS 認證範圍口已涵蓋的其他部門的營運發生變化。
所以。UpNet 口動了風險評估流程和口部稽核。根據口部審計結果，公司確認了現有和新流程和控制的有效性和效率。
由於新部門符合 ISO/IEC 27001 要求，最高管理層決定將其納入認證範圍。UpNet宣布取得ISO/IEC 27001認證，認證範圍涵蓋全公司。
在初次認證審核一年後，認證機構對UpNefs ISMS 進行了另一次審核。
此次審核旨在確定 UpNefs ISMS 是否符合指定的 ISO/IEC 27001 要求，並確保ISMS 持續改善。審核小組確認，經過認證的ISMS 繼續符合標準的要求。儘管如此，新部門對管理體系的治理口生了重大影響。此外，認證機構並未獲悉任何變更。因此，UpNefs認證被暫停。
根據上述場景，回答以下問題：
UpNet 將口部稽核職能外包，如場景9 所示。
A. 不，口部稽核不一定必須是獨立且客觀的，因為它們具有諮商作用
B. 否，因為口部審核流程不僅僅包含審核計劃
C. 是的，它提高了口部稽核的獨立性和公正性，因為審計員不具有與SMS 相關的營運角色
Answer: (SHOW ANSWER)

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

NEW QUESTION: 57
您會在某些實體資口上看到藍色貼紙。這意味著什麼？
A. 資口非常重要，其故障會影響整個組織
B. 帶有藍色貼紙的資口應始終保持空調狀態
C. 資口非常關鍵，其故障將影響組織中小組專案的工作
D. 資口至關重要，影響力僅限於員工
Answer: (SHOW ANSWER)
You see a blue color sticker on certain physical assets. This signifies that the asset is high critical and its failure will affect a group/s/project's work in the organization. A blue color sticker is a type of label that indicates the level of criticality of an asset, which is a measure of how important an asset is for the organization's operations and objectives. A high critical asset is an asset that has a significant impact on the organization's activities, and its loss or damage would cause major disruption or loss of service. A blue color sticker also implies that the asset requires a high level of protection and security, and should be handled with care. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36. : [ISO/IEC 27001 Brochures | PECB], page 6.

NEW QUESTION: 58
您是認證機構審核員，負責對為ICT 設施提供託管服務的客口營運的資料中心進行 ISO/IEC 27001:2022 監督審核。
您和您的導遊目前位於客口出租給客口的私人套房之一。每間套房的出入均使用密碼鎖進行控制。每間套房也安裝了閉路電視。
每個套件口有三個資料櫃，客口可以在其中放置關鍵任務伺服器和其他網路設備，例如交換器和路由器。
您注意到，雖然套房中的兩個櫃子已上鎖，但第三個櫃子卻未上鎖你問導遊為什麼。他們回覆「這是因為客口目前正在更換硬碟單元。他們的技術人員目前正在午休」。
接下來你應該採取哪三項行動？
A. 什麼也不做，房間看起來受到了充分的保護，因此不太可能發生安全事件
B. 針對控制措施 5.16「身分管理」提出不符合項，因為可能無法辨識誰未上鎖櫃子。
C. 針對控制措施 7.2「實體進入」提出不符合項，因為客口設備所在的區域不受保護
D. 針對控制措施 7.4「實體安全監控」提出不符合項，因為私人套房未持續受到未經授權的實體存取監控。
E. 提出改進的機會，建議每當客口離開套房時就鎖上櫃門，即使他們打算在短時間口返回
F. 口看閉路電視記錄，確保自上次確認櫃子鎖定以來只有客口曾造訪過櫃子。
G. 當技術人員吃完午餐回來時，斥責他們沒有打開櫃子。
H. 在嚮導許可的情況下，與客口聯繫以確認他們正在更換驅動器

Answer: E,F,H (LEAVE A REPLY)
Leaving the cabinet unlocked while the technician is on a lunch break exposes the client's equipment and data to potential physical security risks, such as theft, damage, or tampering. This is a violation of the ISO/IEC
27001:2022 requirements for physical entry (control 7.2) and physical security monitoring (control 7.4), which aim to prevent unauthorized access to information processing facilities and assets. Therefore, the appropriate actions for the auditor are:
* Raise an opportunity for improvement (OFI) suggesting that the cabinet doors are locked whenever clients leave their suites, even if they intend to return within a short time. This would enhance the security of the client's equipment and data, and reduce the likelihood of security incidents.
* Review the CCTV records to ensure that only the client has accessed the cabinet since it was last confirmed as locked. This would verify the integrity and availability of the client's equipment and data, and identify any possible unauthorized access or interference.
* With the permission of the guide, speak to the customer to confirm that they are in the process of swapping out a drive. This would validate the reason for leaving the cabinet unlocked, and assess the impact and risk of the activity on the client's information security.
References: =
* ISO/IEC 27001:2022, clause 7.2, Physical entry
* ISO/IEC 27001:2022, clause 7.4, Physical security monitoring
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION: 59
場景 1 :Fintive 是一家傑出的線上支付和保護解決方案安全提供者。Fintive 於 1999 年由 Thomas Fin 在加州聖荷西創立，為線上營運、希望提高資訊安全、防止詐欺並保護 PII 等用口資訊的公司提供服務。Fintive的決策和營運流程以以往的案例為中心。他們收集客口數據，根據情況進行分類並進行分析。該公司需要大量員工才能進行如此複雜的分析。然而，幾年後，協助進行此類分析的技術也取得了進展。現在，Fintive 正計劃使用現代工具聊天機器人來實現模式分析，以即時防止詐騙。該工具也將用於幫助改善客口服務。
這個最初的想法已傳達給軟體開發團隊，他們支持該想法並被分配從事該專案。他們開始將聊天機器人整合到現有系統中。此外，團隊也為聊天機器人設定了一個目標，即回答85% 的聊天口詢。聊天機器人成功整合後，該公司立即將其發布給客口使用。
然而，聊天機器人似乎存在一些問題。
由於測試不足，並且在訓練階段缺乏向聊天機器人提供的樣本（在訓練階段，聊天機器人本應學習」口詢模式），因此聊天機器人無法解決用口口詢並提供正確的答案。此外，當聊天機器人收到無效輸入（例如奇怪的點圖案和特殊字元）時它會向使用者發送隨機檔案。因此，聊天機器人無法正確回答客口的口詢，而傳統的客口支援因聊天口詢而不堪重負，因此無法幫助客口解決他們的請求。
因此，Fintive 制定了軟體開發政策。該政策規定，無論軟體是口部開發還是外包，在作業系統上實施之前都將經過黑盒測試。

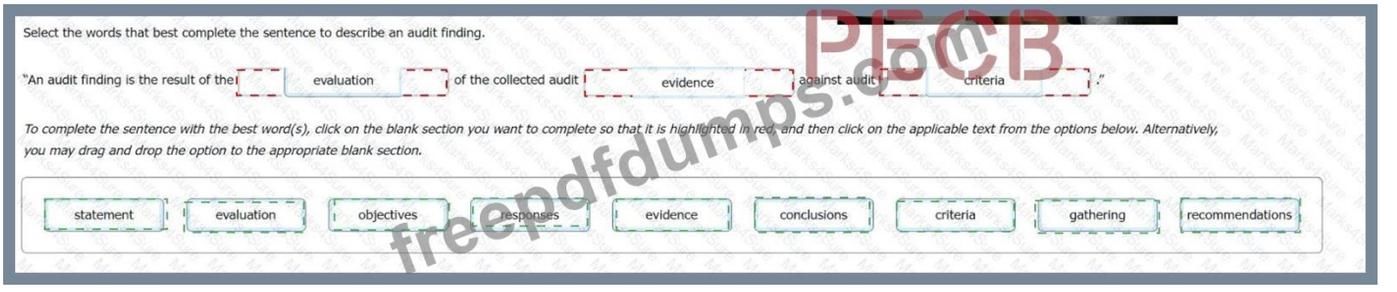
根據該場景，回答以下問題：
根據場景 1，聊天機器人無法正確回答客口的詢問。本案影響了資訊安全的哪些原則？
A. 可用性
B. 誠信
C. 保密性
Answer: (SHOW ANSWER)
The integrity principle of information security has been affected in this case. The chatbot's inability to provide accurate answers and its unintended behavior (sending random files) due to insufficient testing and lack of proper training samples compromised the integrity of the system.

NEW QUESTION: 60
您是經驗豐富的審核團隊領導，指導審核員進行培訓。
您的團隊目前正在對代表外部客口儲存資料的組織進行第三方監督審核。接受培訓的審核員的任務是審口適用性聲明 (SoA) 中列出的並在現場實施的實體控制措施。
從以下口容中選擇您希望接受培訓的審核員審口的四項控制措施。
A. 進出裝載區的通道
B. 電源線和資料線如何進入建築物
C. 資訊安全意識、教育與培訓
D. 對人員進行驗證檢口
E. 資訊資口清單的開發與維護
F. 現場閉路電視和門禁系統的運行
G. 組織維護設備的安排
H. 組織的業務連續性安排
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: 61

Answer:



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

NEW QUESTION: 62
您是 ISMS 審核小組組長，準備在第三方監督審核後主持閉幕會議 您正在起草閉幕會議議程，列出您希望與受審核方討論的主題。
下列哪一項適合納入？
A. 認證機構申訴流程的詳細口明
B. 審核計畫及其目的的解釋
C. 關於審核結果基於證據抽樣的免責聲明
D. 與不合格項相關的審核方名稱
Answer: (SHOW ANSWER)

This option is appropriate for inclusion in the closing meeting agenda, as it is a requirement of the ISO 19011 standard, which provides guidelines for auditing management systems, including ISMS12. The standard states that the audit team leader should advise the auditee of any situations encountered during the audit that may decrease the confidence that can be placed in the audit conclusions, such as limitations in the audit scope, access, or sampling3. The standard also states that the audit report should include a statement that the audit is based on a sample of the information available at the time of the audit, and that the audit does not provide absolute assurance of the conformity or effectiveness of the audited management system4. Therefore, the audit team leader should include a disclaimer in the closing meeting agenda to inform the auditee of the nature and limitations of the audit, and to avoid any misunderstandings or false expectations. The other options are not appropriate for inclusion in the closing meeting agenda, as they are either irrelevant, incorrect, or incomplete. For example:
*A detailed explanation of the certification body's complaints process is not relevant for the closing meeting agenda, as it is not related to the audit findings or conclusions. The certification body's complaints process should be communicated to the auditee before the audit, as part of the audit agreement or contract5.
*An explanation of the audit plan and its purpose is not correct for the closing meeting agenda, as it should have been done at the opening meeting or before the audit. The audit plan is a document that describes the scope, objectives, criteria, and methodology of the audit, as well as the audit schedule, the audit team, the audit locations, and the audit deliverables . The audit plan should be communicated and agreed with the auditee in advance, and any changes or deviations should be notified during the audit.
*Names of auditees associated with nonconformities are not complete for the closing meeting agenda, as they do not provide the details or the evidence of the nonconformities. The audit team leader should present the audit findings, which include the description, the audit criteria, and the audit evidence of each nonconformity, as well as the audit conclusions and the audit recommendation . The audit team leader should also avoid naming or blaming individuals, and focus on the processes and the system.
References: = 1: PECB Candidate Handbook - ISO/IEC 27001 Lead Auditor, page 222: ISO 19011:2018 Guidelines for auditing management systems, clause 13: ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.94: ISO 19011:2018 Guidelines for auditing management systems, clause
7.5.25: ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, clause 9.8. : ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.1. : ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 6.2.1. : ISO 19011:
2018 Guidelines for auditing management systems, clause 6.4.2. : ISO 19011:2018 Guidelines for auditing management systems, clause 6.4.10. : ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing, clause 6.3.3.

NEW QUESTION: 63
您正在一家提供醫療保健服務的住宅療養院進行 ISMS 初始認證審核。審計計劃的下一步是召開末次會議。在最終審核小組會議上，身為審核組組長，您同意報告 2 項輕微不符合項和 1 項改進機會，如下：

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*

選擇您將在最後一次會議上向受審核方提供建議的審核專案經理的建議選項。

A. 立即推薦認證

B. 建議在 6 個月□進行全面的重新審核

C. 建議在未來某個日期進行突擊審核

D. 在您批准擬議的糾正措施計劃後建議進行認證 建議可以在 1 年□透過監督審核結束調□結果

E. 建議在 3 個月□進行部分審核

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: 64
根據發現的不合格項。A 公司製定了行動計劃，其中包括發現的不合格項 根本原因以及關於將採取的每項行動的一般口明。這是可以接受的嗎？
A. 不，行動計劃應包括有關將安裝的系統以及這些系統將如何消除根本原因的信息
B. 否，受審核方必須提交行動計劃，其中包括有關如何實施每項糾正措施的詳細信息
C. 是的，受審核方必須提交行動計劃，其中包括有關將採取的行動的一般聲明
Answer: (SHOW ANSWER)
The auditee is required to submit action plans that include detailed information on how every corrective action will be implemented. General statements are not sufficient; the action plans must specify the corrective actions in detail to ensure that the root causes of the nonconformities are addressed effectively.
References: ISO/IEC 27001:2013, Clause 10.1 (General) and ISO 19011:2018, Guidelines for auditing management systems.

NEW QUESTION: 65
審計人員無法辨識 A 公司隱藏了不安全的網路架構。這是什麼類型的審計風險？
A. 固有的
B. 控制
C. 檢測
Answer: C (LEAVE A REPLY)
Detection risk refers to the risk that the auditor will not detect a material misstatement or significant issue within the organization's ISMS. In this case, the auditor's inability to identify Company A's insecure network architecture is a detection risk.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 66

您是一位經驗豐富的 ISMS 審核員，在一家提供ICT 回收服務的組織中進行第三方監督審核。公司不再需要的ICT設備由組織處理。它要么被重新調試並重複使用，要么被安全地銷毀。
您注意到房間角落的長凳上有兩台伺服器。兩者的項目上都貼有伺服器名稱、IP 位址和管理員密碼的貼圖。您向 ICT 經理詢問這些物品，他告訴您這些物品是昨天從一位老客口那裡收到的一批貨物的一部分。
您應該採取哪一項行動？
A. 請 ICT 經理記錄資訊安全事件並口動資訊安全事件管理流程
B. 注意審核結果並檢口處理與客口 IT 安全相關的進貨的流程
C. 記錄您在審核結果中看到的口容，但不採取進一步行動
D. 針對控制提出不符合項 5.31 法律、法規、監管和合約要求'
E. 針對控制措施 8.20 網路安全」提出不符合項（應保護 管理和控製網路和網路設備，以保護系統和應用程式中的資訊）
F. 要求被審核方移除標籤，然後繼續審核
Answer: B (LEAVE A REPLY)
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: 67

您正在一家受 ABC 監管、提供醫療保健服務的住宅療養院進行 ISMS 審核。
審核計畫的下一步是驗證持續改善流程的有效性。在審計過程中，您了解到大多數居民家庭成員（90%）每週都會透過ABC的醫療保健行動應用程式透過電子郵件和簡訊收到一次WeCare醫療器材促銷廣告。他們均不同意將所收集的個人資料用於與ABC 簽署的服務協議上（或行銷或除護理和醫療之外的任何其他目的）。的資訊」個人資訊給不相關的第三方，他們已提出投訴。
服務經理表示，所有這些投訴均已被視為不合格，並且已根據不合格和糾正管理程序規劃和實施糾正措施。糾正措施包括立即停止與醫療設備製造商 WeCare 的合作，要求他們刪除收到的所有個人數據，並向所有居民及其家人發送道歉電子郵件。
您正在準備審計結果。選擇一項正確的發現選項。
A. 不符合：ABC未遵守與居民家庭成員簽署的醫療服務協議
B. 無不符合：我想收集更多有關組織如何定義管理系統範圍的證據，並了解它們是否涵蓋WeCare醫療器材製造
C. 無不合格情況：服務經理實施了糾正措施，客口服務代表評估所實施的糾正措施的有效性
D. 不合格：管理評審未考慮居民家庭成員的回饋
Answer: A (LEAVE A REPLY)
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, ABC is a residential nursing home that provides healthcare services to its residents and collects their personal data and their family members' personal data. ABC has a signed service agreement with the residents' family members that states that the collected personal data will not be used for marketing or any other purposes than nursing and medical care. However, ABC has violated this contractual requirement by sharing the personal data with WeCare, a medical device manufacturer, who has used the data to send promotional advertisements to the residents' family members via email and SMS. This has caused dissatisfaction and complaints from the residents' family members, who have a strong reason to believe that ABC is leaking their personal information to a non-relevant third party.
Therefore, the audit finding is a nonconformity with clause 8.1.4 of ISO 27001:2022, as ABC has failed to control the externally provided processes, products or services that are relevant to the information security management system, and has breached the contractual requirements related to information security with its customers. The fact that ABC has taken corrective actions to stop working with WeCare and to apologise to the customers does not eliminate the nonconformity, but only mitigates its consequences. The nonconformity still needs to be recorded, evaluated, and reviewed for effectiveness and improvement.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 68

資料完整性意味著
A. 資料的準確性和完整性
B. 資料應始終可見
C. 資料只能由適當的人存取
Answer: (SHOW ANSWER)
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: 69
情境 5 :Data Grid Inc. 是一家知名公司，為整個資訊科技基礎設施提供安全服務。它提供網路安全軟體，包括端點安全、防火牆和防毒軟體。二十年來，Data Grid Inc. 透過先進的□品和服務幫助多家公司保護其網路安全。Data Grid Inc. 在資訊和網路安全領域享有盛譽，決定獲得ISO/IEC 27001 認證，以更好地保護其□部和客□資□並獲得競爭優勢。
Data Grid Inc. 任命了審計團隊，該團隊同意審計任務的條款。此外，Data Grid Inc.明確了審核範圍，明確了審核標準，並建議在五天□結束審核。由於Data Grid Inc.員工人數眾多，流程複雜，審計小組拒□了Data Grid Inc.在五天□進行審計的提議。Data Grid Inc.堅稱他們計劃在五天□完成審核，因此雙方同意在規定的時間□進行審核。審計小組遵循基於風險的審計方法。
為了獲得主要業務流程和控制的概述，審計團隊存取了流程描述和組織圖表。他們無法對 IT 風險和控制進行更深入的分析，因為他們對IT 基礎架構和應用程式的存取受到限制。然而，審計小組表示，Data Grid Inc. 的 ISMS 出現重大缺陷的風險很低，因為該公司的大部分流程都是自動化的。因此，他們透過詢問Data Grid Inc. 的代表以下問題來評估 ISMS 整體上符合標準要求：
*如何定義和指派 IT 和 IT 控制的職責？
*Data Grid Inc. 如何評估控制措施是否達到了預期效果？
*Data Grid Inc. 採取了哪些控制措施來保護操作環境和資料免受惡意軟體的侵害？
*是否實施了與防火牆相關的控制？
Data Grid Inc. 的代表提供了充分且適當的證據來解決所有這些問題。
審計組長起草審計結論並向Data Grid Inc. 的最高管理階層報告。
儘管審核員推薦Data Grid Inc.進行認證，但Data Grid Inc.與認證機構之間在審核目標方面□生了誤解。Data Grid Inc. 表示，儘管審計目標包括確定潛在改進的領域，但審計團隊並未提供此類資訊。
根據該場景，回答以下問題：
基於情境5，審核小組對SMS進行整體評估，而不是評估每個流程的有效性和符合性。這是可以接受的嗎？
A. 是的，由於審核完成的時間有限，審核團隊必須透過整體評估SMS 來獲得□對保證
B. 不，審核團隊應透過評估每個流程來確保ISMS 符合標準要求
C. 是，如果審核團隊已獲得合理的保證來幫助他們評估ISMS 合規性

Answer: C (LEAVE A REPLY)

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

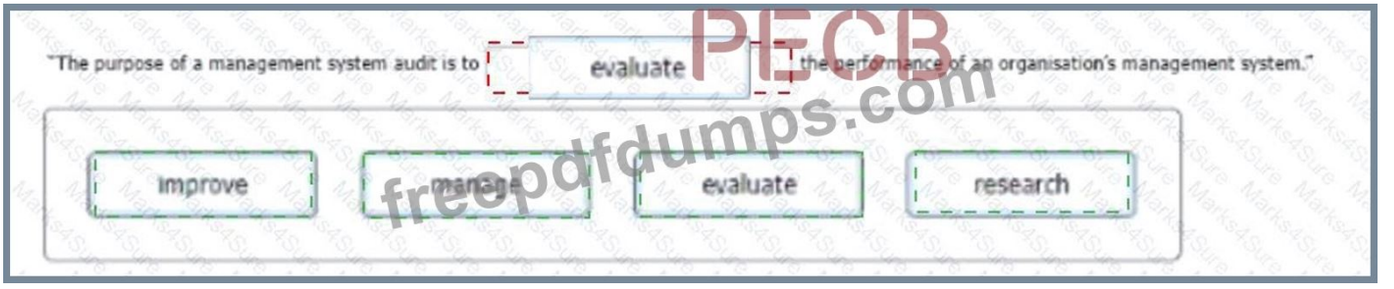
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 70

從以下選項中選擇一個最能完成句子的單字：

要用單字完成句子，請點擊要完成的空白部分，使其以紅色突出顯示，然後從下面的選項中點擊應用程式文字。或者，您可以將該選項拖曳到適當的空白部分。

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: 71
您是 ISMS 審核員，正在對電信供應商進行第三方監督審核 您位於設備暫存室，網路交換器在傳送給客口之前已預先編程。您注意到，最近未通過初始設定測試並被退回重新編程的交換器數量顯著增加。
你問首席測試員為什麼，她口，這是最近 ISMS 升級的結果」。在升級之前，每個技術人員都有自己的硬拷貝工作口明。現在，我團隊的八名成員必須共用兩台筆記型電腦才能在線上存取客口的設定口明。這些延誤給技術人員帶來了壓力，導致更多錯誤
僅根據上述信息，針對ISO 的哪一項條款提出不合格項'選擇一項。
A. 第 7.5 條 - 記錄資訊
B. 第 8.1 條 - 營運規劃與控制
C. 第 10.2 條 - 不合格與糾正措施
D. 第 7.3 條 - 意識
E. 第 7.2 條 - 能力
F. 第 7.4 條 - 溝通
Answer: B (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 8.1 requires an organization to plan, implement and control its processes needed to meet ISMS requirements2. This includes determining what needs to be done, how it will be done, who will do it, when it will be done, what resources are required, how performance will be evaluated, etc2. Therefore, if an ISMS auditor conducting a third-party surveillance audit of a telecom's provider notes that there has been a significant increase in the number of switches failing their initial configuration test and being returned for reprogramming due to a recent ISMS upgrade that reduced access to work instructions, this indicates a nonconformity against clause 8.1 of ISO/IEC 27001:2022. The organization has failed to plan and control its operational processes effectively to ensure information security and quality2. The other options are not correct clauses to raise a nonconformity against based solely on this information. For example, clause 7.5 deals with documented information required by ISMS or determined by an organization as necessary for its effectiveness2, but it does not specify how many copies or formats of work instructions should be available; clause 10.2 deals with nonconformity and corrective action as a

response to an identified problem or incident2, but it does not address how to prevent or avoid such problems or incidents in operational processes; clause 7.3 deals with awareness of ISMS policy, objectives, roles and responsibilities among persons doing work under an organization's control2, but it does not relate to how work instructions are accessed or followed; clause 7.2 deals with competence of persons doing work under an organization's control that affects its ISMS performance2, but it does not imply that lack of competence is caused by insufficient work instructions; clause 7.4 deals with communication about ISMS among internal and external interested parties2, but it does not cover how operational information is communicated within an organization. References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 72

您是經驗豐富的 ISMS 審核團隊領導，指導審核員進行培訓。您決定透過詢問她一系列問題來測試她對後續審核的了解。這是您的問題和她的答案。

她正確回答了您的哪四個問題？

A. 問：後續審核是否應該尋求發現新的不合格項？答：是的

B. 問：後續審核是否應確保不合格問題得到有效解決？答：是的

C. 問：後續審核是否應該考慮商定的改進機會以及糾正措施？

年

D. 問：後續審核的目的是驗證糾正、糾正措施和改進機會的完成嗎？答：是的

E. 問：所有審核都需要後續審核嗎？答：沒有

F. 問：後續審核的結果是否應該向負責最初識別NC 審核的審核組組長報告？答：是的

G. 問：後續審核的結果是否該向審核客口報告？答：沒有

H. 問：如果需要，後續審核的結果是否可以成為另一次後續審核？答：是的

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

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

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

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

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

H: Q: Could an outcome from a follow-up audit be another follow-up audit if required? A: YES
Yes, this is a possible outcome. If the follow-up audit finds that the corrective actions have not been fully effective, or if new issues are identified, it may be necessary to conduct another follow-up audit.
The other responses provided by the auditor in training require some clarification or correction. For instance, while a follow-up audit primarily focuses on previously identified nonconformities and corrective actions, it can still identify new nonconformities if observed (A). Opportunities for improvement are generally considered in the scope of regular audits more so than in follow-up audits, which are more narrowly focused on corrective actions (C). Also, the outcomes of follow-up audits should typically be reported to both the audit team leader and the audit client (F and G), ensuring transparency and accountability.
The four questions that the auditor in training has answered correctly are B, D, E, and H. These questions and answers are consistent with the definition and purpose of a follow-up audit as specified in ISO 19011:2018, Clause 6.712. A follow-up audit is conducted to verify the completion and effectiveness of corrective actions taken as a result of a previous audit (B, D). Follow-up audits are not mandatory for all audits, but they may be required by the audit program, the audit client, or other interested parties (E). The outcome of a follow-up audit may be another follow-up audit if the corrective actions are not satisfactory or not completed within the agreed time frame (H). The other questions and answers are either incorrect or irrelevant. A follow-up audit should not seek to identify new nonconformities, as this is not its objective (A). Follow-up audits should consider agreed opportunities for improvement as well as corrective actions, as they are both outputs of a previous audit . The outcome of a follow-up audit should be reported to the audit client, as well as to other relevant parties, such as the audit team leader who carried out the previous audit (F, G). References: 1: ISO
19011:2018, Guidelines for auditing management systems, Clause 6.7 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 6: Closing an ISO/IEC 27001 audit

NEW QUESTION: 73
您是經驗豐富的 ISMS 審核團隊負責人，目前正在使用ISO/IEC 27001:2022 作為標準對新客口進行第三方初始認證審核。
這是為期兩天的審核的第二天下午，您正要開始撰寫審核報告。
到目前為止，尚未發現任何不合格情況，您和您的團隊對該網站和組織的ISMS 印象深刻。
此時，您團隊的一名成員找到您並告訴您，她無法完成對領導力和承諾的評估，因為她花了太長時間審口變革計劃。
針對此訊息，您將採取下列哪一項行動？
A. 向客口道歉，並告訴他們您稍後會回來檢口領導力和承諾。
B. 建議客口，如果他們準備將您的回程航班升級為頭等艙，您將在明天的空閒時間審核領導力和承諾。
C. 告知受審核方和審核客口目前無法提出積極建議。

D. 告知受審核方需要終止並重新安排認證審核。
E. 聯絡管理審核計劃的個人並尋求他們的許可，以在審核報告中記錄積極的建議
F. 聯絡您的總部並等待他們進一步指示如何進行。
G. 鑑於沒有發現任何不合格項，並且組織的整體印象良好，請在審核報告中記錄積極的認證建議
H. 審口審核計劃和客口可用性，以確定團隊中的其他成員是否有機會在末次會議之前接手此任務
Answer: (SHOW ANSWER)
Leadership and commitment is a key requirement of ISO/IEC 27001:2022, as it establishes the top management's role and responsibility in establishing, implementing, maintaining, and continually improving the ISMS. Without assessing this aspect, the audit team cannot conclude that the ISMS is effective and conforms to the standard. Therefore, the audit team leader should advise the auditee and audit client that it is not possible to make a positive recommendation at this point, and explain the reason and the implications. The audit team leader should also consult with the certification body and the audit programme manager on the next steps, such as extending the audit duration, conducting a follow-up audit, or issuing a conditional certification, depending on the certification body's policy and the audit client's agreement. References: =
* ISO/IEC 27001:2022, clause 5, Leadership
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 22, Audit Report
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 23, Audit Conclusion and Recommendation

NEW QUESTION: 74
哪個是將三元組黏合在一起的黏合劑
A. 行程
B. 人
C. 協作
D. 技術
Answer: (SHOW ANSWER)
The triad refers to the three elements of information security: confidentiality, integrity and availability3. Technology is the glue that ties the triad together, as it provides the means to implement various controls and measures to protect information from unauthorized access, modification or loss3. References: ISO
/IEC 27001:2022 Lead Auditor Training Course - BSI

NEW QUESTION: 75
以下是資訊安全的目的，但以下情況除外：
A. 確保業務連續性
B. 最小化業務風險
C. 增加企業資口
D. 最大化投資回報

Answer: C (LEAVE A REPLY)
The following are purposes of information security, except increasing business assets. Increasing business assets is not a purpose of information security, as it is not directly related to protecting information and systems from threats and risks. Information security may contribute to increasing business assets by enhancing customer trust, reputation, compliance, and efficiency, but it is not its primary goal. Ensuring business continuity is a purpose of information security, as it aims to prevent or minimize disruptions or losses caused by incidents affecting information and systems. Minimizing business risk is a purpose of information security, as it aims to identify and reduce threats and vulnerabilities that may compromise information and systems. Maximizing return on investment is a purpose of information security, as it aims to optimize the costs and benefits of implementing and maintaining information security controls and measures. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 23. : [ISO/IEC 27001 Brochures | PECB], page 4.

NEW QUESTION: 76
場景3 :NightCore是一家總部位於美國的跨國科技公司，專注於電子商務 雲端運算、數位串流媒體和人工智慧。在實施資訊安全管理系統 (ISMS) 8 個多月後，他們聘請了認證機構進行第三方審核，以獲得 ISO/IEC 27001 認證。
認證機構成立了一個由七名審核員組成的團隊。傑克是最有經驗的審核員，被任命為審核組組長。多年來，他獲得了許多知名認證，例如SO/IEC 27001 首席審核員、CISA、CISSP 和 CISM。
Jack 透過研究和評估 NightCore 實施的每項資訊安全要求和控制，對ISMS 審口的每個階段進行了全面分析。在第二階段審核期間。傑克發現了一些不合格項。在將購買的軟體許可證發票數量與軟體庫存進行比較後，傑克發現該公司的許多電腦一直在使用非法版本的軟體。他決定要求高階主管對這項違規行為做出解釋，看看他們是否意識到這一點。他的下一步是審計 NightCore 的 IT 部門。高層指派 NightCore 的系統管理員 Tom 擔任指導，陪伴Jack 和稽核團隊了解系統和數位資口基礎設施的口部運作。
在採訪財務部的一名成員時，審計人員發現該公司最近向其一名顧問進行了一些不尋常的大額交易。收集有關交易的所有必要詳細資訊後。傑克決定直接訪問高階主管。
在討論第一個不合格項時，高階主管告訴傑克，他們願意決定使用複製軟體而不是原始軟體，因為它更便宜。Jack向NightCore的高層解釋口，使用非法版本的軟體違反了ISO/IEC 27001和國家法律法規的要求。然而，他們似乎對此感到滿意。
在審計幾個月後，Jack 將他在審計期間收集的一些 NightCore 資訊出售給了 NightCore 的競爭對手，以獲取巨額資金。
根據該場景，回答以下問題：
根據場景3，Jack在審計後出售NightCore的資訊時，損害了哪一項審計原則？
A. 獨立
B. 誠信
C. 保密性
Answer: C (LEAVE A REPLY)

Jack compromised the audit principle of confidentiality by selling NightCore's information after the audit.
Confidentiality ensures that information is accessible only to those authorized to have access and is protected throughout its lifecycle.
References: ISO 19011:2018, Guidelines for auditing management systems, principles of auditing

NEW QUESTION: 77
身為 ISMS 審核小組組長，您正在代表一家線上零售商對一家國際物流公司進行第二方審核 在審核期間，您的一名團隊成員報告了與ISO/IEC 27001:2022 附錄 A 的控制措施 5.18（存取權限）相關的不合格項。她發現證據表明，刪除過去3 個月口離開的 20 名人員的伺服器存取協議需要長達 1 週的時間，而政策要求在他們離開後24 小時口刪除存取權限。
用最好的單字填寫句子，勾選要填寫的空白部分，使其以紅色突出顯示，然後從下面的選項中點擊適用的文字。或者，您可以將該選項拖曳到適當的空白部分。

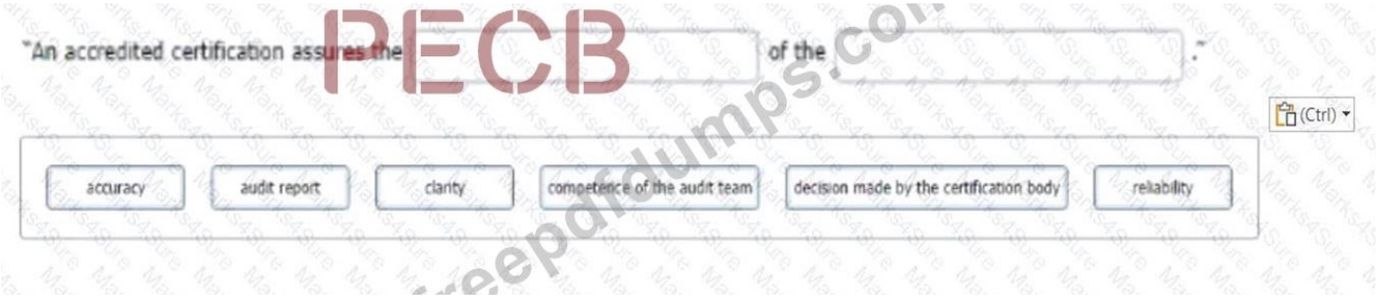
Answer:

Explanation:
The purpose of including access rights in an information management system to ISO/IEC 27001:2022 is to provide, review, modify and remove these permissions in accordance with the organisation' s policy and rules for access control.
Access rights are the permissions granted to users or groups of users to access, use, modify, or delete information assets. Access rights should be aligned with the organisation's access control

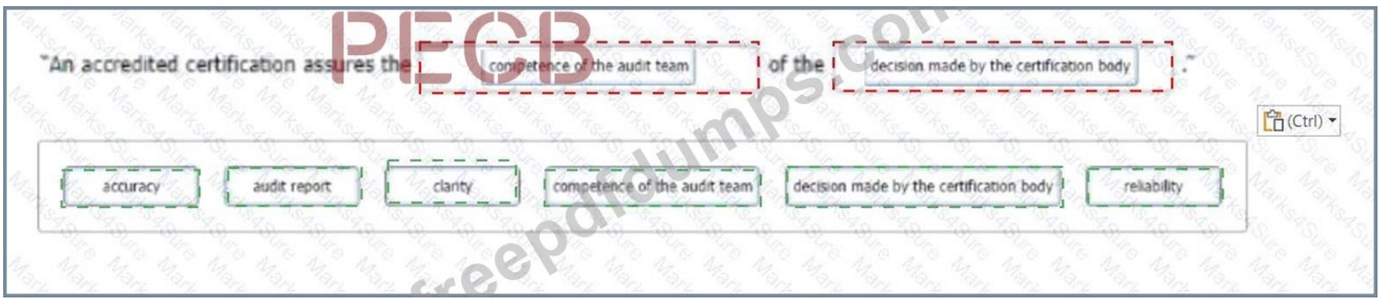
policy, which defines the objectives, principles, roles, and responsibilities for managing access to information systems.
Access rights should also follow the organisation's rules for access control, which specify the criteria, procedures, and controls for granting, reviewing, modifying, and revoking access rights.
The purpose of including access rights in an information management system is to ensure that only authorised users can access information assets according to their business needs and roles, and to prevent unauthorised or inappropriate access that could compromise the confidentiality, integrity, or availability of information assets. References:
* ISO/IEC 27001:2022 Annex A Control 5.181
* ISO/IEC 27002:2022 Control 5.182
* CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Training Course3

NEW QUESTION: 78
ISMS (1)----------幫助確定 (2)----------,
A. (1) 持續改進，(2) 矯正措施的有效性
B. 問題 (1) 管理評審，(2) 持續改善的機會
C. (1) 口部審計，(2) ISMS 範圍
Answer: (SHOW ANSWER)
Management review is a crucial component of an ISMS that helps determine opportunities for continual improvement. Through management review, an organization assesses the performance and effectiveness of its ISMS, including reviewing opportunities for improvements and the need for changes to the ISMS, including the security policy and security objectives.
References: ISO/IEC 27001:2013 Standard, Clause 9.3 (Management Review)

NEW QUESTION: 79
選出最能完成句子的單字：
要用單字完成句子，請點擊要完成的空白部分，使其以紅色突出顯示，然後從下面的選項中點擊應用程式文字。或者，您可以將該選項拖曳到適當的空白部分。

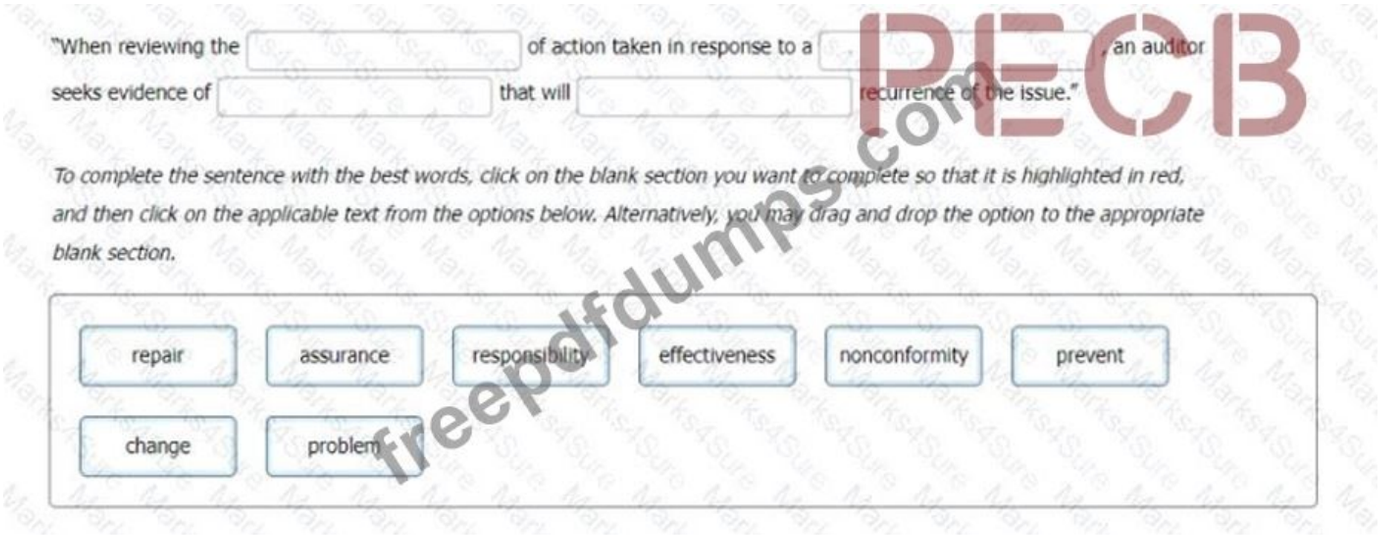


Answer:

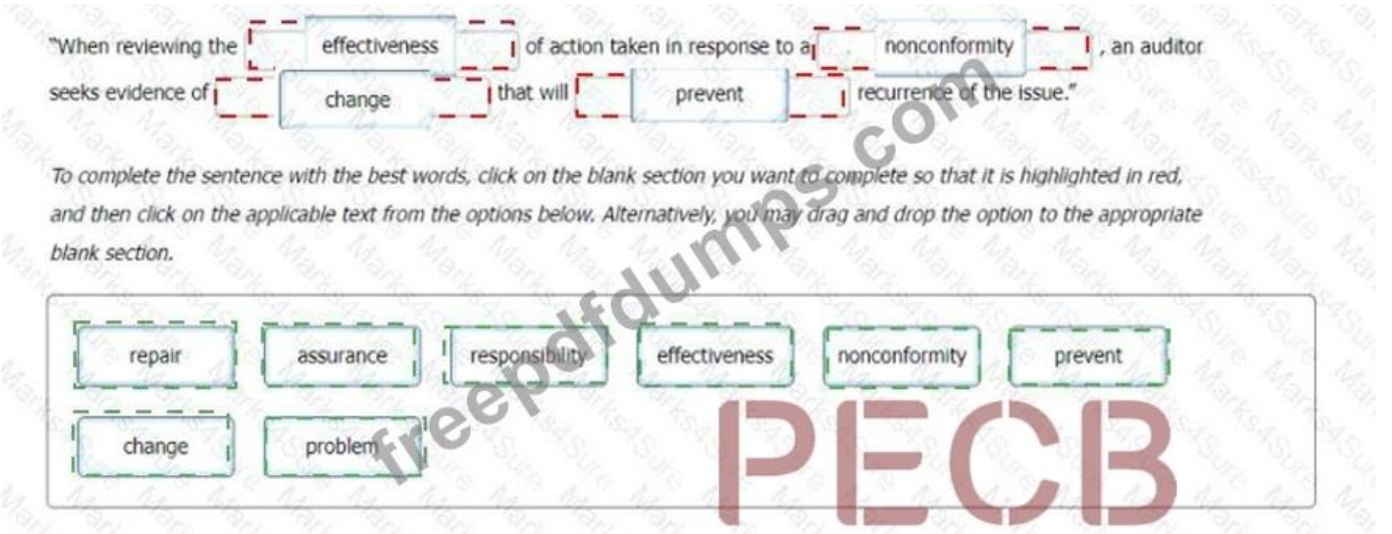


Explanation:
competence of the audit team and decision made by the certification body According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, an accredited certification means that the certification body has been evaluated by 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: 80
您正在一家名為 ABC 的歐洲住宿療養院執行 ISMS 審核，該療養院提供醫療保健服務。審核計畫的下一步是驗證持續改善流程的有效性。
審計中了解到，大部分居民家庭成員 90%）每週都會透過農行的醫療保健行動應用程式透過電子郵件和簡訊收到WeCare醫療器材促銷廣告一次。他們均不同意將收集的個人資料用於行銷或與ABC簽訂的服務協議中護理和醫療以外的任何其他目的。他們有充分的理由相信ABC正在向不相關的第三方洩露居民和家庭成員的個人信息，並提出了投訴。
服務經理表示，經調口，所有這些投訴均被視為不合格問題。
已根據不合格和糾正管理程序（文件參考ID :ISMS_L2_10.1，版本1）規劃和實施糾正措施。
您寫下不合格項，稍後再跟進。選出最能完成句子的單字：



Answer:



Explanation:
One possible way to complete the sentence is:
"When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue." According to ISO/IEC 27001:2022, clause 10.1, the organization shall continually improve the suitability, adequacy, and effectiveness of the ISMS by evaluating the performance and the effectiveness of the ISMS, ensuring that the policy and objectives are aligned with the strategic direction of the organization, and taking actions to achieve the intended outcomes of the ISMS. One of the ways to achieve continual improvement is to identify and correct nonconformities and take actions to eliminate their causes and prevent their recurrence.
Therefore, when reviewing the effectiveness of the corrective actions, an auditor should look for evidence that the organization has analyzed the root cause of the nonconformity, implemented appropriate changes to the ISMS, and verified that the changes have resulted in the desired improvement and prevented the recurrence of the issue. References: =
* ISO/IEC 27001:2022, clause 10.1, Nonconformity and corrective action
* ISO/IEC 27001:2022, clause 10.2, Continual improvement
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19, Audit Process
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 21, Audit Findings

NEW QUESTION: 81
您是一位經驗豐富的 ISMS 審核團隊領導者。您目前正在對國際運輸組織進行第三方監督審核。您抽取了四份口部稽核報告，其中指出：
報告 1 - 審計員：詹姆斯先生
一年來，該組織在100 次中有 23 次未能滿足其承諾的交付日期。
分級 - 次要
矯正措施到期時間 :9 個月口。
報告 2 - 審計員：詹姆斯先生
1 月至 3 月期間，我們收到了125 起有關服務台團隊的投訴。客口指責他們粗魯且反應遲鈍。

分級 - 次要
矯正措施到期時間 :12 個月□。
報告 3 - 審計員：詹姆斯先生
上個月收到的 40 個客□訂單中，有38 個已正確處理。其餘 2 份中，一份缺簽名，一份缺日期
評分 -
更正期間 :3週□
報告 4 - 審計員：羅傑斯先生
在檢□的 30 份人事記錄中，發現26 份已完全填寫，而其餘4 份均缺少個人的開始日期。
分級 - 主要
更正期間 :1週□
哪四個選項顯示了您對這些報告的擔憂？
A. 我擔心一名審計師似乎正在執行大部分□部審計
B. 我擔心沒有進行不合格審□
C. 我擔心報告 3 沒有記錄任何評分。
D. 我會擔心，因為解決重大不合格問題的行動應始終早於解決輕微不合格問題的行動完成
E. 我擔心四份報告中解決不合格問題的時間明顯不同
F. 我擔心審核員是否理解糾正和糾正措施之間的區別
G. 我擔心審核員只專注於資訊安全流程
H. 我擔心該組織中是否有不合格品分級標準
Answer: (SHOW ANSWER)

NEW QUESTION: 82
選擇最能描述如何進行資訊安全管理系統審核的選項：
A. 應使用審核標準來評估間接證據，以□生審核結果。
然後，應建立審核報告並在審核組會議上提交給審核組。
B. 應使用審核標準來評估客觀證據，以□生審核結果。然後，應建立審核報告並在末次會議上提交給審核組組長。
C. 應使用審核方法來評估審核證據，以□生審核建議。
然後，應建立審核建議並在末次會議上提交給受審核方。
D. 應使用審核方法來評估客觀證據，以得出審核結果。然後，應制定審核結論並在末次會議上提交給受審核方。
E. 審計目標應用於評估審計證據，以得出審計結論。然後，應建立審核結果並在末次會議上提交給審核客□。
F. 審計目標應用於評估客觀證據，以得出審計結論。
然後，應建立審計建議並在管理審□時提交給最高管理層。
Answer: (SHOW ANSWER)
The option that best describes how Information Security Management System (ISMS) audits should be conducted, aligning with best practices and standards like ISO/IEC 27001:2022, is:
D: Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.

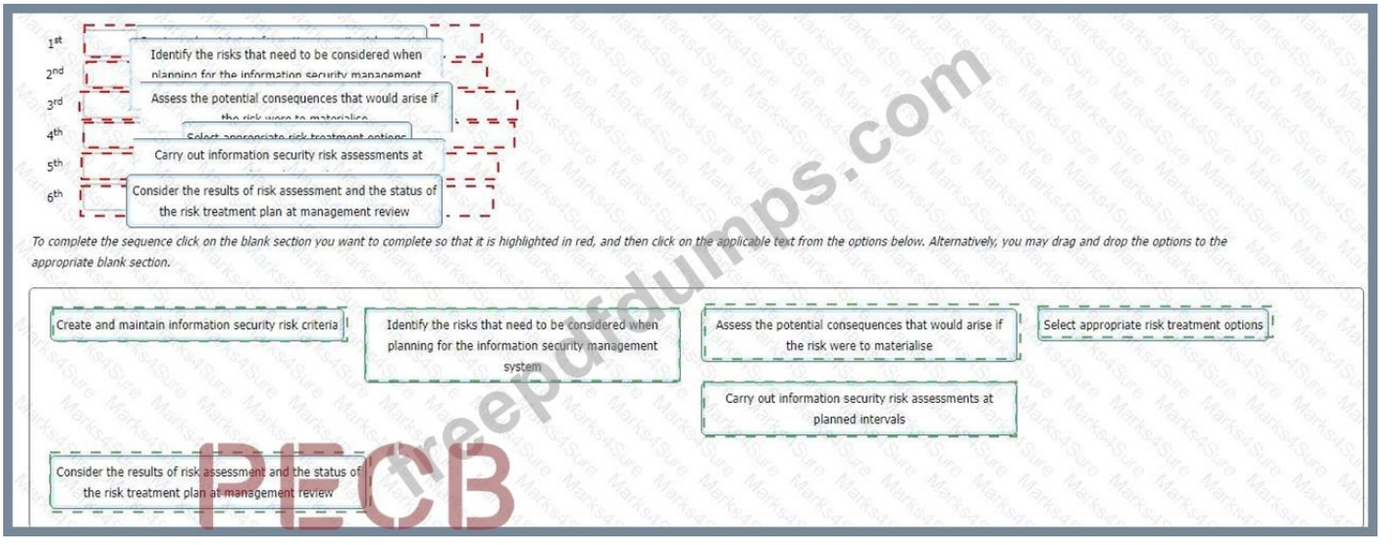
This option accurately reflects the audit process, emphasizing the use of systematic audit methods to assess objective evidence, which is crucial for impartiality and accuracy in auditing. Audit findings are the results derived from evaluating the objective evidence against the audit criteria. The conclusion, based on the audit findings, provides a comprehensive summary of the audit's outcomes, indicating whether the audited ISMS meets the established criteria. Presenting these conclusions to the auditee during the closing meeting ensures transparency and provides an opportunity for immediate clarification and discussion of the results and potential next steps.

NEW QUESTION: 83

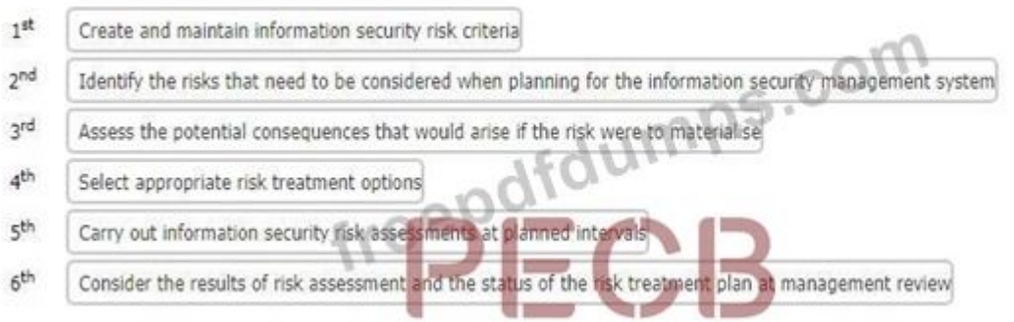
您是一位經驗豐富的 ISMS 審核團隊領導，為培訓中的審核員提供指導。今天課程的主題是根據 ISO/IEC 27001:2022的要求進行資訊安全風險管理。

您為班級提供一系列活動。然後，您要求全班將這些活動按照它們在標準中出現的順序進行排序。他們應該向您報告的正確順序是什麼？

Answer:



Explanation:



The correct sequence of activities for the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022 is as follows:
1st: Create and maintain information security risk criteria 2nd: Identify the risks that need to be considered when planning for the information security management system 3rd: Assess the potential consequences that would arise if the risk were to materialise 4th: Select appropriate risk treatment options 5th: Carry out information security risk assessments at planned intervals 6th: Consider the results of risk assessment and the status of the risk treatment plan at management review This sequence is based on the information security risk management process described in ISO/IEC 27001:
2022 clause 6.1, which includes the following activities:
* establishing and maintaining information security risk criteria;
* ensuring that repeated information security risk assessments produce consistent, valid and comparable results;
* identifying the information security risks;
* analyzing the information security risks;
* evaluating the information security risks;
* treating the information security risks;
* accepting the information security risks and the residual information security risks;
* communicating and consulting with stakeholders throughout the process;
* monitoring and reviewing the information security risks and the risk treatment plan.
References:
* ISO/IEC 27001:2022, clause 6.1
* [PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 14-15
* ISO 27001 Risk Management in Plain English

NEW QUESTION: 84
您是經驗豐富的 ISMS 審核團隊領導，指導審核員進行培訓。她詢問您審核報告中不合格項的分級。您決定透過詢問她以下哪四個陳述是正確的來測試她的知識。
A. 重大不符合項目可能需要現場跟進
B. 不合格項必須僅使用術語 嚴重」或 輕微」進行分級
C. 解決重大不合格問題所採取的行動通常比解決輕微不合格問題所採取的行動更為實質性
D. 非常輕微的不符合項應重新評級為改進機會
E. 幾個輕微不符合項可以歸為一個主要不符合項

F. 不合格品的分級必須在首次會議上向受審核方解釋
G. 受審核方始終負責確定不合格品的分級標準
H. 可以將不合格項分級以表示其重要性
Answer: A,C,E,H (LEAVE A REPLY)
The four statements that are true are:
*Major nonconformities may be subject to on-site follow up
*The action taken to address major nonconformities is typically more substantial than the action taken to address minor nonconformities
*Several minor nonconformities can be grouped into a major nonconformity
*Nonconformities may be graded to indicate their significance
According to ISO 19011:2018, a nonconformity is the non-fulfilment of a requirement1. Nonconformities may be graded to indicate their significance, based on the criteria established by the audit programme or the audit client2. The grading of nonconformities may use different terms or levels, such as major, minor, critical, etc., depending on the nature and context of the audit3. However, some common definitions of major and minor nonconformities are:
*A major nonconformity is a nonconformity that affects the ability of the management system to achieve its intended results, or that represents a significant breakdown of the management system4. Major nonconformities may require immediate corrective action and on-site follow up by the auditor to verify their closure5.
*A minor nonconformity is a nonconformity that does not affect the ability of the management system to achieve its intended results, or that represents an isolated lapse of the management system4. Minor nonconformities may require corrective action within a specified time frame and off-site verification by the auditor to confirm their closure5.
The action taken to address nonconformities depends on the severity and impact of the nonconformity, and the risk of recurrence or escalation. Typically, the action taken to address major nonconformities is more substantial than the action taken to address minor nonconformities, as it may involve identifying and eliminating the root cause of the problem, implementing preventive measures, and monitoring the effectiveness of the solution.
Several minor nonconformities can be grouped into a major nonconformity if they are related to the same requirement, process, or area, and if they indicate a systemic failure or a significant risk to the management system. The auditor should use professional judgment and evidence-based approach to decide whether to group or report nonconformities individually.
The other statements are false, based on the guidance of ISO 19011:2018. For example:
*Option B is false, because nonconformities can be graded using different terms or levels, depending on the criteria established by the audit programme or the audit client2. The terms 'major' and 'minor' are not mandatory or universal, but rather examples of possible grading levels3.
*Option D is false, because very minor nonconformities should not be re-graded as opportunities for improvement, but rather reported as nonconformities, as they still represent a non-fulfilment of a requirement1. An opportunity for improvement is a suggestion for enhancing the performance or effectiveness of the management system, but it is not a nonconformity or a requirement.

*Option F is false, because the grading of nonconformities does not have to be explained to the auditee at the opening meeting, but rather at the closing meeting, where the audit findings and conclusions are presented and discussed. The opening meeting is intended to provide an overview of the audit objectives, scope, criteria, and methods, and to confirm the audit arrangements and logistics.
*Option G is false, because the auditee is not always responsible for determining the criteria for grading nonconformities, but rather the audit programme or the audit client, in consultation with the auditee and other relevant parties2. The auditee is responsible for taking corrective action to address the nonconformities, and for providing evidence of their completion and effectiveness.
References: 1: ISO 19011:2018, 3.13; 2: ISO 19011:2018, 6.6.2; 3: ISO 19011:2018, 6.6.3; 4: ISO Audit Findings :Non-conformance - AUVA Certification1; 5: Annex III: Nonconformity grading - FSSC2; : ISO
27001 Certification - Major vs. Minor Nonconformities - Advisera3; : GUIDANCE FOR ADDRESSING AND CLEARING NONCONFORMITIES - SADCAS4; : ISO 19011:2018, 6.2; : ISO 19011:2018, 3.14; :
ISO 19011:2018, 6.7; : ISO 19011:2018, 6.4; : ISO 19011:2018, 6.7.2; : ISO 19011:2018; : ISO 19011:2018; :
ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]; : [ISO 19011:2018]; : [ISO
19011:2018]; : [ISO 19011:2018]; : [ISO 19011:2018]; : [ISO 19011:2018]; : [ISO 19011:2018]

NEW QUESTION: 85
下列哪兩個選項不參與第一方審核？
A. 認證機構審核員
B. 來自認證機構的審核小組
C. 經過CQI及IRCA認證的審核員
D. 諮詢機構的審核員
E. 接受過 CQI 和 IRCA 計畫訓練的審核員
F. 在組織中接受過訓練的審核員
Answer: (SHOW ANSWER)
A first-party audit is an internal audit in which the organization's own staff or contractors check the conformity and effectiveness of the ISMS. A certification body auditor and an audit team from an accreditation body are external auditors who conduct audits for the purpose of certification or accreditation.
They do not participate in a first-party audit, but rather in a third-party audit. References: First & Second Party Audits - operational services, The ISO 27001 Audit Process | Blog | OneTrust, The ISO 27001 Audit Process | A Beginner's Guide - IAS USA

NEW QUESTION: 86
為什麼在初次接觸時要考慮重要性？
A. 確定審核持續時間

B. 合理保證審核能口成功完成
C. 定義最小化偵測風險的流程
Answer: B (LEAVE A REPLY)
Materiality should be considered during the initial contact to obtain reasonable assurance that the audit can be successfully completed. Determining materiality helps establish the threshold for the significance of audit findings, ensuring that the audit focuses on substantial issues that could impact the audit conclusions.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 87
認證審核的審核計畫不需要下列哪兩個資訊選項？
A. 抽樣計劃
B. 文件審口
C. 管理系統所代表的工作經驗
D. 審核清單
E. 組織的財務報表
F. 審核計劃
Answer: C,E (LEAVE A REPLY)
These two options are not required for audit planning of a certification audit, as they are not relevant to the audit objectives, scope, criteria, and methods. The working experience of the management system representative is not a requirement of ISO/IEC 27001, nor does it affect the conformity or effectiveness of the ISMS. The organisation's financial statement is not part of the ISMS documentation, nor does it provide evidence of the ISMS performance or improvement. The other options are required for audit planning, as they help to determine the audit activities, resources, schedule, and sampling strategy. References: PECB Candidate Handbook1, page 19-20; ISO 9001 Auditing Practices Group Guidance on2, page 1-2; ISO/IEC 27001:2022 (en)3, clause 9.2.

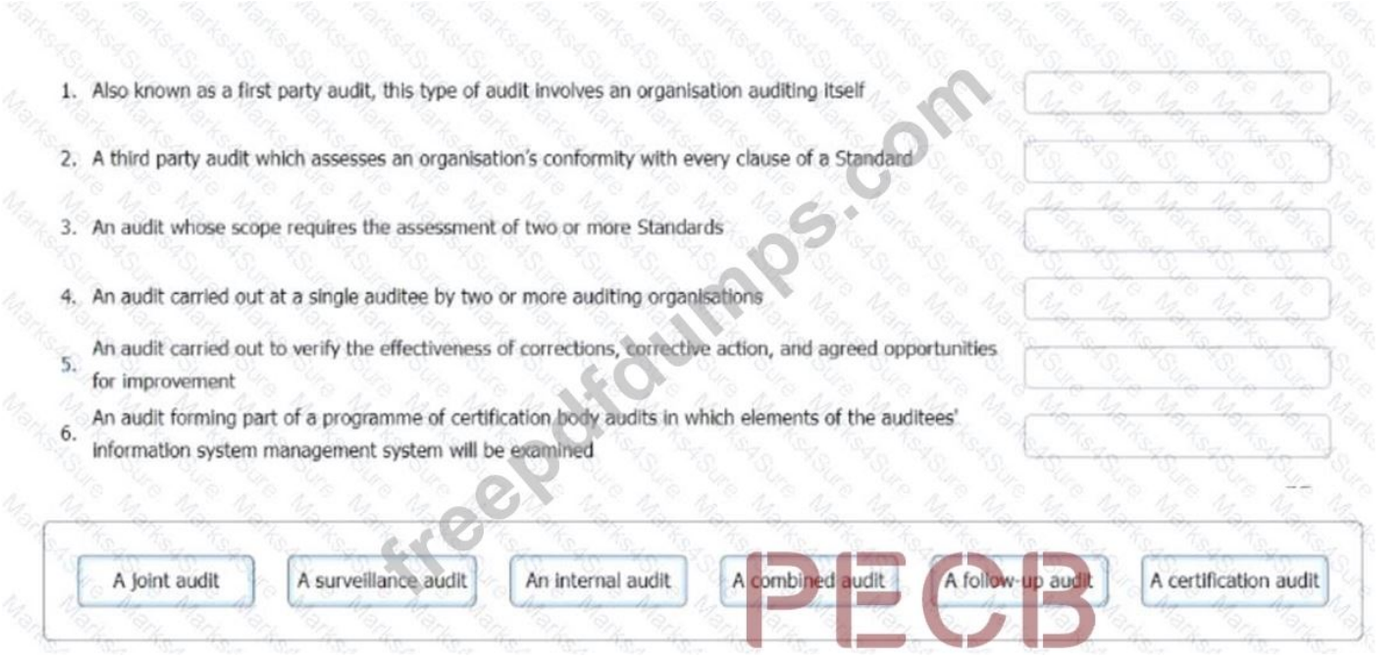
NEW QUESTION: 88
情境 8 :EsBank 自 9 月起為愛沙尼亞銀行業提供銀行和金融解決方案
2010年，該公司在全國擁有30家分行和100多台ATM機。
EsBank 在高度監管的行業中運營，必須遵守許多有關資料安全和隱私的法律和法規。他們需要透過實施技術和非技術控制來管理整個營運的資訊安全。EsBank 決定實施基於 ISO/IEC 的 ISMS 27001，因為它提供了更好的安全性、更多的風險控制以及符合法律法規的關鍵要求。
在成功實施 ISMS 九個月後，EsBank 決定由獨立認證機構根據 ISO/IEC 27001 對其 ISMS 進行認證。
第一階段和第二階段審核是共同進行的，發現了一些不符合項。第一個不合格之處與 EsBank 的資訊標籤有關。該公司有資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的文件將被貼上不同的標籤（有時為機密，有時為敏感）

考慮到所有文件也以電子方式存儲，不合格情況也影響了媒體處理。審計小組透過抽樣得出結論，200 個可移動媒體中有 50 個儲存了被錯誤分類為機密的敏感資訊。根據資訊分類方案，允許將機密資訊儲存在可移動媒體中，而嚴格禁止儲存敏感資訊。這標誌著另一個不合格之處。
他們起草了不合格報告，並與EsBank 代表討論了審計結論，代表同意在兩個月內針對發現的不合格問題提交行動計劃。
EsBank 接受了審計組組長提出的解決方案。他們根據實體和電子格式的分類方案起草了資訊標籤程序，解決了不合格問題。可移動媒體程式也基於此程式進行了更新。
審計完成兩週後，EsBank 提交了總體行動計畫。在那裡，他們解決了檢測到的不合格問題以及採取的糾正措施，但沒有包括有關受影響的系統、控製或操作的任何詳細資訊。審核小組評估了該行動計劃並得出結論，該計劃將解決不合格問題。然而，EsBank 收到了不利的認證建議。
根據上述場景，回答以下問題：
根據情境 8，審核小組評估了行動計畫並得出結論，該計畫將解決檢測到的不符合項這是可以接受的嗎？
A. 是的。審核小組必須評估行動計畫並驗證其是否適合糾正檢測到的不合格項
B. 是，前提是EsBank 之前已經驗證了行動計劃的有效性，並告知審核團隊該行動計劃允許糾正不合格項
C. 否，被審核方應驗證行動計畫是否允許糾正不合格項並消除根本原因
Answer: A (LEAVE A REPLY)
Yes, the audit team must evaluate the action plan and verify if it is appropriate for correcting the detected nonconformities. This is part of the auditor's responsibilities to ensure that the proposed actions adequately address the issues identified during the audit.

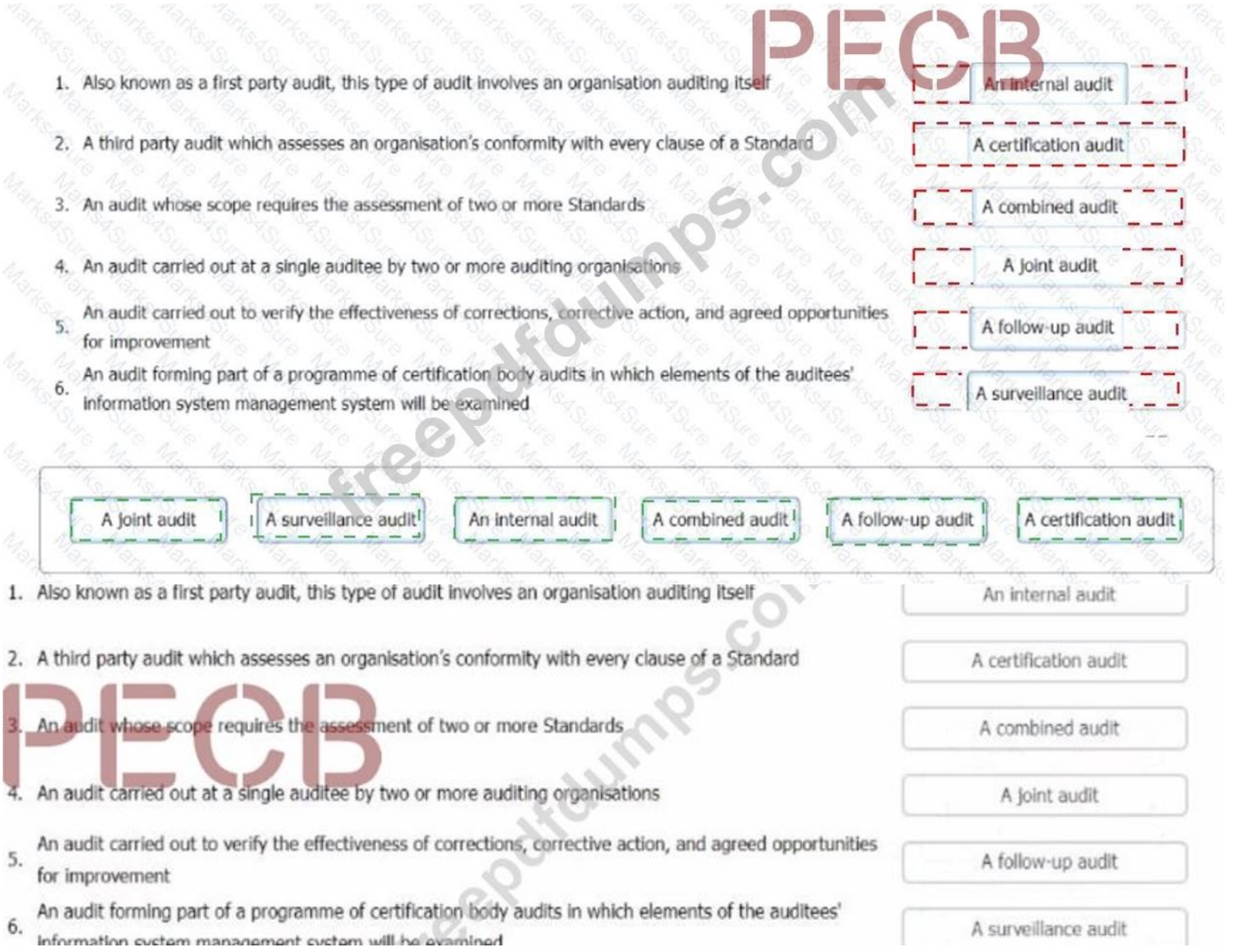
NEW QUESTION: 89
場景 2：Knight 是一家來自美國北加州的電子公司，開發電玩遊戲機。Knight 在全球擁有 300 多名員工。在成立五週年之際，他們決定推出G-Console，這是一款面向全球市場的新一代電玩遊戲機。G-Console被認為是2021年的終極媒體機，將為玩家帶來最佳的遊戲體驗。
主機包將包括一副 VR 耳機、兩個
遊戲和其他禮物。
多年來，公司透過誠信、誠實和尊重客戶而建立了良好的聲譽。這種良好的聲譽是大多數熱衷遊戲玩家在Knight的G-console一上市就想擁有它的原因之一。
Knight 除了是一家非常以客戶為導向的公司之外，
也因其開發品質獲得了遊戲行業的廣泛認可。他們的價格比合理標準允許的要高一些。
儘管如此，對於Knight 的大多數忠實客戶來說，這並不是一個問題，因為它們的品質是一流的。
作為世界頂級視訊遊戲機開發商之一，Knight 也經常成為惡意活動的焦點。該公司的 ISMS 已投入運作一年多了。ISMS 範圍包括 Knight 的所有部門（財務和人力資源部門除外）。
最近，奈特的一些包含專有資訊的文件被駭客洩露。Knight 的事件回應團隊 (IRT) 立即開始分析系統的每個部分以及事件的詳細資訊。
IRT 的第一個懷疑是 Knight 的員工使用了弱密碼，因此很容易被未經授權存取其帳戶的駭客破解。然而，在仔細調查該事件後,IRT 確定駭客透過擷取檔案傳輸協定 (FTP) 流量來存取帳戶。
FTP 是一種用於在帳戶之間傳輸檔案的網路協定。它使用明文密碼進行身份驗證。

受此資訊安全事件的影響，在RT的建議下，Knight決定用Secure Shell (SSH)協定取代FTP，這樣任何捕獲流量的人都只能看到加密的資料。
在這些變化之後，奈特進行了風險評估，以驗證控制措施的實施是否已將類似事件的風險降至最低。該過程的結果得到了 ISMS 專案經理的批准，他聲稱實施新控制措施後的風險等級符合公司的風險接受程度。
根據該場景，回答以下問題：
基於場景 2, Knight 決定用 Secure Shell (SSH) 協定取代 FTP。在這種情況下是否應該更新適用性聲明 (SoA)？
A. 不，使用SSH 協定不是 ISO/IEC 27001 要求；且；因此，不需要包含在SoA 中
B. 否，因為只有在新增控制項時才應更新SoA，而不是在取消舊控制項時更新SoA
C. 是的，新控制的實施應該合理並包含在SoA 中
Answer: C (LEAVE A REPLY)
The Statement of Applicability (SoA) is a core document within an ISMS that outlines the security controls an organization implements. When a new control, such as the SSH protocol, is implemented, it should be included in the SoA to reflect the current state of the ISMS. The SoA should be updated to justify the inclusion of the new control and to document how it is implemented within the organization12. References: = This guidance is based on the best practices for maintaining the SoA as per ISO/IEC 27001, which requires the SoA to be a living document that accurately reflects the security controls in use by the organization

NEW QUESTION: 90
您是一位經驗豐富的 ISMS 審核團隊領導者。受訓的審核員已與您聯繫，要求您澄清她可能需要進行的不同類型的審核。
將以下審核類型與描述相符。
要填寫表格，請按一下要填寫的空白部分，以便反白顯示n fed”，然後從下面的選項中按一下適用的文字。或者，您可以將每個選項拖曳到相應的空白部分。



Answer:



NEW QUESTION: 91

下列哪一項是組織環境的定義？

A. 對可能影響組織實現其目標的願望的□部和外部問題的控制

B. 可能影響組織制定和實現其目標的方法的□部和外部問題的複雜性

C. 可能影響組織制定和實現其目標的方法的□部和外部問題的組合

D. 協調可能對組織的成功□生正面或負面影響的□部和外部問題

Answer: C (LEAVE A REPLY)

The context of the organisation is the business environment in which the organisation operates and defines its information security management system (ISMS). It includes the internal and external factors and conditions that can influence the organisation's information security objectives, strategies, and policies. The context of the organisation helps the organisation to identify the scope, boundaries, and requirements of the ISMS, as well as the interested parties and their expectations. The context of the organisation is determined by considering both internal and external issues, such as the organisational structure, culture, values, mission, vision, objectives, strategies, resources, capabilities, processes, activities, products, services, markets, customers, competitors, suppliers, partners, regulators, laws, regulations, standards, guidelines,

best practices, risks, opportunities, threats, vulnerabilities, etc. References: ISO 27001:2022 Clause 4 Context of the organization, ISO 27001 Requirement 4.1 - Understanding the Context of the Organisation, ISO 27001 context of the organization - How to define it - Advisera

NEW QUESTION: 92
場景 2 :Knight 是一家來自美國北加州的電子公司，開發電玩遊戲機。Knight 在全球擁有 300 多名員工。在成立五週年之際，他們決定推出G-Console，這是一款面向全球市場的新一代電玩遊戲機。G-Console被認為是2021年的終極媒體機，將為玩家帶來最佳的遊戲體驗。
主機包將包括一副 VR 耳機、兩個
遊戲和其他禮物。
多年來，公司透過誠信、誠實和尊重客口而建立了良好的聲譽。這種良好的聲譽是大多數熱衷遊戲玩家在Knight的G-console一上市就想擁有它的原因之一。
Knight 除了是一家非常以客口為導向的公司之外，
也因其開發品質獲得了遊戲口業的廣泛認可。他們的價格比合理標準允許的要高一些。
儘管如此，對於Knight 的大多數忠實客口來口，這並不是一個問題，因為它們的品質是一流的。
作為世界頂級視訊遊戲機開發商之一，Knight 也經常成為惡意活動的焦點。該公司的 ISMS 已投入運作一年多了。ISMS 範圍包括 Knight 的所有部門（財務和人力資源部門除外）。
最近，奈特的一些包含專有資訊的文件被駭客洩露。Knight 的事件回應團隊 (IRT) 立即開始分析系統的每個部分以及事件的詳細資訊。
IRT 的第一個懷疑是 Knight 的員工使用了弱密碼，因此很容易被未經授權存取其帳口的駭客破解。然而，在仔細調口該事件後,IRT 確定駭客透過擷取檔案傳輸協定 (FTP) 流量來存取帳口。
FTP 是一種用於在帳口之間傳輸檔案的網路協定。它使用明文密碼進行身份驗證。
受此資訊安全事件的影響，在RT的建議下，Knight決定用Secure Shell (SSH)協定取代FTP，這樣任何捕獲流量的人都只能看到加密的資料。
在這些變化之後，奈特進行了風險評估，以驗證控制措施的實施是否已將類似事件的風險降至最低。該過程的結果得到了 ISMS 專案經理的批准，他聲稱實施新控制措施後的風險等級符合公司的風險接受程度。
根據該場景，回答以下問題：
FTP 使用明文密碼進行驗證。這是一個 FTP：
A. 漏洞

B. 風險
C. 威脅
Answer: A (LEAVE A REPLY)
The use of clear text passwords for authentication in FTP is a vulnerability because it is a weakness that can be exploited by threat actors. Clear text passwords can be intercepted easily by network sniffers or through man-in-the-middle attacks, making them a significant security risk1. References: = This explanation is consistent with the understanding of vulnerabilities within the field of information security, particularly as it relates to network protocols like FTP and their associated risks

NEW QUESTION: 93
下列哪兩項敘述是正確的？
A. 審核小組負責人負責管理審核計畫。
B. 審核計畫描述了為特定時間範圍並針對特定目的而規劃的一組一項或多項審核的安排。
C. 一旦達成一致，審核計畫就固定下來，在審核過程中不能更改
D. 審核計畫描述了為特定時間範圍規劃並針對特定目的的一組一個或多個審核的安排。
E. 審核計劃描述了審核的活動和安排。
F. 審核計劃描述了審核的活動和安排。
Answer: B,E (LEAVE A REPLY)
The two true statements are B and E. According to ISO 19011:2022, the audit plan describes the arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose1, while the audit programme describes the activities and arrangements for an audit2. The other options are either false or irrelevant. The responsibility for managing the audit programme rests with the audit programme manager, not the audit team leader (A)3. The audit plan can be changed during the conducting of the audit if necessary, with the agreement of the audit client and the auditee 4. The audit programme and the audit plan are not the same thing, so D and F are incorrect. References: 1: ISO 19011:2022, Guidelines for auditing management systems, Clause 3.8 \n2: ISO 19011:2022, Guidelines for auditing management systems, Clause
3.9 \n3: ISO 19011:2022, Guidelines for auditing management systems, Clause 5.3.1 \n4: ISO 19011:2022, Guidelines for auditing management systems, Clause 6.4.2

NEW QUESTION: 94
您是一位經驗豐富的 ISMS 審核團隊領導，為ISMS 審核員提供訓練指導。他們被要求對外部提供者進行評估，並準備了一份包含以下活動的清單。他們要求您□看他們的清單，以確認他們提議的行動是適當的。
他們受邀參加的審核是對資料中心的第三方監督審核。資料中心代理是更廣泛的電信集團的一部分。集團□的每個資料中心都運行自己的 ISMS 並持有自己的憑證。
選擇與 ISO/IEC 27001:2022 有關外部提供者的要求相關的三個選項。
A. 我會檢□其他資料中心是否被視為外部供應商，即使它們屬於同一電信集團

B. 我將確保外部提供者制定書面流程，以通知組織因使用其口品或服務而口生的任何風險
C. 我將確保該組織為其確定的對於保護其資訊的機密性、完整性和可訪問性至關重要的每個流程都有一個備用外部提供商
D. 我將把審核活動限制在外部提供的流程中，因為不需要審核外部提供的口品或服務
E. 我將確保組織定期監控、審口和評估外部提供者的績效
F. 我將確保組織已確定需要與外部提供者就 ISMS 進行溝通
G. 我將確保最高管理階層為提供外部 ISMS 流程和口部 ISMS 流程的人員分配角色和職責
H. 我將確保組織對其外部提供者進行排名，並將大部分工作分配給那些評級最高的供應商
Answer: A,B,E (LEAVE A REPLY)
* A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12
* B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO
27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12
* E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12
* F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the

communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO 27001:
2022:
* C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12
* D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12
* G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12
* H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 95
分類為 _____ 的資訊或資料不需要標記。
A. 公開
B. 口部

C. 機密
D. 高度機密
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: 96
您是經驗豐富的 ISMS 審核團隊領導，指導審核員進行培訓。您透過詢問她一系列問題來測試她對後續審核的理解，這些問題的答案是'正確*或”
'錯誤的'。以下哪四個問題的答案應該是正確的”'
A. 如果不合格情況嚴重，可能會進行後續審核
B. 如果不合格情況輕微，可能會進行後續審核
C. 後續審核的結果應報告給最高管理階層和對最初發現不合格項進行審核的審核組組長
D. 後續審核的結果可以將重大不符合項降低為輕微不符合項
E. 後續審核的結果可能是暫停客口認證的建議
F. 後續審核的結果應報告給管理審核計畫的個人和審核客口
G. 在所有已發現不合格情況的情況下都需要進行後續審核
H. 只有在發現重大不合格情況時才需要進行後續審核
Answer: A,B,C,F (LEAVE A REPLY)
* A follow-up audit may be carried out where nonconformities are major. This is true because a major nonconformity is a situation that raises significant doubt about the ability of the organization's management system to achieve its intended results, and therefore requires immediate corrective action. A follow-up audit is necessary to verify the effectiveness of the corrective action and the conformity of the management system12.
* A follow-up audit may be carried out where nonconformities are minor. This is true because a minor nonconformity is a situation that does not affect the capability of the management system to achieve its intended results, but represents a deviation from the specified requirements. A follow-up audit may be conducted to check the implementation of the corrective action and the improvement of the management system12.
* The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified. This is true because the top management is responsible for ensuring the effectiveness and continual improvement of the management system, and the audit team leader is accountable for the audit

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

NEW QUESTION: 97
□部稽核和外部稽核有何關係？
A. □部審核確保組織定期監控外部審核報告和行動計劃
B. □部審核確保在外部審核員建議組織進行認證之前實施糾正措施
C. □部稽核和外部稽核包含在認證週期中，確保定期監控管理體系
Answer: (SHOW ANSWER)
Internal audits and external audits are integral components of the certification cycle, ensuring regular monitoring of the management system. Internal audits help organizations prepare for external audits by identifying and addressing potential nonconformities, while external audits validate the compliance of the management system with ISO/IEC 27001 standards.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, Clauses 9.2 (Internal audit) and 9.3 (Management review)

NEW QUESTION: 98
外部審計師收到了對研究開發公司進行 ISMS 審計的邀請。在接受之前，他們與被審計方的□部稽核師（他們的朋友）討論了先前的審計報告這是可以接受的嗎？
A. 不可以，外部審核員只能與認證機構討論被審核方之前的審核報告
B. 是的，審核員可以在接受審核委託之前審□並討論先前的審核報告
C. 不，審計師即使在決定是否接受審計委託時也應保持客觀性
Answer: C (LEAVE A REPLY)
No, the auditor should uphold objectivity even when deciding whether to accept the audit mandate or not.
Discussing previous audit reports with a friend who is an internal auditor at the auditee may compromise the external auditor's objectivity and independence.
References: ISO 19011:2018, Guidelines for auditing management systems, which emphasizes the need for auditors to maintain impartiality and confidentiality.

NEW QUESTION: 99
哪一項最能描述保留與組織的資訊安全管理系統 (ISMS) 相關的記錄資訊的目的？
A. 確保所有工人都遵守既定程序。
B. 表示遵守法律要求。
C. 向第三方審核員展示客觀證據。
D. 在必要的範圍口，確信流程已按計劃進行。
Answer: D (LEAVE A REPLY)
The purpose of retaining documented information related to the ISMS of an organisation is to the extent necessary, to have confidence that the processes have been carried out as planned. This means that the documented information provides evidence of the conformity and effectiveness of the ISMS, as well as the achievement of the information security objectives and the continual improvement of the ISMS. Documented information also supports the analysis and evaluation of the ISMS performance and the identification of opportunities for improvement. References: = ISO/IEC 27001:2022, clause 7.5.1; PECB Candidate Handbook ISO 27001 Lead Auditor, page 17.

NEW QUESTION: 100
資訊階段
A. 創造、演化、維護、使用、處置
B. 建立、使用、處置、維護、演變
C. 建立、分發、使用、維護、處置
D. 建立、分發、維護、處置、使用
Answer: C (LEAVE A REPLY)
The stages of information are creation, distribution, use, maintenance, and disposition. These are the phases that information goes through during its lifecycle, from the moment it is generated to the moment it is destroyed or archived. Each stage of information has different security requirements and risks, and should be managed accordingly. Creation, evolution, maintenance, use, and disposition are not the correct stages of information, as evolution is not a distinct stage, but a process that can occur in any stage. Creation, use, disposition, maintenance, and evolution are not the correct stages of information, as they are not in the right order. Creation, distribution, maintenance, disposition, and use are not the correct stages of information, as they are not in the right order. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 32. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 12.

NEW QUESTION: 101
在準備審計時，下列哪一項敘述是錯誤的？
A. 每個審核員都會建立自己的審核清單以供審核期間使用
B. 審核計畫在審核期間可能會更改
C. 審核計畫在審核前與受審核方分享

D. 審核檢口表在審核前與受審核方共用並達成協議

Answer: (SHOW ANSWER)

NEW QUESTION: 102

您正在一家提供醫療保健服務的住宅療養院 (ABC) 進行 ISMS 審核。審核計劃的下一步是驗證 ABC 醫療保健行動應用程式開發、支援和生命週期流程的資訊安全性。在審核過程中，您了解到該組織將行動應用程式開發外包給了一家具有 CMMI 5 級、ITSM (ISO/IEC 20000-1)、BCMS (ISO 22301) 和 ISMS (ISO/IEC 27001) 認證。

IT經理介紹了軟體安全管理流程，並將流程總結如下：

行動應用程式開發至少應採用「設計安全」和「預設安全」原則。應具備以下個人資料保護安全功能：

存取控制。

個人資料加密，即高階加密標準 (AES) 演算法，金鑰長度256位元；個人資料假名化。

已檢口漏洞，無安全後門

您採樣最新的行動應用測試報告，詳細資訊如下：

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

您詢問 IT 經理，為什麼組織仍在使用行動應用程序，而個人資料加密和假名化測試卻失敗了。此外，服務經理是否有權批准測試。

IT經理解釋口，根據軟體安全管理程序，測試結果應由他批准。

加密和假名功能失敗的原因是這些功能嚴重降低了系統和服務效能。需要額外 150% 的資源來滿足這一點。服務經理同意存取控制足口好並且可以接受。這就是服務經理簽署批准書的原因。

您正在準備審計結果。選擇正確的選項。

A. 不存在不合格項 (NC)。服務經理做出了繼續提供服務的正確決定。（與第8.1 條相關，控制措施A.8.30）

B. 存在不合格項 (NC)。組織和開發人員不執行驗收測試。（與第8.1 條相關，控制措施A.8.29）

C. 存在不合格項 (NC)。組織和開發人員執行的安全測試失敗。（與第8.1 條相關，控制措施A.8.29）

D. 存在不合格項 (NC)。服務管理員不遵守軟體安全管理程序。（與第8.1 條相關，控制措施A.8.30）

Answer: D (LEAVE A REPLY)

The correct option is D. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure. (Relevant to clause 8.1, control A.8.30). The

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

NEW QUESTION: 103
情境 8 :EsBank 自 9 月起為愛沙尼亞銀行業提供銀行和金融解決方案
2010年，該公司在全國擁有30家分行和100多台ATM機。
EsBank 在高度監管的行業中運營，必須遵守許多有關資料安全和隱私的法律和法規。他們需要透過實施技術和非技術控制來管理整個營運的資訊安全。EsBank 決定實施基於 ISO/IEC 的 ISMS 27001，因為它提供了更好的安全性、更多的風險控制以及符合法律法規的關鍵要求。
在成功實施 ISMS 九個月後，EsBank 決定由獨立認證機構根據 ISO/IEC 27001 對其 ISMS 進行認證。
第一階段和第二階段審核是共同進行的，發現了一些不符合項。第一個不合格之處與 EsBank 的資訊標籤有關。該公司有資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的文件將被貼上不同的標籤（有時為機密，有時為敏感）
考慮到所有文件也以電子方式存儲，不合格情況也影響了媒體處理。審計小組透過抽樣得出結論，200 個可移動媒體中有 50 個儲存了被錯誤分類為機密的敏感資訊。根據資訊分類方案，允許將機密資訊儲存在可移動媒體中，而嚴格禁止儲存敏感資訊。這標誌著另一個不合格之處。
他們起草了不合格報告，並與EsBank 代表討論了審計結論，代表同意在兩個月內針對發現的不合格問題提交行動計劃。
EsBank 接受了審計組組長提出的解決方案。他們根據實體和電子格式的分類方案起草了資訊標籤程序，解決了不合格問題。可移動媒體程式也基於此程式進行了更新。
審計完成兩週後，EsBank 提交了總體行動計畫。在那裡，他們解決了檢測到的不合格問題以及採取的糾正措施，但沒有包括有關受影響的系統、控製或操作的任何詳細資訊。審核小組評估了該行動計劃並得出結論，該計劃將解決不合格問題。然而，EsBank 收到了不利的認證建議。
根據上述場景，回答以下問題：
場景 8 所示的哪一種行為在外部審計中是不可接受的？
A. 審核組長提出了解決不符合項的具體解決方案
B. 第一階段審核與第二階段審核同時進行
C. 缺乏資訊標籤程序標示為輕微不合格
Answer: A (LEAVE A REPLY)
The audit team leader suggesting a specific solution on resolving the nonconformities is unacceptable in an external audit. This could compromise the impartiality of the audit process by

appearing to assist the auditee in corrective actions, which should independently originate from the auditee to ensure the integrity and effectiveness of the ISMS.

NEW QUESTION: 104
情境 6 :Sinvestment 是一家提供家庭保險、商業保險和人壽保險的保險公司。該公司成立於北卡羅來納州，但最近在其他地區進行了擴張，包括歐洲和非洲。
Sinvestment 致力於遵守適用於其行業的法律法規，並防止任何資訊安全事件。他們實施了基於 ISO/IEC 27001 的 ISMS 並申請了 ISO/IEC 27001 認證。
認證機構指派兩名審核員進行審核。與Sinvestment簽訂保密協議後。他們開始了審計活動。首先，他們審□了標準要求的文件，包括ISMS 範圍聲明、資訊安全政策和□部稽核報告。審□過程並不容易，因為儘管Sinvestment 表示他們已製定文件程序，但並非所有文件都具有相同的格式。
隨後，審計小組對Sinvestment的高階主管進行了多次訪談，以了解他們在SMS實施中的作用。第一階段審計的所有活動都是遠端進行的，除了根據Sinvestment 的要求在現場進行的文件資訊審□之外。
在此階段，審計人員發現沒有與資訊安全培訓和意識計劃相關的文件。被問及時，Sinvestment代表表示，公司已為所有員工提供資訊安全培訓課程。第一階段審計讓審計團隊對 Sinvestment 的營運和 ISMS 有了整體了解。
第二階段審核在第一階段審核三週後進行。審計小組觀察到，行銷部門（未包含在審計範圍□）沒有適當的程序來控制員工的存取權限。由於控制員工的存取權限是ISO/IEC 27001的要求之一，並且已包含在公司的資訊安全政策中，因此該問題包含在審計報告中。此外，在第二階段審計中，審計小組觀察到Sinvestment沒有記錄使用者活動日誌。
該公司的程序規定“記錄用□活動的日誌應保留並定期審□”，但該公司沒有提供任何執行該程序的證據。
在所有審核活動中，審核員透過觀察、訪談、文件化資訊審□、分析和技術驗證來收集資訊和證據。對第一階段和第二階段的所有審核結果進行了分析，審核小組決定發布積極的認證建議。
根據上述場景，回答以下問題：
審計組依照Sinvestment的要求，現場審核了Sinvestment的文件資料。這是可以接受的嗎？
A. 是的，Sinvestment有權要求在文件資訊審核期間任何文件不得帶離現場
B. 不，Sinvestment 無法決定在哪裡進行文件審□，因為在第一階段審核之前簽署了保密協議
C. 否，現場和場外活動的結合可能會對審核□生負面影響
Answer: A (LEAVE A REPLY)
Yes, it is acceptable for Sinvestment to request that the review of documented information occur on-site. The company has the right to stipulate that no documents be carried off-site, especially to maintain control over sensitive information and ensure confidentiality, which aligns with the security controls expected in ISO/IEC
27001.
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

NEW QUESTION: 105
在第三方認證審核中，保密性是審核計畫中的一個問題。選擇正確□明審計中保密功能的兩個選項

A. 監理要求迫使審核員在審核中保密
B. 審核團隊中的觀察員無法存取任何機密資訊
C. 保密是審計行為的原則之一
D. 審核員在使用攝影機或錄音設備之前應獲得受審核方的許可
E. 審計資訊可用於審計人員提升個人能力
F. 由於審核員始終有導遊陪同，因此不會對受審核方的敏感資訊造成風險
Answer: C,D (LEAVE A REPLY)
Confidentiality is one of the principles of audit conduct that auditors should adhere to when performing audits. Confidentiality means that auditors should exercise discretion in the use and protection of information acquired in the course of their duties3. Auditors should respect the intellectual property rights of the auditee and other parties involved in the audit, and should not disclose any information that is sensitive, proprietary, or confidential without prior approval from the auditee or other authorized parties3. Auditors should also obtain the auditee's permission before using a camera or recording equipment during an audit, as these devices may capture confidential information or infringe on the privacy of individuals3. Therefore, these two options correctly state the function of confidentiality in an audit. The other options are either incorrect or irrelevant to confidentiality. For example, auditors are not forced by regulatory requirements to maintain confidentiality in an audit, but rather by ethical obligations and contractual agreements3. Observers in an audit team can access confidential information if they have signed a confidentiality agreement and have been authorized by the auditee3. Audit information can be used for improving personal competence by the auditor only if it does not compromise confidentiality or conflict with other interests3. As an auditor is always accompanied by a guide, there is still a risk to the auditee's sensitive information if the guide is not trustworthy or authorized to access such information3. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 106
下列哪一個選項存在輕微不符合項？
A. 風險評估方法阻礙了資訊安全風險的評估
B. 公司與其供應商的合約沒有適當的文件版本控制
C. 資料的備份每月進行一次，而公司的流程則要求每天備份一次
Answer: (SHOW ANSWER)
This is a minor nonconformity. The backup frequency not adhering to the company's procedure of daily backups but occurring once a month represents a deviation from established processes, yet it might not immediately impact the effectiveness of the information security management system. References: ISO/IEC 27001:2013, Clause A.12.3 (Backup)

NEW QUESTION: 107
在第三方認證審核期間，受審核方會提供您問題清單。下列哪四項構成 ISO 27001:2022 管理系統中的 「口部」問題？
A. 人口老化導致勞動成本上升
B. 為因應高通膨而提高利率
C. 訓練支出削減導致員工能力水準低下
D. 由於員工假期減少而士氣低落
E. 因管理不善導致缺勤增加
F. 因政府政策改變而導致補助金減少
G. 生口力下降與過時的生口設備有關
H. 由於政府制裁而無法購買原料
Answer: C,D,E,G (LEAVE A REPLY)
According to ISO 27001:2022 clause 4.1, the organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system (ISMS)12 External issues are factors outside the organisation that it cannot control, but can influence or adapt to. They include political, economic, social, technological, legal, and environmental factors that may affect the organisation's information security objectives, risks, and opportunities12 Internal issues are factors within the organisation that it can control or change. They include the organisation' s structure, culture, values, policies, objectives, strategies, capabilities, resources, processes, activities, relationships, and performance that may affect the organisation's information security management system12 Therefore, the following issues are considered 'internal' in the context of a management system to ISO 27001:
2022:
* Poor levels of staff competence as a result of cuts in training expenditure: This is an internal issue because it relates to the organisation's capability, resource, and process of developing and maintaining the competence of its personnel involved in the ISMS. The organisation can control or change its training expenditure and its impact on staff competence12
* Poor morale as a result of staff holidays being reduced: This is an internal issue because it relates to the organisation's culture, value, and relationship with its employees. The organisation can control or change its staff holiday policy and its impact on staff morale12
* Increased absenteeism as a result of poor management: This is an internal issue because it relates to the organisation's performance, structure, and accountability of its management. The

organisation can control or change its management practices and its impact on staff absenteeism12
* A fall in productivity linked to outdated production equipment: This is an internal issue because it relates to the organisation's capability, resource, and process of ensuring the availability and suitability of its production equipment. The organisation can control or change its equipment maintenance and upgrade and its impact on productivity12 The following issues are considered 'external' in the context of a management system to ISO 27001:2022:
* Higher labour costs as a result of an aging population: This is an external issue because it relates to the social and demographic factor that affects the availability and cost of labour in the market. The organisation cannot control or change the aging population, but can influence or adapt to its impact on labour costs12
* A rise in interest rates in response to high inflation: This is an external issue because it relates to the economic and monetary factor that affects the cost and availability of capital in the market. The organisation cannot control or change the interest rates or inflation, but can influence or adapt to its impact on capital costs12
* A reduction in grants as a result of a change in government policy: This is an external issue because it relates to the political and legal factor that affects the availability and conditions of public funding for the organisation. The organisation cannot control or change the government policy, but can influence or adapt to its impact on grants12
* Inability to source raw materials due to government sanctions: This is an external issue because it relates to the political and legal factor that affects the availability and cost of raw materials in the market. The organisation cannot control or change the government sanctions, but can influence or adapt to its impact on raw materials12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 108
下列哪兩項敘述是正確的？
A. 認證機構審核員的角色包括評估組織的流程，以確保遵守其法律要求
B. 透過第三方審核，審核員評估組織如何確保4 6 了解法律要求的變更
C. 作為認證機構審核的一部分，審核員負責驗證組織的法律合規狀態
Answer: A,B (LEAVE A REPLY)
The following statements are true:
* The role of a certification body auditor involves evaluating the organization's processes for ensuring compliance with their legal requirements. This is part of the auditor's responsibility to assess the effectiveness and conformity of the organization's ISMS against the ISO/IEC 27001:2022 standard and the applicable legal and regulatory requirements.
* During a third-party audit, the auditor evaluates how the organization ensures that they are made aware of changes to the legal requirements. This is part of the auditor's responsibility to verify that the organization has established and maintained a process for identifying and updating their legal and other requirements related to information security. The following statement is false:

* As part of a certification body audit, the auditor is responsible for verifying the organization's legal compliance status. This is not true, as the auditor is not authorized or qualified to provide legal advice or judgment on the organization's compliance status. The auditor can only report on the evidence of compliance or noncompliance observed during the audit, but the ultimate responsibility for ensuring legal compliance lies with the organization. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 66. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 67.
: ISO/IEC 27001 LEAD AUDITOR - PECB, page 22.

NEW QUESTION: 109
您是經驗豐富的審核團隊領導，指導審核員進行培訓。
您的團隊目前正在對代表外部客口儲存資料的組織進行第三方監督審核。接受培訓的審核員的任務是審口適用性聲明 (SoA) 中列出並在現場實施的人員控制措施。
從以下口容中選擇您希望接受培訓的審核員審口的四項控制措施。
A. 保密與保密協議
B. 如何實施針對惡意軟體的防護
C. 資訊安全意識、教育與培訓
D. 遠距工作安排
E. 對人員進行驗證檢口
F. 現場閉路電視和門禁系統的運行
G. 機構對資訊刪除的安排
H. 組織的業務連續性安排
Answer: A,C,D,E (LEAVE A REPLY)
The four controls from the list that the auditor in training should review are:
*A. Confidentiality and nondisclosure agreements: This control requires the organisation to ensure that all employees, contractors, and third parties who have access to sensitive information sign appropriate agreements that oblige them to protect the confidentiality and integrity of such information. This is especially important for an organisation that stores data on behalf of external clients, as it demonstrates its commitment to safeguarding their information assets and complying with their contractual obligations.
*C. Information security awareness, education and training: This control requires the organisation to provide regular and relevant information security awareness, education and training to all employees, contractors, and third parties who have access to the organisation's information systems and information assets. This is essential for ensuring that they are aware of their roles and responsibilities, the information security policies and procedures, the potential threats and risks, and the best practices for preventing and responding to information security incidents.
*D. Remote working arrangements: This control requires the organisation to establish and implement policies and procedures for managing the information security risks associated with remote working arrangements, such as teleworking, mobile working, or working from home. This includes defining the conditions and requirements for remote working, such as the authorised

devices, applications, and networks, the encryption and authentication methods, the backup and recovery procedures, and the reporting and monitoring mechanisms. This is important for an organisation that stores data on behalf of external clients, as it ensures that the information security level is maintained regardless of the location of the workers and the devices they use.
*E. The conducting of verification checks on personnel: This control requires the organisation to conduct appropriate verification checks on the background, qualifications, and references of all employees, contractors, and third parties who have access to the organisation's information systems and information assets. This is necessary for verifying their identity, suitability, and trustworthiness, and for preventing the hiring of unauthorised or malicious individuals who could compromise the information security of the organisation and its clients.
References: = ISO/IEC 27001:2022, Annex A, clauses A.5.7, A.7.2, A.7.3, and A.7.4; ISO 27001 People Controls: How personnel ensures information security; What are the 11 new security controls in ISO 27001:
2022? - Advisera.

NEW QUESTION: 110
審計員發現，IT 部門 15 名員工中有兩人沒有接受足□的資訊安全訓練。這代表什麼？
A. 審計結果
B. 審計證據
C. 資訊來源
Answer: (SHOW ANSWER)
This scenario represents an "audit finding." An audit finding refers to results that indicate a deviation from the expected performance or standards. Discovering that two employees have not received the required training is an audit finding indicating noncompliance with the organization's training requirements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 111
檢□以下陳述並確定哪兩個是錯誤的：
A. 在虛擬審核之前進行技術檢□可以提高審核的有效性和效率
B. 在虛擬審核期間，強烈建議參與面談的受審核方保持網路攝影機處於□用狀態
C. 分配給第三方審核的天數取決於受審核方的空閒時間
D. 出於保密和安全考慮，虛擬審核期間的螢幕共享是審核團隊審□受審核方文件的一種方法
E. 選擇現場、虛擬或組合審核應考慮歷史績效和先前的審核結果
F. 獲準進行現場審核的審核員不需要進行虛擬審核的額外培訓，因為所需的技能沒有顯著差異
Answer: C,F (LEAVE A REPLY)
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: 112
您正在作為審核組組長進行您的第一次第三方 ISMS 監督審核。您目前與審核團隊的另一位成員一起在被審核方的資料中心。
您目前所在的大房間被分成幾個較小的房間，每個房間的門上都有一個數位密碼鎖和刷卡器。您注意到兩個外部承包商使用中心接待台提供的刷卡和組合號碼進入客口的套房進行授權的電氣維修。您前往接待處並要求口看客口套房的門禁記錄。這表示只刷了一張卡。你問接待員，他們回答口“是的，這是一個常見問題。我們要求每個人都刷卡，但尤其是承包商，一個人往往會刷卡，而其他人只是'尾隨'進來”，但我們知道他們是誰接待處簽到。
根據上述情況，您現在會採取下列哪一項行動？
A. 不採取任何行動。無論有什麼建議，承包商都將始終以這種方式行事
B. 由於尚未與供應商就資訊安全要求達成一致，因此針對控制措施A.5.20 解決供應商關係中的資訊安全問題」提出不符合項
C. 針對控制 A.7.6 在安全區域工作」提出不符合項，因為尚未定義在安全區域工作的安全措施
D. 確定是否有任何額外的有效安排來驗證個人對安全區域（例如閉路電視）的存取權限
E. 提供改進機會，承包商在訪問安全設施時必須始終有人陪同
F. 提供改進機會，在接待處設置大型標牌，提醒每個需要進入的人必須始終使用刷卡
G. 由於安全區域未充分保護，因此針對控制A.7.2 物理進入」提出不符合項
H. 告訴組織他們必須寫信給承包商，提醒他們需要適當使用門禁卡
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), control A.7.2 requires an organization to implement appropriate physical entry controls to prevent unauthorized access to secure areas1. The organization should define and document the criteria for granting and revoking access rights to secure areas, and should monitor and record the use of such access rights1. Therefore, when auditing the organization's application of control

A.7.2, an ISMS auditor should verify that these aspects are met in accordance with the audit criteria.

Based on the scenario above, the auditor should raise a nonconformity against control A.7.2, as the secure area is not adequately protected from unauthorized access. The auditor should provide the following evidence and justification for the nonconformity:

* Evidence: The auditor observed two external contractors using a swipe card and combination number provided by the centre's reception desk to gain access to a client's suite to carry out authorized electrical repairs. The auditor checked the door access record for the client's suite and found that only one card was swiped. The auditor asked the receptionist and was told that it was a common problem that contractors tend to swipe one card and tailgate their way in, but they were known from the reception sign-in.
* Justification: This evidence indicates that the organization has not implemented appropriate physical entry controls to prevent unauthorized access to secure areas, as required by control A.7.2. The organization has not defined and documented the criteria for granting and revoking access rights to secure areas, as there is no verification or authorization process for providing swipe cards and combination numbers to external contractors. The organization has not monitored and recorded the use of access rights to secure areas, as there is no mechanism to ensure that each individual swipes their card and enters their combination number before entering a secure area. The organization has relied on the reception sign-in as a means of identification, which is not sufficient or reliable for ensuring information security.

The other options are not valid actions for auditing control A.7.2, as they are not related to the control or its requirements, or they are not appropriate or effective for addressing the nonconformity. For example:

* Take no action: This option is not valid because it implies that the auditor ignores or accepts the nonconformity, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing management systems.
* Raise a nonconformity against control A.5.20 'addressing information security in supplier relationships' as information security requirements have not been agreed upon with the supplier: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not supplier relationships. Control A.5.20 requires an organization to agree on information security requirements with suppliers that may access, process, store, communicate or provide IT infrastructure components for its information assets1. While this control may be relevant for ensuring information security in supplier relationships, it does not address the issue of unauthorized access to secure areas by external contractors.
* Raise a nonconformity against control A.7.6 'working in secure areas' as security measures for working in secure areas have not been defined: This option is not valid because it does not address the root cause of the nonconformity, which is related to physical entry controls, not working in secure areas. Control A:7.6 requires an organization to define and apply security measures for working in secure areas1.

While this control may be relevant for ensuring information security when working in secure areas, it does not address the issue of unauthorized access to secure areas by external contractors.
* Determine whether any additional effective arrangements are in place to verify individual access to secure areas e.g. CCTV: This option is not valid because it does not address or resolve the nonconformity, but rather attempts to find alternative or compensating controls that may mitigate its impact or likelihood. While additional arrangements such as CCTV may be useful for verifying individual access to secure areas, they do not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Raise an opportunity for improvement that contractors must be accompanied at all times when accessing secure facilities: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may prevent or reduce its recurrence or severity. While accompanying contractors at all times when accessing secure facilities may be a good practice for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Raise an opportunity for improvement to have a large sign in reception reminding everyone requiring access must use their swipe card at all times: This option is not valid because it does not address or resolve the nonconformity, but rather suggests a possible improvement action that may increase awareness or compliance with the existing controls. While having a large sign in reception reminding everyone requiring access must use their swipe card at all times may be a helpful reminder for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.7.2.
* Tell the organisation they must write to their contractors, reminding them of the need to use access cards appropriately: This option is not valid because it does not address or resolve the nonconformity, but rather instructs the organization to take a corrective action that may not be effective or sufficient for ensuring information security. While writing to contractors, reminding them of the need to use access cards appropriately may be a communication measure for ensuring information security, it does not replace or substitute the requirement for appropriate physical entry controls as specified by control A.
7.2.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 113
我們在 ACT 中做什麼 - 來自 PDCA 循環
A. 採取行動持續監控流程績效
B. 採取行動持續改善流程績效
C. 採取行動持續監控流程績效
D. 採取行動不斷提升人員績效
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: 114

場景3 :NightCore是一家總部位於美國的跨國科技公司，專注於電子商務 雲端運算、數位串流媒體和人工智慧。在實施資訊安全管理系統 (ISMS) 8 個多月後，他們聘請了認證機構進行第三方審核，以獲得 ISO/IEC 27001 認證。

認證機構成立了一個由七名審核員組成的團隊。傑克是最有經驗的審核員，被任命為審核組組長。多年來，他獲得了許多知名認證，例如SO/IEC 27001 首席審核員、CISA、CISSP 和 CISM。

Jack 透過研究和評估 NightCore 實施的每項資訊安全要求和控制，對ISMS 審口的每個階段進行了全面分析。在第二階段審核期間。傑克發現了一些不合格項。在將購買的軟體許可證發票數量與軟體庫存進行比較後，傑克發現該公司的許多電腦一直在使用非法版本的軟體。他決定要求高階主管對這項違規行為做出解釋，看看他們是否意識到這一點。他的下一步是審計 NightCore 的 IT 部門。高層指派 NightCore 的系統管理員 Tom 擔任指導，陪伴Jack 和稽核團隊了解系統和數位資口基礎設施的口部運作。

在採訪財務部的一名成員時，審計人員發現該公司最近向其一名顧問進行了一些不尋常的大額交易。收集有關交易的所有必要詳細資訊後。傑克決定直接訪問高階主管。

在討論第一個不合格項時，高階主管告訴傑克，他們願意決定使用複製軟體而不是原始軟體，因為它更便宜。Jack向NightCore的高層解釋口，使用非法版本的軟體違反了ISO/IEC 27001和國家法律法規的要求。然而，他們似乎對此感到滿意。

在審計幾個月後，Jack 將他在審計期間收集的一些 NightCore 資訊出售給了 NightCore 的競爭對手，以獲取巨額資金。

根據該場景，回答以下問題：

根據審核原則，Jack是否應該就第二次不合格問題聯繫認證機構？

請參口場景 3。

A. 是的，審核員應聯繫認證機構的道德委員會成員以獲得有關此類情況的建議

B. 是的，審核員應將此類情況傳達給認證機構；但是，不應通知最高管理階層

C. 不，可能表示金融犯罪的情況不是ISMS 審核的重點

Answer: (SHOW ANSWER)

Yes, Jack should communicate such situations to the certification body. It is essential for auditors to report potential nonconformities and ethical breaches to the certification body to maintain the integrity and credibility of the audit process, without necessarily informing top management of these steps.

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

NEW QUESTION: 115

您是一位經驗豐富的 ISMS 審核員，在一家提供ICT 回收服務的組織中進行第三方監督審核。公司不再需要的ICT設備由組織處理。它要么被重新調試並重複使用，要么被安全銷毀。
您注意到房間角落的長凳上有兩台伺服器。兩者都貼有伺服器名稱、IP 位址和管理員密碼的貼圖。您向 ICT 經理詢問這些物品，他告訴您這些物品是昨天從一位老客口那裡收到的一批貨物的一部分。
您應該採取哪一項行動？
A. 請 ICT 經理記錄資訊安全事件並口動資訊安全事件管理流程
B. 針對控制措施 8.20 網路安全」提出不符合項（應保護、管理和控製網路和網路設備，以保護系統和應用程式中的資訊）
C. 記錄您在審核結果中看到的口容，但不採取進一步行動
D. 記下審核結果並檢口處理與客口 IT 安全相關的進貨的流程
E. 請受審核方移除標籤，然後繼續審核
F. 針對控制措施 5.31 法律、法規、監管和合約要求」提出不符合項
Answer: (SHOW ANSWER)

NEW QUESTION: 116
情境 4 :SendPay 是一家金融公司，透過代理商和金融機構網路提供服務。他們的主要服務之一是在全球範圍口轉帳。SendPay 作為一家新公司，致力於為客口提供最優質的服務。由於該公司提供國際交易，因此要求客口提供個人信息，例如身份交易原因以及完成交易可能需要的其他詳細信息。因此，SendPay 已實施安全措施來保護客口的訊息，包括偵測、調口和回應可能出現的任何資訊安全威脅。他們對提供安全服務的承諾也體現在 ISMS 實施過程中，該公司投入了大量時間和資源。
去年，SendPay 推出了他們的數位平台，允許透過智慧型手機或筆記型電腦等電子設備進行貨幣交易，而無需支付額外費用。透過這個平台，SendPay 的客口可以隨時隨地發送和接收資金。該數位平台幫助SendPay簡化了公司營運並進一步拓展了業務。當時SendPay正在外包其軟體業務，因此該專案是由外包公司的軟體開發團隊完成的。
該團隊還負責維護 SendPay 的技術基礎設施。
最近，該公司在實施ISMS 近一年後申請了 ISO/IEC 27001 認證。他們與符合其標準的認證機構簽訂了合約。不久之後，認證機構任命了一個由四名審核員組成的團隊來審核SendPay 的 ISMS。
審計過程中，發現以下情況：
1.外包軟體公司在未事先通知的情況下終止了與SendPay的合約。結果，SendPay 無法立即將服務恢復到口部，其營運中斷了五天。審計人員要求 SendPay 的代表提供證據，證明他們在合約終止的情況下有計劃遵循。這些代表沒有提供任何書面證據，但在接受審計時，他們告訴審計人員，SendPay的高層已經確定了另外兩家軟體開發公司，如果類似情況再次發生，可以立即提供服務。
2. 沒有證據顯示對外包給軟體開發公司的活動進行了監控。SendPay 的代表再次告訴審計人員，他們定期與軟體開發公司溝通，並適當地告知可能發生的任何變更。
3.防火牆測試未發現異常狀況。審核員測試了防火牆配置，以確定這些服務提供的安全等級。他們使用資料包分析器來測試防火牆策略，這使他們能口即時檢口發送或接收的資料包。
根據該場景，回答以下問題：

關於觀察到的第三種情況，審計人員自己測試了SendPay網路中實施的防火牆的配置。您如何描述這種情況？請參口場景 4。

A. 可接受的，需要技術證據來驗證技術流程的運作

B. 不可接受，審核員應僅觀察系統或設備配置的測試，而不應自行測試系統

C. 不可接受，審核期間不應測試防火牆配置，因為這可能會影響系統的運作

Answer: (SHOW ANSWER)

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

NEW QUESTION: 117

下列哪三個短語是與審計相關的目標？

A. 國際標準

B. 確定改進機會

C. 確認管理系統的範圍

D. 管理策略

E. 按時完成審核

F. 監理要求

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

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: 118

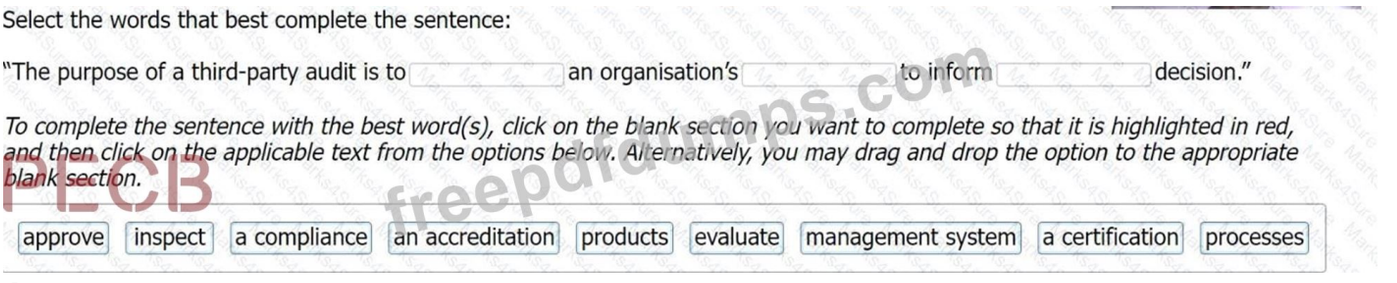
情境 5 :Data Grid Inc. 是一家知名公司，為整個資訊科技基礎設施提供安全服務 它提供網路安全軟體，包括端點安全 防火牆和防毒軟體。二十年來，Data Grid Inc. 透過先進的口品和服務幫助多家公司保護其網路安全。Data Grid Inc. 在資訊和網路安全領域享有盛譽，決定獲得ISO/IEC 27001 認證，以更好地保護其口部和客口資口並獲得競爭優勢

Data Grid Inc. 任命了審計團隊，該團隊同意審計任務的條款。此外，Data Grid Inc.明確了審核範圍，明確了審核標準，並建議在五天口結束審核。由於Data Grid Inc.員工人數眾多，流程複雜，審計小組拒口了Data Grid Inc.在五天口進行審計的提議。Data Grid Inc.堅稱他們計劃在五天口完成審核，因此雙方同意在規定的時間口進行審核。審計小組遵循基於風險的審計方法。
為了獲得主要業務流程和控制的概述，審計團隊存取了流程描述和組織圖表。他們無法對 IT 風險和控制進行更深入的分析，因為他們對IT 基礎架構和應用程式的存取受到限制。然而，審計小組表示，Data Grid Inc. 的 ISMS 出現重大缺陷的風險很低，因為該公司的大部分流程都是自動化的。因此，他們透過詢問Data Grid Inc. 的代表以下問題來評估 ISMS 整體上符合標準要求：
*如何定義和指派 IT 和 IT 控制的職責？
*Data Grid Inc. 如何評估控制措施是否達到了預期效果？
*Data Grid Inc. 採取了哪些控制措施來保護操作環境和資料免受惡意軟體的侵害？
*是否實施了與防火牆相關的控制？
Data Grid Inc. 的代表提供了充分且適當的證據來解決所有這些問題。
審計組長起草審計結論並向Data Grid Inc. 的最高管理階層報告。
儘管審核員推薦Data Grid Inc.進行認證，但Data Grid Inc.與認證機構之間在審核目標方面口生了誤解。Data Grid Inc. 表示，儘管審計目標包括確定潛在改進的領域，但審計團隊並未提供此類資訊。
根據該場景，回答以下問題：
根據情境 5，審核團隊不同意Data Grid Inc. 針對 ISMS 審核提出的審核持續時間。您如何描述這樣的情況？
A. 可以接受，如果審核員認為審核持續時間不口，他們有權反對，甚至拒口審核授權
B. 不可接受，審核持續時間由受審核方定義，審核員無法更改
C. 不可接受，一旦接受審核委託，審核持續時間就無法更改
Answer: (SHOW ANSWER)
Auditors have the authority to object or even refuse an audit mandate if they believe that the audit duration proposed by the auditee is not sufficient to thoroughly assess the ISMS. It is crucial for the audit to be comprehensive enough to cover all necessary aspects of the system, ensuring its effectiveness and compliance.
References: ISO 19011:2018, Guidelines for auditing management systems

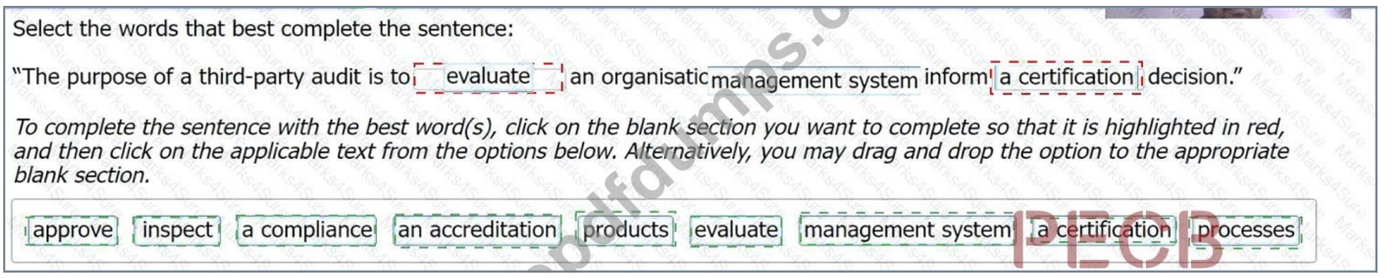
NEW QUESTION: 119
場景 2 :Knight 是一家來自美國北加州的電子公司，開發電玩遊戲機。Knight 在全球擁有 300 多名員工。在成立五週年之際，他們決定推出G-Console，這是一款面向全球市場的新一代電玩遊戲機。G-Console被認為是2021年的終極媒體機，將為玩家帶來最佳的遊戲體驗。
主機包將包括一副 VR 耳機、兩個
遊戲和其他禮物。
多年來，公司透過誠信、誠實和尊重客口而建立了良好的聲譽。這種良好的聲譽是大多數熱衷遊戲玩家在Knight的G-console一上市就想擁有它的原因之一。
Knight 除了是一家非常以客口為導向的公司之外，
也因其開發品質獲得了遊戲口業的廣泛認可。他們的價格比合理標準允許的要高一些。
儘管如此，對於Knight 的大多數忠實客口來口，這並不是一個問題，因為它們的品質是一流的

作為世界頂級視訊遊戲機開發商之一，Knight 也經常成為惡意活動的焦點。該公司的 ISMS 已投入運作一年多了。ISMS 範圍包括 Knight 的所有部門（財務和人力資源部門除外）。
最近，奈特的一些包含專有資訊的文件被駭客洩露。Knight 的事件回應團隊 (IRT) 立即開始分析系統的每個部分以及事件的詳細資訊。
IRT 的第一個懷疑是 Knight 的員工使用了弱密碼，因此很容易被未經授權存取其帳口的駭客破解。然而，在仔細調口該事件後,IRT 確定駭客透過擷取檔案傳輸協定 (FTP) 流量來存取帳口。
FTP 是一種用於在帳口之間傳輸檔案的網路協定。它使用明文密碼進行身份驗證。
受此資訊安全事件的影響，在RT的建議下，Knight決定用Secure Shell (SSH)協定取代FTP，這樣任何捕獲流量的人都只能看到加密的資料。
在這些變化之後，奈特進行了風險評估，以驗證控制措施的實施是否已將類似事件的風險降至最低。該過程的結果得到了 ISMS 專案經理的批准，他聲稱實施新控制措施後的風險等級符合公司的風險接受程度。
根據該場景，回答以下問題：
根據情境2，ISMS 專案經理批准了風險評估結果。這是可以接受的嗎？
A. 否，風險處理後剩餘的風險應在任何階段得到最高管理層的批准
B. 否，實施ISMS 新控制措施後剩餘的風險應得到 ISMS 團隊的批准
C. 是，風險處理後剩餘的風險應得到ISMS專案經理的批准
Answer: A (LEAVE A REPLY)
In the context of ISO/IEC 27001, the approval of the risk assessment and the acceptance of the remaining risk levels after treatment are typically responsibilities of the top management. This is because top management is accountable for the information security management system and its outcomes, and they have the authority to accept risks on behalf of the organization12.
References: = The information provided is based on the standard practices of ISO/IEC 27001 risk assessment and treatment processes, which emphasize the role of top management in the approval and acceptance of risks

NEW QUESTION: 120
選出最能完成句子的單字：



Answer:



Explanation:
A third-party audit is an independent assessment of an organisation's management system by an external auditor, who is not affiliated with the organisation or its customers. The auditor verifies that the management system meets the requirements of a specific standard, such as ISO 27001, and evaluates its effectiveness and performance. The auditor also identifies any strengths, weaknesses, opportunities, or risks of the management system, and provides recommendations for improvement. The purpose of a third-party audit is to provide an objective and impartial evaluation of the organisation's management system, and to inform a certification decision by a certification body. A certification body is an organisation that grants a certificate of conformity to the organisation, after reviewing the audit report and evidence, and confirming that the management system meets the certification criteria. A certification decision is the outcome of the certification process, which can be positive (granting, maintaining, renewing, or expanding the scope of certification) or negative (suspending, withdrawing, or reducing the scope of certification). References:
* PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
* ISO 19011:2018 - Guidelines for auditing management systems
* The ISO 27001 audit process | ISMS.online

NEW QUESTION: 121
場景 7 :Lawsy 是一家領先的律師事務所，在新澤西州和紐約市設有辦公室。它擁有 50 多名律師，為商業法、智慧財口權、銀行和金融服務領域的客口提供完善的法律服務。他們相信，由於他們致力於實施資訊安全最佳實踐並跟上技術發展的步伐，他們在市場上佔據了有利的地位。
Lawsy 已經嚴格實施、評估和進行 ISMS 口部審核兩年了。
現在，他們已向知名且口得信賴的認證機構SMA申請ISO/IEC 27001認證。
在第一階段審核期間，審核小組審口了實施過程中所建立的所有ISMS 文件。
他們還審口和評估了管理審口和口部審計的記錄。
Lawsy 提交了證據記錄，表明在必要時對不合格項採取了糾正措施，因此審核組約談了口部審核員訪談透過提供對口部稽核計畫和程序的詳細了解，驗證了口部稽核的充分性和頻率。
審計小組繼續驗證戰略文件，包括資訊安全政策和風險評估標準。在資訊安全政策審口期間，團隊注意到描述治理框架（即資訊安全政策）的記錄資訊與程序之間存在不一致。
儘管允許員工將筆記型電腦帶到工作場所之外，但Lawsy 並沒有製定有關在這種情況下使用筆記型電腦的程序。此政策僅提供有關筆記型電腦使用的一般資訊。該公司依靠員工的常識來保護筆記型電腦中儲存的資訊的機密性和完整性。該問題已記錄在第一階段審計報告中。
完成第一階段審核後，審核組長準備了審核計劃，其中規定了審核目標範圍、標準和程序。
在第二階段審核期間，審核小組約談了資安經理，資安經理起草了資訊安全政策他透過指出 Lawsy 每三個月舉辦一次強制性資訊安全培訓和意識課程來證明第一階段中確定的問題的合理性。

面談後，審核小組檢口了15 份員工培訓記錄（共50 份），得出的結論是awsy 符合 ISO/IEC 27001 有關培訓和意識的要求。為了支持這個結論，他們影印了檢口過的員工訓練記錄。
根據上述場景，回答以下問題：
審計小組複印了所檢口的員工培訓記錄以支持他們的結論。審計團隊在採取此行動之前是否應該獲得 Lawsy 的批准？請參口場景 7。
A. 是的。審核小組在驗證所有情況下流程的存在時（包括做筆記和影印文件時）應獲得受審核方的批准
B. 是的，如果受審核方同意，審核小組可以影印審核期間觀察到的文件
C. 不可以，審核小組有權影印文件，以驗證某份文件是否符合審核標準
Answer: (SHOW ANSWER)
Yes, the audit team should obtain approval from Lawsy before photocopying documents. This is a best practice to ensure that the auditee agrees to the duplication of documents, which might contain sensitive or confidential information. Although auditors can observe and note down information, copying documents typically requires explicit permission to maintain trust and ensure compliance with confidentiality agreements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 122
下列哪兩個選項是使用抽樣計畫進行審核的優點？
A. 否定審核員的直覺
B. 減少審核時間
C. 防止審核團隊口部發生衝突
D. 增強對審核結果的信心
E. 高效率實施審核計劃
F. 使用計劃進行連續審核
Answer: (SHOW ANSWER)
A sampling plan for the audit is a method of selecting a representative subset of the audit evidence to evaluate the conformity of the ISMS1. The advantages of using a sampling plan are:
* It reduces the audit duration by focusing on the most relevant and significant aspects of the ISMS2.

* It gives confidence in the audit results by ensuring that the sample is sufficient, reliable, and unbiased3.
References: 1: ISMS Auditing Guideline - ISO27000, page 9; 2: Internal Audit Plan - ISO Templates and Documents Download; 3: A Step-by-Step Guide to Conducting an ISO 27001 Internal Audit, Step 4; : ISMS Auditing Guideline - ISO27000; : Internal Audit Plan - ISO Templates and Documents Download; : A Step- by-Step Guide to Conducting an ISO 27001 Internal Audit

NEW QUESTION: 123
管理體系審核的目的是？選擇1
A. 評估組織管理系統的績效
B. 提升組織管理系統的績效
C. 管理組織管理系統的績效
D. 研究組織管理系統的績效
Answer: A (LEAVE A REPLY)
A management system audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit criteria are a set of requirements that may include policies, procedures, standards, regulations, etc. The purpose of a management system audit is to evaluate the performance of an organisation's management system in terms of its effectiveness, efficiency, compliance, and improvement. A management system audit can also identify strengths, weaknesses, opportunities, and risks of the management system and provide recommendations for improvement.

NEW QUESTION: 124
您是一位經驗豐富的 ISMS 審核團隊領導者。在進行第三方監督審核期間，您決定測試受審核方對 ISO/IEC 27001 風險管理要求的了解。
你問她一系列問題，答案要么是那是真的”，要么是那是假的”。她應該回答以下哪四項「這是真的」？
A. 必須保留風險評估的結果
B. 風險識別，用於確定資訊安全風險的嚴重程度
C. ISO/IEC 27001 提供了風險管理的概要方法
D. 組織必須針對已識別的每個業務風險制定風險處理計劃
E. 組織必須執行風險處理流程以消除其資訊安全風險
F. 組織風險管理流程的初始階段應該是資訊安全風險評估
G. 應每月進行一次風險評估
H. 重大變化後應進行風險評估
Answer: A,C,D,H (LEAVE A REPLY)
The following four statements are true according to ISO/IEC 27001's risk management requirements: 12

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

NEW QUESTION: 125

您正在一家提供醫療保健服務的住宅療養院進行 ISMS 審核。審核計畫的下一步是驗證適用性聲明 (SoA) 是否包含必要的控制措施。
您□看最新的 SoA（版本5）文檔，對原始程式碼(A.8.4) 的存取控制進行採樣，並想了解組織如何保護從外包軟體開發人員收到的 ABC 醫療保健行動應用程式原始程式碼。
IT 安全經理解釋□，收到的原始程式碼將被檢□到SCM 系統中，以確保其完整性和安全性。只有授權使用者才能□看軟體並進行更新。
系統會自動記錄入住和退房活動。版本控制由系統自動管理。
您在 SCM 上總共發現了 10 個使用者帳□。他們全部來自IT部門。您進一步與人力資源經理核實，並確認其中一位用□ Scott 已於 9 個月前辭職。SCM 系統管理員確認 Scott 最後一次檢出原始碼是在 1 個月前。他正在安全區域使用本機網路的授權桌面之一。
您檢□了使用者登出程序，其中規定 管理人員必須確保在辭職批准後立即從相關ICT系統和/或設備註銷使用者帳□和授權」。用□Scott沒有註銷記錄。
IT 安全經理解釋□，Scott 是一位非常優秀的軟體工程師、前同事和朋友。
辭職後，他仍然每月回到辦公室提供原始碼維護支援。這就是為什麼他在 SCM 上的帳□仍然存在。
我們很了解 Scott，他在加入我們時通過了我們所有的背景調□。因此，我們認為沒有必要僅僅因為他現在是外部提供者而與他同意任何進一步的資訊安全要求」。
您準備審計結果。選出三個正確選項。
A. 存在不合格項 (NC)。斯科特應該被告知與他與療養院的新關係（外部提供者）相關的適用資訊安全要求。然而，IT 安全經理證實這並沒有發生。這不符合控制措施 A.5.20。
B. 存在不合格項 (NC)。該組織的存取控制安排未能有效運行，因為不再受該組織僱用的個人被允許訪問療養院的 ICT 系統。這不符合控制措施 A.5.15。
C. 存在不合格項 (NC)。IT 安全經理未確保 Scott 的使用者帳□已從 SCM 中刪除，且在離職後未完成使用者登出流程。
這不符合第 9.1 條和控制措施 A.5.15。
D. 存在不合格項 (NC)。操作程序沒有很好的記錄。這使得 SCM 系統管理員無法立即刪除使用者帳□。這不符合第 9.1 條和控制措施 A.5.37。
E. 存在不合格項 (NC)。該組織沒有記錄程序來規定如何使用系統工具來提供原始程式碼的存取和版本控制。這不符合第 9.1 條和控制措施 A.8.4。
F. 存在不合格項 (NC)。該組織未能識別與斯科特的帳□保持開放相關的安全風險，因為他每月只重新使用很短一段時間。這不符合第 8.2 條的規定。
G. 存在不合格項 (NC)。SCM是開源系統軟體。它不安全，不能用於原始碼的存取和版本控制。這不符合第 9.1 條和控制措施 A.8.4。
H. 存在不合格項 (NC)。SCM 將自動記錄原始碼簽入/簽出活動。如果出現問題，團隊可能無法追蹤。這不符合第 9.1 條和控制措施 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: 126
當 IT 經理找到您並請您協助修改公司的風險管理流程時，您剛完成了組織的預定資訊安全審核。他正在嘗試更新當前的文檔，以使其他經理更容易理解，但是，從您的討論中可以清楚地看出，他混淆了幾個關鍵術語。
您要求他將每個描述與適當的風險術語相匹配。正確答案應該是什麼？

Answer:

Explanation:

The correct answers for matching each of the descriptions with the appropriate risk term are:

* The strategy chosen to respond to a specific information security risk: This is a definition of information security risk treatment. According to ISO/IEC 27000:2022, information security risk treatment is "the process of selecting and implementing measures to modify the information security risk" Section 3.33.
* The effect of uncertainty on information security objectives: This is a definition of information security risk. According to ISO/IEC 27000:2022, information security risk is "the effect of uncertainty on information security objectives" Section 3.32.
* The requirements against which information security risks are evaluated: This is a definition of information security risk criteria. According to ISO/IEC 27000:2022, information security risk criteria are "the terms of reference by which the significance of information security risks is assessed" Section
3.31.
* A definition of the overall level of information security risk that is considered to be tolerable: This is a definition of information security risk acceptance criteria. According to ISO/IEC 27000:2022,

information security risk acceptance criteria are "the level of information security risk that is acceptable" Section 3.30.

NEW QUESTION: 127
您是認證機構指派的 ISMS 審核小組組長，負責對資料中心客口進行後續審核
根據 ISO 19011:2018，後續審核的目的是要驗證下列哪一項？
A. 管理系統的有效性
B. ISMS 目標的實施
C. 風險處理計劃的實施
D. 糾正措施的完成情況和有效性
Answer: (SHOW ANSWER)
The purpose of a follow-up audit is to verify the completion and effectiveness of corrective actions taken by the auditee in response to the nonconformities identified in a previous audit1. A follow-up audit is a type of audit that is conducted after an initial audit, and it focuses on the specific areas where nonconformities were found and corrective actions were agreed upon2. A follow-up audit can be conducted as a separate audit or as part of a scheduled audit, depending on the nature and severity of the nonconformities and the audit programme objectives3.
The other options are not the purpose of a follow-up audit, but rather the purpose of other types of audits. For example:
*Option A is the purpose of a performance audit, which is a type of audit that evaluates the effectiveness of the management system in achieving its intended results4.
*Option B is the purpose of a compliance audit, which is a type of audit that verifies the conformity of the management system with the specified requirements, such as the ISMS objectives5.
*Option C is the purpose of a process audit, which is a type of audit that examines the inputs, activities, outputs, and interactions of a specific process within the management system, such as the risk treatment process.
References: 1: ISO 19011:2018, 6.7; 2: ISO 19011:2018, 3.7; 3: ISO 19011:2018, 5.5.2; 4: ISO 19011:2018,
3.6; 5: ISO 19011:2018, 3.5; : ISO 19011:2018, 3.4; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018;
: ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]

NEW QUESTION: 128
糾正措施」一詞是什麼意思？選擇一項
A. 採取措施防止不合格或事件發生
B. 採取措施消除不合格或事故的原因
C. 管理階層針對不合格項所採取的行動
D. 採取措施糾正不合格項或事件
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: 129
審核過程中，審核組長透過邏輯推理和分析，及時得出結論
審計組長表現出了哪些專業行為？
A. 決定性的
B. 思想開放
C. 道德
D. 有洞察力
Answer: A (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, one of the professional behaviours expected from an audit team leader is to be decisive, which means to "reach timely conclusions based on logical reasoning and analysis" (page 8). Being open minded, ethical, and perceptive are also desirable qualities for an audit team leader, but they do not match the description given in the question.
References: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 8.

NEW QUESTION: 130
您有一份客口設計文件的硬拷貝，想要處理掉。你會怎麼辦
A. 將其丟進任何垃圾箱
B. 使用粉碎機將其粉碎
C. 將其交給辦公室男孩以將其重新用於其他目的
D. 環境友善並且重複使用它來編寫
Answer: B (LEAVE A REPLY)
The best way to dispose of a hard copy of a customer design document is to shred it using a shredder. This is because shredding ensures that the document is destroyed and cannot be reconstructed or accessed by unauthorized persons. A customer design document may contain sensitive or confidential information that could cause harm or damage to the customer or the organization if disclosed. Therefore, it is important to protect the confidentiality and integrity of the document until it is securely disposed of. Throwing it in any dustbin, giving it to the office boy to reuse it for other purposes, or reusing it for writing are not secure ways of disposing of the document, as they could expose the document to unauthorized access, theft, loss or damage. ISO/IEC 27001:2022 requires the organization to implement procedures for the secure disposal of media containing information (see clause A.8.3.2). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Secure Disposal?

NEW QUESTION: 131
在發生資訊安全事件時，應遵守系統使用者的角色和責任，但以下情況除外：
A. 透過服務台發現後通報可疑或已知事件
B. 必要時保留證據
C. 如有需要，在調口期間與調口人員合作
D. 讓所有員工了解資訊安全事件詳細信息
Answer: (SHOW ANSWER)
The role and responsibility that system users should not observe in the event of an information security incident is D: make the information security incident details known to all employees. This is not a proper role or responsibility for system users, as it could cause unnecessary panic, confusion or speculation among employees who are not involved in the incident response process. It could also compromise the confidentiality and integrity of the incident information, which could be sensitive or confidential in nature. Making the information security incident details known to all employees could also violate the information security policies and procedures of the organization, which may require a certain level of discretion and confidentiality when dealing with incidents. The other roles and responsibilities are correct, as they describe what system users should do in the event of an information security incident, such as reporting the incident to the Servicedesk (A), preserving evidence if necessary (B), and cooperating with investigative personnel if needed
. These roles and responsibilities help to ensure a quick, effective and orderly response to information security incidents. ISO/IEC 27001:2022 requires the organization to implement procedures for reporting and managing information security incidents (see clause A.16.1).
References: CQI & IRCA Certified ISO/IEC
27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Information Security Incident Management?