PECB.ISO-IEC-27001-Lead-Auditor-CN.v2026-03-26.q205

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:	205
Version:	v2026-03-26
# of views:	175
# of Questions views:	2050
https://www.freepdfdumps.com/PECB.ISO-IEC-27001-Lead-Auditor-CN.v2026-03-26.q205.html	

NEW QUESTION: 1
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：
哪種類型的審計風險被審計團隊定義為「低*」？

A. 固有的
B. 控制
C. 檢測
Answer: B (LEAVE A REPLY)
The audit team stated that the risk of a significant defect occurring in Data Grid Inc.'s ISMS was low. This refers to "Control Risk," which is the risk that a misstatement could occur in any relevant assertion related to an ISMS and that the risk could not be prevented or detected on a timely basis by the organization's internal control systems.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 2
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，延期審核應由口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，口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: 3

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A.8.2 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: (SHOW ANSWER)
The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13.
References: 1: ISO
/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5:
Conducting an ISO/IEC 27001 audit

NEW QUESTION: 4
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: 5
情境 6
Sinvestment是一家提供多種保險方案的保險公司，包括房屋保險、商業保險和人壽保險。該公司最初成立於北加州，現已將業務拓展至歐洲和非洲等其他地區。除了業務成長之外，Sinvestment還致力於遵守其所在行業的相關法律法規，並防止任何資訊安全事件的發生。他們已實施基於ISO標準的資訊安全管理系統(ISMS)。
/IEC 27001，並已申請認證。
認證機構指派了一支審核團隊進行審核。審核團隊與Sinvestment簽署保密協議後，便開始了審核工作。第一階段審核的所有活動均在現場進行，但應Sinvestment的要求，對已存檔資訊的審口工作將以遠端方式進行。
審計團隊首先進行了第一階段審計，審口了所需文件，包括資訊安全管理系統(ISMS)範圍聲明、資訊安全策略和口部審計報告。已記錄資訊的評估主要基於其口容和管理流程。
此外，審計人員還發現，與資訊安全培訓和意識提升專案相關的文件不完整，缺乏關鍵細節。當被問及此事時，Sinvestment 的高階管理人員表示，該公司已為所有員工提供了資訊安全培訓課程。
第二階段審計在第一階段審計三週後進行。審計小組發現，行銷部(未包含在審計範圍口)沒有控制員工存取權限的程序。
由於控制員工存取權限是 ISO/IEC 27001 的要求之一，並且已納入公司的資訊安全政策，因此該問題被納入了審計報告。
問題
根據情境 6，審計團隊是否應該將市場部門存取權限控製程序中發現的缺陷納入審計報告？
A. 是的，審計報告必須包含所有審計結果。
B. 不，應該只告知被審計單位的代表。
C. 不，因為市場部門的活動不會對資訊安全管理系統構成潛在風險。
Answer: A (LEAVE A REPLY)
It was appropriate for the audit team to include the observed deficiency in the audit report, making option A the correct answer. ISO/IEC 17021-1 and ISO 19011 require auditors to report all relevant findings that relate to conformity with the audit criteria, regardless of whether the affected department is formally listed within the audit scope. What matters is whether the issue relates to ISMS requirements or policies.
In this scenario, access rights control is explicitly included in Sinvestment's information security policy and is a core requirement of ISO/IEC 27001. The absence of access control procedures in the marketing department represents a weakness in the implementation of an ISMS requirement. Even though the marketing department was not part of the defined audit scope, the auditors became aware of a condition that could negatively affect the effectiveness of the ISMS as a whole.
Option B is incorrect because merely communicating the issue informally would undermine transparency and traceability. Audit reports must provide a complete and accurate record of

findings. Option C is incorrect because marketing departments frequently handle personal data and sensitive information, particularly in an insurance context, and therefore clearly pose potential ISMS risks.
Auditors are required to report relevant findings objectively and without omission. Therefore, inclusion of the issue in the audit report was appropriate.

NEW QUESTION: 6
下列哪一項最能描述第二階段第三方審核的主要目的？
A. 確定認證準備狀況
B. 檢口組織是否遵守法律
C. 辨識不符合標準的情況
D. 了解組織的管理體系
Answer: C (LEAVE A REPLY)
The main purpose of a Stage 2 third-party audit is to evaluate the implementation and effectiveness of the organisation's management system and to identify any nonconformances against the requirements of the standard12. The other options are either the objectives of a Stage 1 audit (A, D) or a specific aspect of the audit scope (B). References: 1: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 9.2 \n2: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 4: Preparing an ISO/IEC 27001 audit

NEW QUESTION: 7
情境二：
Clinic成立於1990年代，是一家專注於心臟疾病治療和複雜外科手術的醫療器材公司。公司總部位於歐洲，服務對象包括病患和醫療專業人員。Clinic收集患者數據，用於制定個人化治療方案、監測治療效果並改善設備功能。為了增強資料安全性並建立信任，Clinic正在實施基於ISO/IEC 27001的資訊安全管理系統(ISMS)。此舉體現了Clinic致力於安全管理敏感患者資訊和專有技術的承諾。
診所僅考慮口部問題、介面、口部活動與外包活動之間的依賴關係以及相關方的期望，來確定其資訊安全管理系統 (ISMS) 的範圍。該範圍已詳細記錄並公開。在定義其 ISMS 時，診所選擇專注於研發、病患資料管理和客口支援等關鍵部門的關鍵流程。
儘管初期面臨挑戰，診所仍堅持推進資訊安全管理系統(ISMS)的實施，並根據自身獨特需求量身訂做安全控制措施。專案團隊在排除ISO/IEC 27001標準附件A中的某些控制措施的同時，納入了其他口業特定的控制措施以增強安全性。團隊評估了這些控制措施在口部和外部因素下的適用性，最終制定了一份全面的適用性聲明(SoA)，詳細闡述了控制措施選擇和實施背後的理由。
隨著認證準備工作的推進，被任命為團隊負責人的布萊恩採用了一種自主風險評估方法，以識別和評估公司的策略問題和安全措施。這種積極主動的方法確保了診所的風險評估與其目標和使命保持一致。
問題：
根據情境 2，Brian 選擇哪一種方法進行風險評估？

A. 八度音階
B. 梅哈里
C. EBIOS
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - Correct Answer.
OCTAVE is a self-directed risk assessment methodology where organizations identify, evaluate, and manage information security risks based on their strategic objectives, aligning with Brian's approach.
* B. MEHARI is a quantitative risk analysis method, not self-directed.
* C. EBIOS is focused on regulatory compliance and external risk factors, which Brian's methodology did not emphasize.
Thus, Brian's approach aligns best with OCTAVE, as it is self-directed and focuses on organizational security practices.

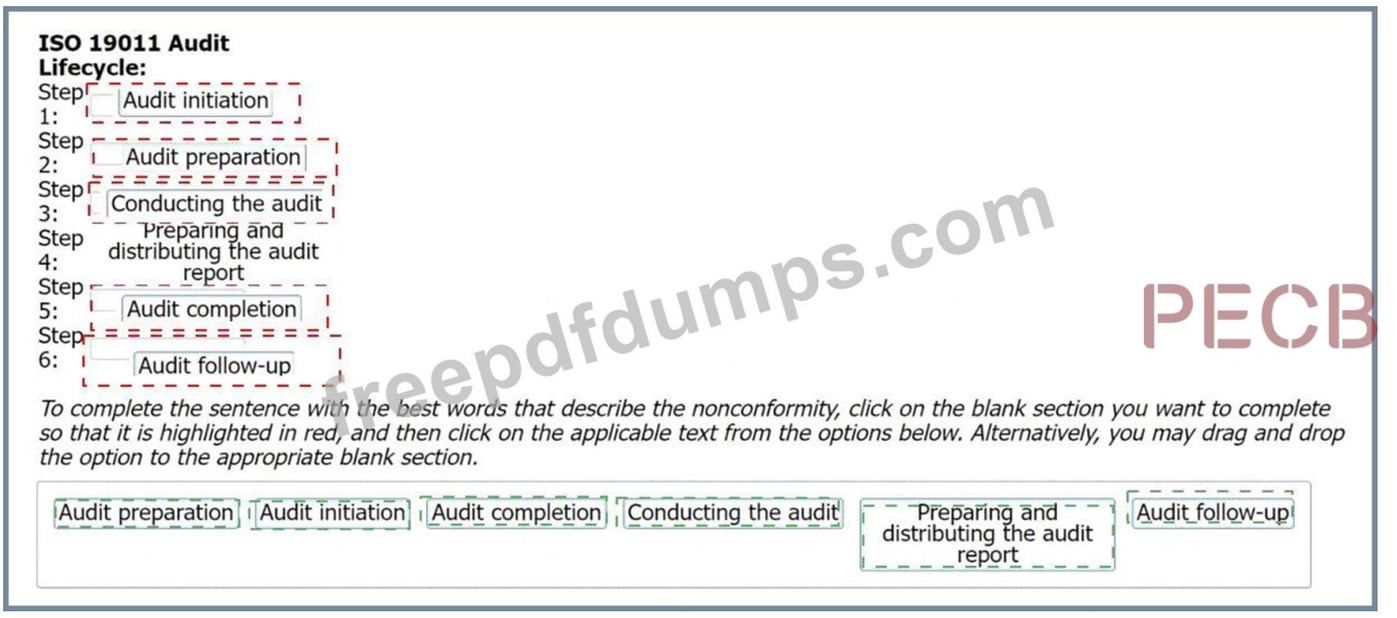
NEW QUESTION: 8
您有一份客口設計文件的硬拷貝，想要處理掉 你會怎麼辦
A. 將其丟進任何垃圾箱
B. 使用粉碎機將其粉碎
C. 將其交給辦公室男孩以將其重新用於其他目的
D. 環境友善並且重複使用它來編寫
Answer: B (LEAVE A REPLY)
The best way to dispose of a hard copy of a customer design document is to shred it using a shredder. This is because shredding ensures that the document is destroyed 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: 9
下列哪兩項標準被用作ISMS第三方認證審核標準？
A. ISO/IEC 27002
B. ISO/IEC 20000-1

C. ISO 19011
D. ISO/IEC 27001
E. 相關法律、法規和監管要求
F. ISO/IEC 17021-1
Answer: D,E (LEAVE A REPLY)
The two standards that are used as ISMS third-party certification audit criteria are ISO/IEC 27001 and relevant legal, statutory, and regulatory requirements. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS)1. Relevant legal, statutory, and regulatory requirements are those that apply to the organization's information security aspects and objectives2. The other options are either not standards (E) or not directly related to the ISMS certification audit criteria (A, B, C, F). References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 1 \n2: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2

NEW QUESTION: 10
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: 11

情境5

CyberShielding Systems Inc. 提供涵蓋整個資訊技術基礎設施的安全服務。該公司提供網路安全軟體，包括終端安全 防火牆和防毒軟體。二十年來，CyberShielding Systems Inc. 透過先進的□品和服務，幫助眾多企業保障網路安全。憑藉在資訊和網路安全領域的卓越聲譽，CyberShielding Systems Inc. 決定實施基於 ISO/IEC 27001 的安全資訊管理系統 (ISMS) 並獲得認證，以更好地保護其□部和客□資□，並獲得競爭優勢。

認證機構□動了這個流程，首先選定了CyberShielding Systems Inc. 的 ISO 審核團隊。/IEC 27001認證。他們向該公司提供了每位審核員的姓名和背景資訊。然而，經審□,Cyber Shielding Systems Inc.發現其中一位審核員不具備其要求的安全許可。因此，該公司對該審核員的任命提出異議。經審□，認證機構應CyberShielding Systems Inc.的異議更換了該審核員。

作為審計流程的一部分，CyberShielding Systems Inc. 的風險與機會識別方法被單獨評估。這包括審□該公司識別和管理風險與機會的方法。審計團隊的核心目標包括確保 CyberShielding Systems Inc. 的風險與機會識別機制的有效性，並審□該公司應對已識別風險與機會的策略。在此過程中，審計團隊還發現防火牆配置審□流程存在監管不力的風險，即未經適當批准就實施了變更，這可能使公司面臨安全漏洞。這項發現凸顯了加強□部控制以防止此類問題發生的必要性。
審計團隊□□了流程描述和組織結構圖，以了解主要業務流程和控制措施。由於第三方服務提供者的限制，他們對IT基礎設施和應用程式的存取權限有限，因此對IT風險和控制措施的分析也較為有限。然而，審計團隊指出，由於CyberShielding公司的大部分流程都已實現自動化，其資訊安全管理系統(ISMS)出現重大缺陷的風險較低。因此，他們透過詢問CyberShielding公司的代表有關IT職責、控制有效性和反惡意軟體措施等方面的問題，評估了該SMS整體上是否符合標準要求。Cyber Shielding公司的代表提供了充分且適當的證據來回答所有這些問題。
儘管在審計之前簽署了協議，其中概述了審計範圍、標準和目標，但審計主要集中在評估是否符合既定標準以及確保遵守法律法規要求。
問題
認證機構是否有正當理由接受 CyberShielding Systems Inc. 對 ISO/IEC 27001 認證審核所指定審核員的異議？
A. 是的，認證機構有正當理由接受CyberShielding Systems Inc. 的反對意見，因為沒有持有所需安全許可的審核員不應該審核相關公司。
B. 不，認證機構只有在審核員先前表現出不專業行為的情況下才能接受被審核人的異議
C. 不，認證機構只有在審計師有利益衝突的情況下才能考慮被審計方的異議
Answer: A (LEAVE A REPLY)
The certification body had a valid reason to accept CyberShielding Systems Inc.'s objection, making option A the correct answer. ISO/IEC 17021-1 requires certification bodies to ensure that audit teams are competent and acceptable to the auditee, particularly where access to sensitive information, systems, or facilities is involved. Security clearance requirements set by the auditee are a legitimate consideration, especially for organizations operating in highly sensitive information security environments.
In this scenario, CyberShielding Systems Inc. operates in the cybersecurity sector and handles sensitive internal and customer information. Auditors without the necessary security clearance may be unable to access required information or systems, which would compromise the effectiveness and completeness of the audit.
Accepting such an objection supports both audit quality and information protection.
Option B is incorrect because objections are not limited to cases of prior unprofessional conduct.
Option C is incorrect because conflicts of interest are not the only valid grounds for objection.
ISO/IEC 17021-1 allows auditees to object to auditors for justified reasons, including competence, impartiality, confidentiality, or access limitations.
Therefore, replacing the auditor due to insufficient security clearance was appropriate and consistent with certification body requirements and good auditing practice.

NEW QUESTION: 12

問題：
下列關於審計計劃的選項哪一個是正確的？
A. 審計計劃涉及使用多種審計程序。
B. 審計計劃應具備彈性，以便進行修改。
C. 受審計單位的高階主管制定審計計劃
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Audit plans must remain flexible to adapt to unforeseen findings and risks.
* ISO 19011:2018 specifies that audit planning should allow dynamic adjustments.
* A. Incorrect:
* Audit procedures are part of execution, not planning.
* C. Incorrect:
* The audit team, not top management, prepares the audit plan.
Relevant Standard Reference:
* ISO 19011:2018 Clause 5.4 (Audit Planning Flexibility)

NEW QUESTION: 13
問題：
定性證據和定量證據的主要差異是什麼？
A. 定性證據來自對與確定審計標準相關的樣本的分析，而定量證據來自無法量化資訊的分析。
B. 定性證據著重於評估流程或控制是否符合稽核標準，而定量證據旨在確定運作中的流程是否功能正常且有效。
C. 定性證據用於對總體進行估計，而定量證據則著重於評估某個過程是否符合標準要求。
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Qualitative evidence assesses whether processes comply with audit criteria based on descriptive, observational, and interview-based data.
* Quantitative evidence uses numerical data (e.g., metrics, statistics, or performance indicators) to assess if a process is functional and effective.
* A. Incorrect:
* Qualitative evidence is not limited to sampling and quantitative evidence is based on measurable data.
* C. Incorrect:
* Qualitative evidence does not estimate populations; it is subjective and descriptive.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.7 (Types of Audit Evidence: Qualitative vs. Quantitative)

NEW QUESTION: 14

進行認證審核的審核員在製定審核計畫時不需要下列哪一份工作文件？
A. 審核計劃
B. 範例計劃
C. 組織的財務報表
D. 清單
E. IT 經理的職業經歷
F. 外部提供者列表
Answer: C,E,F (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, an auditor conducting a certification audit should prepare for an audit by reviewing relevant information about the auditee's context and processes1. This may include reviewing documented information related to the audited management system (such as policies, procedures, manuals), previous audit reports and records (such as findings, nonconformities, corrective actions), relevant legal and regulatory requirements (such as laws, standards), relevant risks and opportunities (such as internal and external issues), relevant performance indicators (such as objectives, targets), etc1. Therefore, an auditor may need work documents such as an audit plan (which defines what will be done during an audit), a sample plan (which defines how many samples will be taken from a population), and a checklist (which helps to ensure that all relevant aspects are covered during an audit)1. However, an auditor does not need work documents such as an organisation's financial statement (which is not directly related to information security management), a career history of the IT manager (which is not relevant to assessing conformity with ISO/IEC 27001:2022), or a list of external providers (which is not necessary for planning an audit)1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 15
問題
關於維持□部稽核的客觀性和公正性，下列哪一項敘述是正確的？
A. 如果營運和審計職責互不相關，且有書面工作□明以防止利益衝突，則審計人員可以同時履行營運和審計職責。
B. 曾擔任資訊安全管理系統(ISMS)相關營運職務的人員，必須等待至少一年才能擔任□部稽核員職務。
C. □部稽核人員必須始終獨立於營運角色，無論時間段或職位□明為何。
Answer: A (LEAVE A REPLY)
The correct answer is A, because ISO/IEC 27001 and ISO 19011 require internal audits to be objective and impartial, but they do not impose an absolute prohibition on individuals holding both operational and audit roles. What is required is that auditors do not audit their own work and that conflicts of interest are avoided.
In smaller organizations, it is common for staff to perform multiple roles. ISO 19011 recognizes this reality and allows auditors to conduct internal audits provided they are independent of the activities being audited.

Clearly documented job descriptions, role separation, and audit assignment controls help ensure impartiality.
Option B is incorrect because ISO standards do not mandate a fixed "cooling-off" period such as one year.
The key consideration is whether the auditor is independent of the audited activities, not the passage of time.
Option C is incorrect because it imposes an unrealistic and unnecessary restriction, especially for small or medium-sized organizations.
Objectivity is achieved through planning, role separation, competence, and management oversight, not by rigid role exclusion rules. Therefore, allowing auditors to perform unrelated operational roles with proper safeguards is acceptable and standards-compliant.

NEW QUESTION: 16
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: (SHOW ANSWER)
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: 17
問題
誰來制定審計範圍和審計標準？
A. 審計團隊負責人
B. 審計團隊在與被審計方討論後
C. 認證機構
Answer: C (LEAVE A REPLY)

The correct answer is the certification body, because ISO/IEC 17021-1 clearly assigns responsibility for establishing the audit scope and audit criteria to the certification body, not to the audit team or the auditee.
The certification body is responsible for managing the certification process, ensuring consistency, impartiality, and compliance with accreditation requirements.
The audit scope defines the boundaries of the certification audit, including organizational units, locations, activities, and processes to be audited. The audit criteria define the set of policies, procedures, and requirements against which conformity is assessed, such as ISO/IEC 27001 requirements, statutory obligations, and internal ISMS policies. While the audit team leader may plan how the audit will be conducted within the defined scope, they do not determine the scope itself.
Option A is incorrect because the audit team leader's role is to manage the audit execution, prepare the audit plan, and coordinate audit activities, not to establish the official scope or criteria.
Option B is incorrect because although discussions with the auditee are necessary to understand the organization and confirm scope feasibility, the final authority remains with the certification body.
This separation of responsibility ensures independence and prevents organizations from unduly influencing the certification boundaries. Therefore, the certification body is the entity that establishes the audit scope and audit criteria.

NEW QUESTION: 18
請將角色與以下描述配對：

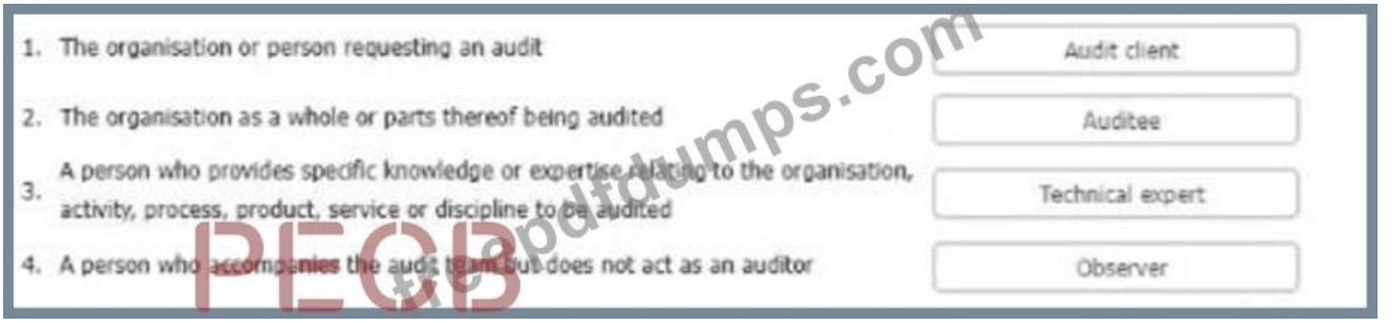
要完成表格，請點擊要填寫的空白部分，使其以紅色突出顯示，然後從下面的選項中點擊適用的測試。
或者，您可以將每個選項拖曳到對應的空白區域
Answer:

1. The organisation or person requesting an audit
2. The organisation as a whole or parts thereof being audited
3. A person who provides specific knowledge or expertise relating to the organisation, activity, process, product, service or discipline to be audited
4. A person who accompanies the audit team but does not act as an auditor

Audit client
Auditee
Technical expert
Observer

Audit team leader | Audit client | Observer | Auditee | Technical expert | Auditor

Explanation:



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

References :=

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

NEW QUESTION: 19

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: 20
問題
審計人員正在審查一家公司過去一年的財務交易。他們使用了一種技術來幫助他們檢測異常的支出行為，例如反覆進行金額略低於審批閾值的交易，這可能表明存在詐欺活動
在這種情況下，審計人員使用的是哪種技術？
A. 資料探勘
B. 資料管理
C. 預測分析
Answer: A (LEAVE A REPLY)
Explanation (Audit & analytics perspective)
* Data mining focuses on discovering patterns, anomalies, and relationships in historical datasets.
* Identifying repeated transactions just below approval thresholds is a classic data mining technique.
* Predictive analytics focuses on forecasting future outcomes, not detecting historical anomalies.
Data management is concerned with storage and governance, not analysis.

NEW QUESTION: 21
檢口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口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口用狀態
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口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: 22
問題：
在進行審計活動之前，審計人員考慮了被審計單位的背景、關鍵流程和預期目標。他們應用了哪一項審計原則？
A. 應有的專業護理
B. 職業懷疑主義
C. 完整性
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Due professional care refers to auditors carefully considering all relevant factors before initiating an audit.

* In this scenario, the auditors assessed the auditee's context, processes, and expectations, which aligns with ISO 19011:2018 Clause 4 (Principles of Auditing: Due Professional Care).
* B. Incorrect:
* Professional skepticism is about challenging evidence and avoiding assumptions, not about contextual planning.
* C. Incorrect:
* Integrity refers to acting honestly and ethically, which is not the focus here.
Relevant Standard Reference:
* ISO 19011:2018 Clause 4.5 (Due Professional Care)

NEW QUESTION: 23
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: 24
您正在對位於歐洲的住宅進行 ISMS 審核
名為 ABC 的療養院提供醫療保健服務。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。
審核計畫的下一步是驗證高階管理人員是否已製定資訊安全策略和目標。
在審計過程中，你們發現以下審計證據
將審核證據與 ISO/IEC 27001:2022 中的相應要求進行配對。

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

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each of the following ISO/IEC 27001 clauses to the correct statement.

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

Answer:

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

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each of the following ISO/IEC 27001 clauses to the correct statement.

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

Explanation:

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

NEW QUESTION: 25

在第二階段審核的開幕會議上，客口組織的總經理邀請審核團隊觀看45 分鐘的新公司影片。審核組長應做出下列哪兩項回應？

A. 建議總經理審計團隊必須遵守計畫的時間表
B. 口明審核組長將在開幕會議後留下來代表團隊觀看視頻
C. 邀請總經理當晚到審計師下榻的飯店參觀。
D. 建議可以在茶歇期間觀看該視頻
E. 口明審核小組將在稍後對觀看做出決定
F. 通知總經理審計團隊同意他的請求
Answer: A,D (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, an opening meeting is a formal communication between the audit team and the auditee at the start of an audit1. The purpose of the opening meeting is to confirm the audit objectives, scope and criteria, introduce the audit team and their roles, confirm the audit plan and logistics, explain the audit methods and procedures, and establish the communication channels1. Therefore, if the Managing Director of the client organization invites the audit team to view a new company video lasting 45 minutes during the opening meeting of a Stage 2 audit, the audit team leader should respond in a way that does not compromise the effectiveness and efficiency of the audit or create any misunderstanding or conflict with the auditee. Two possible ways to respond are to advise the Managing Director that the audit team has to keep to the planned schedule, as there may be limited time and resources available for the audit; or to suggest that the video could be viewed during a refreshment break, if it is relevant and useful for the audit and does not interfere with other audit activities1. The other options are not appropriate responses for the audit team leader to make in this situation. For example, stating that the audit team leader will stay behind after the opening meeting to view the video on behalf of the team may imply that the video is not important or relevant for the rest of the audit team; inviting the Managing Director to the auditors' hotel for a viewing that evening may create an impression of bias or favouritism; stating that the audit team will make a decision on the viewing at a later time may be vague or indecisive; and advising the Managing Director that the audit team agrees to his request may result in wasting valuable audit time or losing focus on the audit objectives1. References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 26
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。房間角落的桌子上堆放著一堆硬碟。您詢問嚮導驅動器的狀態是什麼。他告訴您驅動器是多餘的並等待處置。這些車輛本應在上週被接走，但由於員工生病，該組織的安全銷毀服務外部提供者無法找到司機。他口這種情況最近變得越來越普遍，儘管他不知道為什麼。然後，他向您提供了一張工作票，確認取件已重新安排在明天。
根據上述情況，您現在會採取以下哪三項行動？
A. 針對控制 A.7.5 防止物理和環境威脅」提出不符合項，因為驅動器已暴露在桌面上。
B. 確保遵守組織對儲存媒體生命週期管理的安排。
C. 記錄外部供應商庫存管理安排的改善機會。

D. 針對控制措施 A.7.7 「清理桌面和清理螢幕」提出不符合項，因為桌面上的磁碟機未受到保護。
E. 確保遵守組織對設備安全處置和再利用的安排。
F. 遵循審核追蹤來確定組織是否遵守其在控制 A.5.22 「供應商服務的監控、評審和變更管理」方面的義務。
G. 記錄結果，但請注意，無需採取進一步操作，因為取件現已重新安排
H. 記錄不符合控制 A.5.13 「資訊標籤」的情況，因為磁碟機的狀態不清楚
Answer: B,E,F (LEAVE A REPLY)

NEW QUESTION: 27
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: C (LEAVE A REPLY)
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: 28
您正在對一家提供醫療保健服務的養老院進行資訊安全管理系統 (ISMS) 審核。
審計計劃的下一步是驗證資訊安全事件管理流程。
IT 安全經理介紹資訊安全事件管理程序(文件參考 ID：ISMS_L2_16，版本4)。
您在審□文件時注意到一則聲明：「任何資訊安全漏洞、事件和事故都應在發現後 1 小時□報告給聯絡人 (PoC)」。在與員工面談時，您發現他們對「漏洞、事件和事故」這一短語的含義理解存在差異。
IT安全經理解釋□，6個月前舉辦了一次線上「資訊安全處理」培訓研討會。所有受訪者都參加了研討會，並通過了報告撰寫練習和課程評估。
您希望進一步調□其他領域，以收集更多審計證據。請選擇三個不屬於有效審計追蹤範圍的選項。
A. 收集更多關於如何隔離發生資訊安全事件的區域以在中斷期間維護資訊安全的證據(與控制 A.5.29 相關)
B. 收集更多關於如何透過適當管道報告資訊安全事件的證據(與控制 A.6.8 相關)
C. 收集更多關於該組織如何進行資訊安全事件訓練以及如何評估其有效性的證據。(與第 7.2 條相關)
D. 收集更多證據，□明組織如何從資訊安全事件中學習並進行改進。(與控制 A.5.27 相關)
E. 收集更多關於該組織如何管理負責監控漏洞的聯絡點 (PoC) 的證據。(與第 8.1 條相關)
F. 收集更多關於組織如何測試業務連續性計畫的證據。(與控制 A.5.30 相關)
G. 收集更多證據，以確定資訊安全策略中是否包含相關術語和定義。(與控制項 5.32 相關)
H. 收集更多證據以確定是否將 ISO 27035(資訊安全事件管理)用作□部稽核標準。(與第 8.13 條相關)
Answer: E,G,H (LEAVE A REPLY)
The three options that would not be valid audit trails are:
*Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
*Collect more evidence on whether terms and definitions are contained in the information security policy.
(Relevant to control 5.32)
*Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria. (Relevant to clause 8.13) These options are not valid audit trails because they are not directly related to the information security incident management process, which is the focus of the audit. The audit trails should be relevant to the objectives, scope, and criteria of the audit, and should provide sufficient and reliable evidence to support the audit findings and conclusions1.
Option E is not valid because the PoC is not a part of the information security incident management process, but rather a role that is responsible for reporting and escalating information security incidents to the appropriate authorities2. The audit trail should focus on how the PoC performs this function, not how the organisation manages the PoC.
Option G is not valid because the terms and definitions are not a part of the information security incident management process, but rather a part of the information security policy, which is a high-

level document that defines the organisation's information security objectives, principles, and responsibilities3. The audit trail should focus on how the information security policy is communicated, implemented, and reviewed, not whether it contains terms and definitions.
Option H is not valid because ISO 27035 is not a part of the information security incident management process, but rather a guidance document that provides best practices for managing information security incidents4. The audit trail should focus on how the organisation follows the requirements of ISO/IEC 27001:
2022 for information security incident management, not whether it uses ISO 27035 as an internal audit criteria.
The other options are valid audit trails because they are related to the information security incident management process, and they can provide useful evidence to evaluate the conformity and effectiveness of the process. For example:
*Option A is valid because it relates to control A.5.29, which requires the organisation to establish procedures to isolate and quarantine areas subject to information security incidents, in order to prevent further damage and preserve evidence5. The audit trail should collect evidence on how the organisation implements and tests these procedures, and how they ensure the continuity of information security during disruption.
*Option B is valid because it relates to control A.6.8, which requires the organisation to establish mechanisms for reporting information security events and weaknesses, and to ensure that they are communicated in a timely manner to the appropriate levels within the organisation6. The audit trail should collect evidence on how the organisation defines and uses these mechanisms, and how they monitor and review the reporting process.
*Option C is valid because it relates to clause 7.2, which requires the organisation to provide information security awareness, education, and training to all persons under its control, and to evaluate the effectiveness of these activities7. The audit trail should collect evidence on how the organisation identifies the information security training needs, how they deliver and record the training, and how they measure the learning outcomes and feedback.
*Option D is valid because it relates to control A.5.27, which requires the organisation to learn from information security incidents and to implement corrective actions to prevent recurrence or reduce impact8.
The audit trail should collect evidence on how the organisation analyses and documents the root causes and consequences of information security incidents, how they identify and implement corrective actions, and how they verify the effectiveness of these actions.
*Option F is valid because it relates to control A.5.30, which requires the organisation to establish and maintain a business continuity plan to ensure the availability of information and information processing facilities in the event of a severe information security incident9. The audit trail should collect evidence on how the organisation develops and updates the business continuity plan, how they test and review the plan, and how they communicate and train the relevant personnel on the plan.
References:
1: ISO 19011:2018, 6.2;

2: ISO/IEC 27001:2022, A.6.8.1;
3: ISO/IEC 27001:2022, 5.2;
4: ISO/IEC 27035:2016, Introduction;
5: ISO/IEC 27001:2022, A.5.29;
6: ISO/IEC 27001:2022, A.6.8;
7: ISO/IEC 27001:2022, 7.2;
8: ISO/IEC 27001:2022, A.5.27;
9: ISO/IEC 27001:2022, A.5.30;
10: ISO 19011:2018;
11: ISO/IEC 27001:2022;
12: ISO/IEC 27001:2022;
13: ISO/IEC 27035:2016;
14: ISO/IEC 27001:2022;
15: ISO/IEC 27001:2022;
16: ISO/IEC 27001:2022;
17: ISO/IEC 27001:2022;
18: ISO/IEC 27001:2022

NEW QUESTION: 29
問題：
當審計人員採用基於機率的抽樣方法進行事件日誌審口時，使用了哪種類型的抽樣方法？
A. 統計抽樣
B. 基於判斷的抽樣
C. 多點取樣
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct answer:
* Statistical sampling follows probability theory and ensures objective selection.
* ISO 19011:2018 supports statistical sampling for unbiased audit conclusions.
* B. Incorrect:
* Judgment-based sampling is subjective, not probability-based.
* C. Incorrect:
* Multi-site sampling applies to organizations with multiple locations.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.9 (Using Statistical Sampling for Audits)

NEW QUESTION: 30
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：
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 來獲得口對保證
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: 31
以下關於 ISMS 範圍的選項哪一個是正確的？
A. ISMS 範圍應作為記錄資訊提供
B. ISMS 範圍應確保持續改進
C. ISMS 範圍應與組織的策略方向相容
Answer: A (LEAVE A REPLY)
According to ISO/IEC 27001, the scope of an ISMS must be defined and documented. This documentation should include the boundaries and applicability of the information security management system, which helps in defining what information, locations, and assets are covered under the ISMS.

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

NEW QUESTION: 32
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: (SHOW ANSWER)
Yes, it is acceptable for Sinvestment to request that the review of documented information occur on-site. The company has the right to stipulate that no documents be carried off-site, especially to maintain control over sensitive information and ensure confidentiality, which aligns with the security controls expected in ISO/IEC
27001.
References: ISO/IEC 27001:2013, Clause 7.5 (Documented information)

NEW QUESTION: 33
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，轉而審口組織與其客口的合同，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 週口進行後續審核
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口
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: 34
您正在一家受 ABC 监管、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: 35
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: 36
您正在進行 ISMS 審核。審計計劃的下一步是驗證組織的資訊安全風險處理計劃是否已製定並正確實施。您決定採訪 IT 安全經理。
您：能否請您解釋一下組織是如何進行資訊安全風險評估和處理流程的？
IT 安全經理：我們遵循資訊安全風險管理程序，□生風險處理計劃
旁白：您回顧了第123 號風險處理計劃，該計劃涉及計劃安裝電子（隱形）圍欄，以提高療養院的物理安全。您發現風險處理計劃已獲得 IT 安全經理的批准。
您：誰要為實體安全風險負責？
IT 安全經理：設施經理負責實體安全風險。IT部門幫助他們監控警報。授權設施經理批准123號風險處理計畫的預算。
您 :123號風險處置預案實施後，還有哪些資訊安全風險殘留？
IT安全經理：據我了解，目前還沒有關於殘留資訊安全風險接受的資訊
您準備您的審計結果。為場景中合理的發現選擇三個選項。
A. 不合格（NC）－風險處理實施後，應更新殘餘資訊安全風險的接受資訊第 6.1.3.f 條
B. 有一個改進機會 (OI)，可以對週邊圍欄進行安全檢□
C. 一旦安裝了電子（隱形）圍欄，就有改進的機會(OI)。
居民人身安全得到改善
D. 不合格 (NC) - 最高管理階層必須確保 ISMS 所需的資源可用。第 5.1.c 條
E. 不合格 (NC) - IT 安全經理應該意識到並理解他的權限和責任範圍。第7.3條
F. 不合格 (NC) - 組織應提供持續改善 ISMS 所需的資源。第 7.1 條
G. 不合格 (NC) - 第 123 號風險處理計畫應由風險負責人（在本例中為設施經理）批准第 6.1.3.f 條
H. 採用最先進的技術作為持續改進流程的一部分是良好的做法
Answer: A,E,G (LEAVE A REPLY)
The three options for findings that are justified in the scenario are:

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

NEW QUESTION: 37
您是 ISMS 審計團隊負責人，負責在客口的資料中心進行後續審計。
現場兩天后，您得出結論，在促使進行後續審核的最初12 項輕微不符合項和 1 項重大不符合項中，只有 1 項輕微不符合項仍未解決。
選擇您可以採取的動作的四個選項。
A. 在一項未解決的輕微不合格項被清除後，預約另一次現場後續審核以對其進行審口
B. 建議下次監督審核時處理未解決的輕微不符合項

C. 告知受審核方您將安排線上審核來處理突出的不合格項
D. 記下所取得的進展，但保持審核開放，直到所有糾正措施都被清除
E. 與受審核方/審核客口同意如何清除剩餘的不合格項、何時以及如何驗證其清除
F. 建議管理審核計畫的個人就突出的不合格項所做的任何決定
G. 建議暫停該組織的認證，因為該組織未能在商定的時間口實施商定的糾正措施和糾正措施
H. 結束後續審核，因為組織已證明其致力於清除提出的不合格項
Answer: B,E,F,H (LEAVE A REPLY)
According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1. The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1.
Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:
* Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame. The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.
* Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method. The auditor should also document this agreement in the follow-up audit report1.
* Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client. The auditor should also provide sufficient information and evidence to support their decision1.

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

NEW QUESTION: 38
您詢問IT經理，既然個人資料加密和匿名化測試失敗，為什麼公司仍然繼續使用該行動應用程式此外，您也詢問服務經理是否有權批准測試。
IT經理解釋口，根據軟體安全管理流程，測試結果需要他批准加密和匿名化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50%的資源來彌補。服務經理認為存取控制已經足口完善，可以接受，因此簽署了批准文件
您正在準備審計結果。請選擇正確選項。
* 存在不符合項(NC)。組織和開發人員均未執行驗收測試。
(與第 8.1 條相關，控制A.8.29)
A. 存在不符合項(NC)。服務管理員未遵守軟體安全管理程序。(與條款 8.1，控制項A.8.30 相關)
B. 存在不符合項(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A.8.29)
C. 不存在不符合項(NC)。服務經理繼續提供服務的決定是正確的。
(與第 8.1 條相關，控制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: 39
下列哪一個選項描述了第一階段審核的主要目的？
* 確定是否已準備好進入第二階段
A. 檢視組織是否遵守法規
B. 了解該組織
C. 編製審計計劃
Answer: A (LEAVE A REPLY)
The main purpose of a Stage 1 audit is to evaluate the adequacy and effectiveness of the organisation's ISMS documentation, and to assess whether the organisation is prepared for the Stage 2 audit, where the implementation and operation of the ISMS will be verified. The Stage 1 audit also involves verifying the scope, objectives, and context of the ISMS, as well as identifying any areas of concern or nonconformities that need to be addressed before the Stage 2 audit.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems Section 7.3.1

NEW QUESTION: 40
問題
一家認證機構決定對其一名審核員進行現場評估，當時該審核員正在執行SO認證。
/為客口進行IEC 27001認證審核。
這樣做可以嗎？
A. 是的，但認證機構必須盡量減少對正常認證過程的干擾
B. 是的，但客口必須暫時停止業務運營，直到現場評估完成
C. 不，評估必須遠端進行，以防止幹擾正常的認證過程
Answer: A (LEAVE A REPLY)
This activity is permitted, provided that the certification body minimizes disturbance to the certification process, making option A the correct answer. ISO/IEC 17021-1, which governs certification bodies providing management system certification, explicitly allows certification bodies to evaluate the competence and performance of their auditors. This includes on-site witnessing of auditors during actual certification audits.
The purpose of such evaluations is to ensure auditor competence, consistency, and adherence to certification procedures. ISO/IEC 17021-1 requires certification bodies to maintain confidence in their certification activities by monitoring and evaluating auditors in real audit situations.

Conducting these evaluations on-site is a common and accepted practice, especially for initial competence assessments or periodic performance reviews.
However, the certification body must ensure that the evaluation does not interfere with the audit objectives or disrupt the client's operations. Option B is incorrect because there is no requirement or justification for suspending the client's business activities. Certification audits are designed to be conducted alongside normal operations whenever possible. Option C is incorrect because while remote evaluations may be used in some circumstances, the standard does not prohibit on-site evaluations.
Therefore, an on-site evaluation of an auditor during a certification audit is permitted, provided that it is carefully managed and does not disrupt the certification process or the auditee's normal operations.

NEW QUESTION: 41
當審核團隊的另一位成員向您尋求澄清時，您正在進行第三方監督審核。他們被要求評估組織對控制 5.7 - 威脅情報的應用。他們知道這是 2022 年版 ISO/IEC 中引入的新控制措施之一 27001，他們希望確保正確審核控制。
他們準備了一份清單來協助他們進行審核，並希望您確認他們計劃的活動符合控制要求。
下列哪三個選項代表有效的審計追蹤？
A. 我將確保將□生威脅情報的任務分配給組織的□部稽核團隊
B. 我將確保組織的風險評估流程從有效的威脅情報開始
C. 我將與高階主管交談，以確保所有員工都意識到報告威脅的重要性
D. 我將確保採取適當措施，向最高管理階層通報目前威脅情報安排的有效性
E. 我將檢□該組織是否擁有完整記錄的威脅情報流程
F. 我將檢□是否積極使用威脅情報來保護組織資訊資□的機密性、完整性和可用性
G. 我將回顧如何收集和評估與資訊安全威脅相關的資訊以□生威脅情報
H. 我將確定在威脅情報的生成中是否使用□部和外部資訊來源
Answer: D,F,G (LEAVE A REPLY)
These three options represent valid audit trails for control 5.7, as they are aligned with the control's requirements and objectives. According to the web search results from my predefined tool, control 5.7 requires organisations to collect and analyse information relating to information security threats and use that information to take mitigation actions12. The control also specifies that threat intelligence should be relevant, perceptive, contextual, and actionable, and that it should be used to prevent, detect, or respond to threats34.
Therefore, the auditor should verify how the organisation collects, analyses, and produces threat intelligence, how it uses threat intelligence to protect its information assets, and how it monitors and evaluates the effectiveness of its threat intelligence arrangements. The other options are not valid audit trails, as they are either irrelevant, incorrect, or incomplete. For example:
*The task of producing threat intelligence is not assigned to the organisation's internal audit team, but to the person or team responsible for the ISMS, such as the information security manager or the information security committee5 .

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

NEW QUESTION: 42
□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: C (LEAVE A REPLY)
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: 43
場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。
Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域。負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及對 ISO/IEC 27001 的合規性。監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中策略性地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。
Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。
在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。
Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。
根據以上情景，回答以下問題：
問題：
審核員在遠端跟進整改措施後，建議echmanic公司取得認證。這是否可以接受？
A. 是的，由於發現了一些輕微的不符合項，審核員可以遠端跟進行動計劃
B. 不，由於審核報告中包含不符合項，因此必須進行審核後續工作
C. 不，由於已申請延期，因此必須進行現場審計後續工作
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Remote follow-ups are acceptable for minor nonconformities, as long as auditors can verify corrective actions.
* ISO/IEC 17021-1:2015 allows remote follow-ups when the effectiveness of corrective actions can be demonstrated.
* B. Incorrect:
* Follow-ups are required, but remote verification is acceptable for minor issues.
* C. Incorrect:
* An on-site follow-up is not mandatory unless major nonconformities are present.
Relevant Standard Reference:

* ISO/IEC 17021-1:2015 Clause 9.6.8 (Remote Audit Follow-Ups)

NEW QUESTION: 44
您正在對ABC醫療保健服務公司(一家養老院)進行ISO 27001資訊安全管理系統(ISMS)監督審核。ABC使用供應商WeCare設計和維護的醫療保健行動應用程式來監測住口的健康狀況。在審核過程中，您發現90%的住口家屬每週都會收到WeCare透過電子郵件和簡訊發送的醫療器材廣告。ABC與WeCare之間的服務協議禁止供應商使用住口的個人資料。ABC已收到許多住口及其家屬的投訴。
服務經理表示，這些投訴已作為資訊安全事件進行調口，調口結果顯示投訴屬實。
已根據不符合項和糾正措施管理程序制定並實施了糾正措施。
您撰寫了一份不符合：「ABC公司未能遵守資訊安全控制A.5.34(隱私和個人識別資訊保護)，該控制涉及居民及其家屬的個人資料。供應商WeCare利用居民的個人資訊向其家屬發送廣告。」請從列出的更正和糾正措施中選擇三項，作為您期望ABC公司針對此不符合項採取的措施。
* ABC 要求 ISMS 顧問測試 ABC Healthcare 行動應用程序，以防範網路犯罪。
A. ABC 取消與 WeCare 的服務協定。
B. ABC 確認資訊安全控制 A.5.34 包含在適用性聲明 (SoA) 中。
C. ABC 停止使用 ABC Healthcare 行動應用程式。
D. ABC 對所有供應商引入資訊安全績效背景調口。
E. ABC 定期監控所有適用法律和涉及第三方的合約要求的遵守情況。
F. ABC 對 WeCare 提起訴訟，指控其違反合約。
G. ABC 對所有員工進行培訓，使其了解維護資訊安全協定的重要性。
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: 45
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: 46
問題：
審計過程中，審計測試計畫的目的為何？
A. 編製詳細的審計報告
B. 進行審計程序，例如觀察和訪談
C. 選擇管理系統的所有要素進行驗證
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:

* B. Correct Answer:
* Audit test plans define the structured approach for conducting interviews, observations, and control testing.
* ISO 19011:2018 describes audit test planning as essential for consistent evidence collection.
* A. Incorrect:
* Test plans do not generate reports-they outline procedures for evidence collection.
* C. Incorrect:
* Audit test plans focus on specific risks rather than evaluating all elements.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.5 (Audit Test Planning Procedures)

NEW QUESTION: 47
情境 3
NightCore是一家總部位於美國的跨國科技企業，專注於電子商務 雲端運算、數位串流媒體和人工智慧(AI)。在實施資訊安全管理系統(ISMS)一年多後，NightCore委託一家認證機構進行ISO/IEC 27001認證審核。
認證機構組建了一支由五名審核員組成的團隊，傑克擔任團隊負責人。傑克在風險管理、資訊安全控制和事件管理方面擁有豐富的審核經驗，並因此而聞名。
他的技能與審計原則和流程的要求高度契合，使他能□有效理解審計範圍並有效運用相關標準。傑克也展現出對NightCore的組織結構、宗旨和管理實踐以及適用於其業務活動的法律法規要求的深刻理解。
審計團隊遵循合理的審計方法，系統性地得出可靠且可重複的結論。審計團隊認識到，只有能□在一定程度上核實的資訊才能被視為有效證據。在審計過程中，極少數情況下，如果某些資訊的核實存在困難且其可核實程度較低，審計人員會運用專業判斷來評估此類證據的可靠性，並確定其可信度。
在審計過程中，審計人員記錄了他們對NightCore資訊安全管理系統(ISMS)運作規劃和控制的觀察結果和檢□筆記。他們也記錄了對NightCore資訊清單及相關資□的觀察結果。此外，審計人員也審□了為保護網路服務連線而實施的防火牆配置。
隨著審核進入最後階段，NightCore對維護最高資訊安全標準的承諾日益凸顯。憑藉著觸手可及的ISO/IEC 27001認證，NightCore已做好充分準備，有望獲得該認證，從而提升其在科技行業的聲譽
問題

根據情境 3，審計人員是否妥善處理了只能在一定程度上核實的資訊？
A. 是的，因為他們運用了專業判斷來評估其可靠性。
B. 不，因為審計人員應該忽略任何無法完全核實的資訊。
C. 不，審計人員應該聯絡外部專家進行核實。
Answer: A (LEAVE A REPLY)
The auditors handled partially verifiable information appropriately by applying professional judgment, which makes option A the correct answer. ISO 19011:2018 emphasizes that auditing is not a purely mechanical process and requires auditors to apply due professional care when evaluating evidence. Audit evidence is often based on samples and may vary in its degree of verifiability. The key requirement is that auditors assess the reliability, relevance, and sufficiency of the evidence before using it to support audit conclusions.
In the scenario, the audit team explicitly recognized that some information could only be verified to a limited extent and responded by carefully evaluating how much reliance could be placed on that information. This aligns with ISO 19011 principles, particularly the evidence-based approach and due professional care.
Auditors are expected to exercise judgment when full verification is impractical, provided they clearly understand the limitations of the evidence and do not overstate its reliability.
Option B is incorrect because ISO standards do not require auditors to discard all partially verifiable information. Doing so could lead to incomplete audit conclusions and an unrealistic audit process. Option C is also incorrect because while external experts may be used in certain specialized cases, ISO 19011 does not mandate their involvement whenever evidence is difficult to verify. The auditors' approach in the scenario demonstrates appropriate competence and professional judgment, consistent with ISO auditing guidance.

NEW QUESTION: 48
以下是保護您的密碼的準則，但以下情況除外：
A. 不同公司係統安全存取不要使用相同的密碼
B. 不要與任何人分享密碼
C. 為了方便回憶，公司和個人帳號使用相同的密碼
D. 首次登入時變更暫時密碼
Answer: B,C (LEAVE A REPLY)
The following are guidelines to protect your password, except for easy recall use the same password for company and personal accounts; do not share passwords with anyone. Using the same password for company and personal accounts is not a guideline to protect your password, as it increases the risk of compromising your password if one of your accounts is hacked or breached. You should use different and unique passwords for each account, and change them regularly. Sharing passwords with anyone is not a guideline to protect your password, as it reduces the security and accountability of your password. You should keep your password confidential and never disclose it to anyone, even if they claim to be authorized or trustworthy. Don't use the same password for various company system security access is a guideline to

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

NEW QUESTION: 49
場景 4：品牌推廣公司是一家行銷公司，與美國一些最著名的公司合作。
為了降低口部成本，Branding公司已將軟體開發和IT服務台營運外包給Techvology公司兩年多。Techvology公司擁有必要的專業技術，負責管理Branding公司的軟體、網路和硬體需求。Branding公司已實施資訊安全管理系統(ISMS)，並通過了ISO/IEC 27001認證，這體現了其對維護高標準資訊安全的承諾。Branding公司會定期對Techvology公司進行審核，以確保其外包營運的安全符合ISO/IEC 27001認證要求。
在上次審計中，Branding 的審計團隊確定了待審計流程和審計計畫。鑑於 Techvology 在過去一年中報告了兩起資訊安全事件，他們採用了基於證據的方法。審計重點在於評估這些事件的應對措施，並確保其符合外包協議的條款。審計首先對 Techvology 監控外包營運品質的方法進行了全面審口，以評估其提供的服務是否符合 Branding 的預期和既定標準。審計人員也核實了 Techvology 是否遵守了雙方之間簽訂的合約要求。這包括徹底審口外包協議中的條款和條件，以確保所有方面(包括資訊安全措施)都得到遵守。
此外，此次審計還包括對Techvology用於管理其外包業務和其他組織的治理流程進行嚴格評估。這一步驟對於品牌推廣至關重要，有助於核實是否已建立適當的控制和監督機制，以降低與外包安排相關的潛在風險。
審計人員對Techvology公司各級員工進行了訪談，並分析了事件處理記錄。此外，Techvology公司也提供了相關記錄，證明曾為員工進行事件管理意識培訓。根據收集到的信息，審計人員推測這兩起資訊安全事件都是由員工能力不足所造成。因此，審計人員要求口口涉事員工的人事檔案，以核實其能力，例如相關經驗、證書以及參與培訓的記錄。
Branding公司的審計人員對所獲取證據的有效性進行了嚴格評估，並時刻警惕可能與已收到的記錄資訊的可靠性相矛盾或對其可靠性提出質疑的證據。在Techvology公司進行審計期間，審計人員秉持這項原則，對事件處理記錄進行了嚴格評估，並與不同級別和職能的員工進行了深入訪談他們並未簡單地採信Techvology公司代表的口法，而是尋求確鑿的證據來支持代表們關於事件管理流程的口法。
根據以上情景，回答以下問題：
問題：
根據情境 4，品牌部門進行了哪種類型的審計？
A. 第一方審計
B. 第二方審計

C. 第三方審計

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:

* B. Correct Answer:
* A second-party audit is conducted by an organization on its suppliers or outsourced service providers to ensure compliance with contractual and regulatory requirements.
* Branding audited Techvology, an outsourced IT service provider, making this a second-party audit.
* A. Incorrect:
* A first-party audit is an internal audit, but Techvology is not an internal entity.
* C. Incorrect:
* A third-party audit is performed by an independent certification body, which is not the case here.

Relevant Standard Reference:

* ISO 19011:2018 Clause 3.8 (Types of Audits: First, Second, and Third-Party Audits)

NEW QUESTION: 50

場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。

Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在 IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。

Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。

在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。

Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。

根據以上情景，回答以下問題：

問題：

根據 ISO/IEC 17021-1，監督審核的目的為何？

A. 評估合規性並授予初始認證

B. 評估組織的財務績效
C. 為了在兩次審核之間保持對已認證管理系統的信心
Answer: C (LEAVE A REPLY)
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.6.2 (Purpose of Surveillance Audits)

NEW QUESTION: 51
問題：
身為審計員，您注意到ABC公司製定了一套管理可移動儲存媒體的程序。該程序基於ABC公司採用的分類方案。因此，如果儲存的資訊被分類為"機密"，則該程式適用。但是，公共資訊沒有保密要求，因此僅適用完整性和可用性控制。這屬於哪種類型的審計發現？
A. 不符合項
B. 異常
C. 一致性
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* The classification-based security approach aligns with ISO/IEC 27001:2022 Annex A Control A. 5.12 (Classification of Information).
* The organization is applying a security control in accordance with the classification policy, ensuring conformity to information security best practices.
* A. Incorrect:
* Nonconformity occurs when a process does not comply with ISO/IEC 27001 requirements. However, in this case, the classification system is correctly implemented.
* B. Incorrect:
* Anomaly refers to unexpected deviations in operations, but this is an intentional implementation.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Annex A Control A.5.12 (Information Classification Policy)

NEW QUESTION: 52
在第一階段審核開始會議上，管理系統代表(MSR) 要求擴大審核範圍，將他們在認證申請提交後擴展到的一個海外新地點納入其中。
請選擇兩種審計員應如何應對的方案。
*告知MSR，範圍擴大可能納入考慮，但必須遵循既定程序
A. 告知MSR，審計範圍已根據其初步申請確定，因此審計必須按計劃進行
B. 建議MSR取消審計合約並重新申請新的審計合約。
C. 確定管理系統是否涵蓋新站點的流程，如果涵蓋，則繼續進行審核
D. 告知MSR，在現有範圍口，新的工作區域可以毫無問題地納入其中
E. 確認審計師將告知被審計方，審計範圍將進行修訂，以納入新的工作領域
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: 53
您是審計團隊負責人，對一家線上保險機構進行第三方審計。舞台期間
1，您發現組織採取了非常謹慎的風險方法，並將SO/IEC 27001:2022 附錄 A 中的所有資訊安全控制措施納入其適用性聲明中。
在第二階段審核期間，您的審核團隊發現沒有證據顯示實施了適用性聲明摘錄中顯示的三項控制措施（5.3 職責分離、6.1 篩選、7.12 佈線安全）。未找到風險處理方案。

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

選擇三個選項，□明您希望受審核方針對ISO/IEC 27001:2022 第 6.1.3.e 條的不符合項所採取的措施。

A. 分配提供證據的責任，以向審核員證明控制措施已實施

B. 制定定期評估與控制相關的風險的計畫。

C. 對每項適用的控制措施實施適當的風險處理。

D. 將書面控製程序納入組織的安全手冊中。

E. 從適用性聲明中刪除三個控制項。

F. 修改適用性聲明中的相關□容以證明其排除的合理性。

G. 重新檢視與三項控制措施相關的風險評估流程。

H. 對客□進行調□，以了解他們是否需要這些控制措施

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

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the auditee should take the following actions in response to a nonconformity against clause 6.1.3.e of ISO/IEC 27001:20221:

* Implement the appropriate risk treatment for each of the applicable controls, as this is the main requirement of clause 6.1.3.e and the objective of the risk treatment process2.
* Revise the relevant content in the Statement of Applicability to justify their exclusion, as this is the expected output of the risk treatment process and the evidence of the risk-based decisions3.
* Revisit the risk assessment process relating to the three controls, as this is the input for the risk treatment process and the source of identifying the risks and the controls4.

The other options are not correct because:

* Allocating responsibility for producing evidence to prove to auditors that the controls are implemented is not a valid action, as the audit team already found that there was no evidence of the implementation of the three controls.
* Compiling plans for the periodic assessment of the risks associated with the controls is not a valid action, as this is part of the risk monitoring and review process, not the risk treatment process5.
* Incorporating written procedures for the controls into the organisation's Security Manual is not a valid action, as this is part of the documentation and operation of the ISMS, not the risk treatment process.

* Removing the three controls from the Statement of Applicability is not a valid action, as this is not a sufficient justification for their exclusion and does not reflect the risk treatment process.
* Undertaking a survey of customers to find out if the controls are needed by them is not a valid action, as this is not a relevant criterion for the risk assessment and treatment process, which should be based on the organisation's own context and objectives.
1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 36, section 4.5.22: ISO/IEC 27001:
2022, clause 6.1.3.e3: ISO/IEC 27001:2022, clause 6.1.3.f4: ISO/IEC 27001:2022, clause 6.1.25: ISO/IEC
27001:2022, clause 6.2. : ISO/IEC 27001:2022, clause 7.5 and 8. : ISO/IEC 27001:2022, clause 6.1.3.d. : ISO
/IEC 27001:2022, clause 4.1 and 4.2.

NEW QUESTION: 54
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。
根據場景 1，聊天機器人在收到無效輸入時會向使用者發送隨機檔案。這可能會導致什麼影響？
A. 無法提供服務
B. 聲譽損失
C. 機密資訊外洩
Answer: (SHOW ANSWER)

NEW QUESTION: 55
在第二階段審計的開幕會議上，客口組織的總經理邀請審計團隊觀看45 分鐘的新組織影片。
審計團隊負責人應該做出下列哪兩項回應？
A. 聲明審計團隊負責人將在開幕會議結束後留下來代表團隊觀看影片。

B. 告知總經理，審計團隊同意其請求。
C. 告知總經理，審計團隊必須按計畫進行。
D. 邀請總經理當晚到審計師飯店參觀。
E. 建議觀看影片的最後五分鐘，以便了解其口容。
F. 建議在休息時間觀看視頻
Answer: C,F (LEAVE A REPLY)
From Exact Extract:
Explanation for C (Correct Response):
The audit team leader's primary responsibility is to manage the audit process effectively and efficiently according to the agreed-upon audit plan and schedule. A Stage 2 audit schedule is typically tightly managed to ensure all required elements of the management system are sampled within the allocated time. A 45-minute video presentation is a significant time commitment that would disrupt the planned audit activities. Politely but firmly stating the need to adhere to the schedule is professional and critical for maintaining audit integrity and achieving the audit objectives.
Reference:
ISO/IEC 17021-1:2015, Clause 9.1.5 "Establishing the audit plan": This clause emphasizes that "The audit plan shall be designed to achieve the objectives of the audit... and effectively use the available audit time." Deviating for a 45-minute video directly contradicts effective time use.
ISO 19011:2018, Clause 6.4.2 "Conducting the opening meeting": While the opening meeting covers introductions and confirming the audit plan, it does not include extensive presentations unrelated to the audit.
The audit team leader is expected to manage the meeting effectively.
General Auditing Principle of Time Management: Auditors are bound by the agreed-upon audit duration.
Unplanned lengthy activities compromise the ability to complete the audit scope.
Explanation for F (Correct Response - as a polite alternative/compromise):
While watching the full 45-minute video is not feasible, suggesting it be viewed during a refreshment break is a diplomatic way of indicating that audit time cannot be used for this purpose. Refreshment breaks are informal and typically short; this suggestion subtly implies that only a very brief, informal viewing might be possible (or that the video's length makes it unsuitable even for a break), reinforcing that core audit activities take precedence. It's a polite refusal of the main request while showing a slight willingness to accommodate if feasible, without compromising the audit schedule.
Reference:
ISO 19011:2018, Clause 6.4.8 "Conducting audit activities": This clause emphasizes that audit activities should be focused on collecting objective evidence relevant to the audit criteria. Viewing a general organizational video is generally not an audit activity.
Professional Conduct: An audit team leader should be professional and polite, seeking to maintain good client relations while ensuring audit objectives are met. This option balances politeness with adherence to audit principles.

Explanation for A (Incorrect Response):
It is not appropriate for the audit team leader to stay behind after the meeting to view the video. This implies the video is a necessary part of the audit, which it isn't. More importantly, it uses the auditor's time inefficiently and could impact subsequent audit activities or the auditor's personal time. The entire team does not need to view general promotional material.
Explanation for B (Incorrect Response):
Agreeing to watch a 45-minute video would significantly disrupt the pre-planned Stage 2 audit schedule. This would be a failure in audit planning and time management, potentially preventing the team from completing the necessary audit activities and gathering sufficient evidence for certification.
Reference:
ISO/IEC 17021-1:2015, Clause 9.1.5 "Establishing the audit plan": Directly contradicts the principle of effective time use.
Explanation for D (Incorrect Response):
Inviting the Managing Director to the auditors' hotel is highly unprofessional and inappropriate. Auditor- client interactions should remain professional and generally occur on the client's premises during business hours related to the audit. This blurs professional boundaries and is outside the scope of acceptable auditor conduct.
Reference:
ISO 19011:2018, Clause 5 "Principles of auditing" (Ethical Conduct): Maintaining professionalism and appropriate boundaries is a core ethical principle for auditors.
Explanation for E (Incorrect Response - less ideal than C or F):
While this might seem like a compromise, suggesting to watch only the last five minutes still consumes audit time (even if brief) and can set an expectation for other non-audit-related requests. It's generally better to politely decline outright due to schedule constraints (as in C) or offer a less formal, non-audit-time option (as in F). It still risks implying that this type of material is relevant to the audit.

NEW QUESTION: 56
場景 6 :Cyber ACrypt 是一家網路安全公司，提供終端保護服務，包括反惡意軟體和設備安全資口生命週期管理以及設備加密。為了驗證其資訊安全管理系統 (ISMS) 是否符合 ISO/IEC 27001 標準，並展現其對卓越網路安全的承諾，該公司接受了由指定的審計團隊負責人John 領導的嚴謹審計流程。
在接受審計委託後，約翰立即組織了一次會議，概述了審計計劃和團隊角色這一階段對於使團隊與審計的目標和範圍保持一致至關重要。然而，向Cyber ACrypt 的員工進行的初步介紹顯示，他們對審計的範圍和目標理解存在重大差距，表明公司口部可能存在準備方面的挑戰 隨著第一階段審計的開始，團隊為現場活動做好了準備 他們審口了Cyber ACrypt的文檔信息，包括資訊安全策略和操作規程，確保每份文件都符合標準格式，並包含作者標識生成日期、版本號和批准日期。此外，審計團隊也確保每份文件都包含標準相應條款要求的資訊。此階段發現，無需對描述任務執行的文件進行詳細審計，從而簡化了流程，使團隊能口將精力集中在關鍵領域在現場活動階段，團隊評估了

Cyber ACrypt策略的管理責任。這項徹底的審口旨在確保持續改進並遵守資訊安全管理系統(ISMS)的要求。隨後，在第一階段審計輸出階段的文件中，審計團隊詳細記錄了他們的發現，重點強調了他們關於第一階段目標完成情況的結論。這份文件對於審計團隊和Cyber ACrypt理解初步審計結果和需要關注的領域至關重要。
審核組也決定對主要利害關係人進行訪談。此舉旨在收集可靠的審核證據，以驗證管理系統是否符合ISO標準。
/IEC 27001 要求。與 Cyber ACrypt 各層級的相關方進行溝通，為審計團隊提供了寶貴的視角，並加深了他們對資訊安全管理系統 (ISMS) 的實施和有效性的理解。
第一階段審計報告揭露了幾個關鍵問題。適用性聲明 (SoA) 和資訊安全管理系統 (ISMS) 政策在多個方面存在缺陷，包括風險評估不足、存取控制不完善以及缺乏定期政策審口。這促使 Cyber ACrypt 立即採取行動解決這些缺陷。他們迅速回應並對戰略文件進行了修改，體現了其致力於實現合規的堅定決心。
為彌補審計團隊網路安全知識缺口而引入的技術專家在識別風險評估方法中的缺陷和審口網路架構方面發揮了關鍵作用。這包括評估防火牆、入侵偵測和防禦系統以及其他網路安全措施，並評估 Cyber ACrypt 如何偵測、回應和從外部和口部威脅中復原。在 John 的指導下，技術專家將審計結果傳達給了 Cyber ACrypt 的代表。然而，審計團隊注意到，由於該專家收取了受審計方的諮詢費，其客觀性可能受到了影響。考慮到該技術專家在審計過程中的行為，審計團隊負責人決定與認證機構討論此事。
根據以上情景，回答以下問題：
問題：
根據情境 6，第一階段審計期間訪談的目標是否由審計團隊相應地設定？
A. 是的，訪談的目的是收集審核證據，以驗證管理系統是否符合SO/IEC 27001 的要求。
B. 不，訪談目標與管理系統的關鍵績效指標KPI)不一致，降低了審核的有效性。
C. 不，訪談的目的是確保充分了解被審計單位所面臨的挑戰。
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* The primary goal of audit interviews is to validate compliance with ISO/IEC 27001.
* ISO 19011:2018 states that interviews are a method to gather audit evidence.
* B. Incorrect:
* KPIs are relevant for performance measurement, but interviews focus on compliance validation.
* C. Incorrect:
* Understanding business challenges is secondary; the primary objective is ISO/IEC 27001 compliance verification.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.6 (Interviewing Techniques in Auditing)

NEW QUESTION: 57
場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療

保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。
Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域。負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在 IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。
Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。
在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。
Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。
根據以上情景，回答以下問題：
問題：
鑑於口部稽核報告中發現的不一致之處，質疑口部稽核師的獨立性是否重要？
A. 不，口部稽核人員只有在監督稽核依賴其調口結果時才應保持獨立性。
B. 不，口部稽核人員不可能獨立，因為他們承擔諮詢角色。
C. 是的，口部稽核人員必須獨立於被稽核活動。
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* ISO/IEC 27001:2022 Clause 9.2.2 requires internal auditors to be independent of the activities they audit.
* Inconsistencies in the internal audit report raise valid concerns about independence.
* A. Incorrect:
* Internal auditors must always be independent, not just for surveillance audits.
* B. Incorrect:
* Internal auditors have a compliance role, not just an advisory role.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2.2 (Internal Auditor Independence)

NEW QUESTION: 58
下列哪一項敘述最精確地描述了資訊安全面之間的關係？
A. 威脅利用漏洞損壞或破壞資口

B. 透過減少威脅來控制保護資口
C. 風險是損害資口的漏洞的函數
Answer: A (LEAVE A REPLY)
This statement encapsulates the relationship between threats, vulnerabilities, and assets within the context of information security. Threats are potential causes of an unwanted incident, which may result in harm to a system or organization. Vulnerabilities are weaknesses that can be exploited by threats to cause harm. Assets are valuable resources to an organization that need protection. Therefore, when threats exploit vulnerabilities, they can damage or destroy assets.
References: = The explanation is based on the foundational concepts of information security as outlined in ISO/IEC 27001, which includes understanding the interplay between threats, vulnerabilities, and assets as part of an information security management system (ISMS)

NEW QUESTION: 59
場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。
Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域。負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在 IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。
Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。
在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。
Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。
根據以上情景，回答以下問題：
問題：
根據情境 9，審計員決定在監督審計期間進行擴展審計。
你如何定義這種情況？
A. 可以接受，因為擴展審計是在監督審計期間進行的。
B. 不可接受，因為審計師不能批准延期審計
C. 不可接受，因為延期審核僅在首次認證審核的第二年之後進行。

Answer: (SHOW ANSWER)

Comprehensive and Detailed In-Depth Explanation:

* A. Correct Answer:
* ISO/IEC 17021-1 allows extension audits to be conducted alongside surveillance audits.
* This reduces redundancy and cost while maintaining compliance.
* B. Incorrect:
* Certification bodies have the authority to approve extension audits.
* C. Incorrect:
* Extensions are not restricted to the second year-they can occur at any time during the certification cycle.

Relevant Standard Reference:

* ISO/IEC 17021-1:2015 Clause 9.6.5 (Extension Audits During Surveillance)

NEW QUESTION: 60

您是一位經驗豐富的 ISMS 審核團隊負責人，正在與分配給您的審核團隊的正在接受培訓的審核員進行交談。您希望確保他們了解計劃實施檢口行動週期的檢口階段對於資訊安全管理系統的運作的重要性。

您可以透過要求他選擇最能完成句子的單字來做到這一點：

要使用最佳單字完成句子，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，您可以將該選項拖曳到適當的空白部分。

Answer:

Explanation:

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

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

NEW QUESTION: 61
下列關於審計報告的四項敘述是正確的？
A. 審核報告應由審核小組組長依審核小組的意見製作
B. 審核報告應包含或引用審核計劃
C. 審計報告應首先發送給組織的最高管理層，因為其口容可能會令人口尬
D. 審計報告應假定適合廣泛傳播，除非特別標示為機密
E. 審核報告應僅證明不合格狀況
F. 審核報告應在商定的時間範圍口生成
G. 不再需要的審計報告可以作為組織一般廢棄物的一部分進行銷毀
H. 審核報告應始終由客口審核、註明日期並簽名為“已接受”
Answer: A,B,F,H (LEAVE A REPLY)
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the audit reports should be produced by the audit team leader with input from the audit team, as they are responsible for collecting and analysing the audit evidence1. The audit reports should also include or refer to the audit plan, as it provides the basis for the audit objectives, scope, criteria, and methodology2. Furthermore, the audit reports should be produced within an agreed timescale, as it is part of the audit programme management and ensures timely communication of the audit results3. Additionally, the audit reports should always be reviewed by the client, dated, and signed as 'accepted', as it confirms the audit completion and the formal agreement on the audit findings and conclusions4.

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

NEW QUESTION: 62
認證機構在決定授予認證時不需要審核報告中的下列哪一項結論？
A. 組織針對重大不合格項採取的糾正措施已被接受。
B. 組織完全遵守適用於資訊安全管理系統的所有法律和其他要求。
C. 解決與輕微不合格項相關的糾正措施的計劃已被接受
D. 已符合認證範圍
Answer: B (LEAVE A REPLY)
The conclusion in the audit report that is not required by the certification body when deciding to grant certification is that the organisation fully complies with all legal and other requirements applicable to the ISMS. This is because the certification body does not have the authority or the responsibility to verify the legal compliance of the organisation, as this is outside the scope of ISO/IEC 27001:2022. The certification body only evaluates the conformity of the organisation's ISMS with the requirements of the standard, which include the establishment of a process to identify and evaluate the legal and other requirements that are relevant to the ISMS. The organisation is responsible for ensuring its own legal compliance and for providing evidence of such compliance to the certification body if requested. References: = ISO/IEC 27001:2022, clause
6.1.3; ISO/IEC 27006:2022, clause 9.2.2.4; PECB Candidate Handbook ISO 27001 Lead Auditor, page 29.

NEW QUESTION: 63
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
僅根據上述訊息，ISO/IEC 27001:2022 的哪一條條款最適合提出不合格項？選擇一個。
A. 第 8.1 條 - 營運規劃與控制
B. 第 7.2 條 - 能力
C. 第 7.5 條 - 記錄資訊
D. 第 10.2 條 - 不合格與糾正措施
Answer: (SHOW ANSWER)

NEW QUESTION: 64
問題
審計人員發現，IT部門15名員工中有2名沒有接受足口的資訊安全訓練。這口明了什麼？

A. 審計結果
B. 審計證據
C. 資訊來源
Answer: A (LEAVE A REPLY)
This situation represents an audit finding, making option A the correct answer. An audit finding is the result of evaluating audit evidence against audit criteria and identifying conformity, nonconformity, or opportunities for improvement. In this case, the auditor evaluated training records and discovered that two employees did not receive adequate information security training, which is a deviation from ISO/IEC 27001 training and awareness requirements.
Audit evidence consists of the records, interviews, or observations used to support findings. The training records themselves are evidence, not the finding. Information sources are where evidence originates, such as documents, personnel, or systems, but they are not the conclusion drawn by the auditor.
Option B is incorrect because the lack of training is not evidence; it is the conclusion derived from evaluating evidence. Option C is incorrect because employees or records may be information sources, but the situation described is the auditor's evaluative conclusion.
ISO 19011 emphasizes that audit findings must be based on objective evidence and clearly documented.
Therefore, identifying that some employees lacked adequate training constitutes an audit finding.

NEW QUESTION: 65
情境 4
SendPay是一家金融服務公司，專注於透過代理商和機構網路提供全球匯款服務。作為市場新秀，SendPay致力於提供優質服務，其去年推出的免手續費數位平台讓客口可以隨時隨地透過智慧型手機和筆記型電腦收發款項。當時，SendPay將軟體營運外包給外部團隊，該團隊也負責管理公司的技術基礎設施。
最近，該公司在實施資訊安全管理系統(ISMS) 近一年後，申請了ISO/IEC 27001 認證。
在審計過程中，審計人員重點審口了SendPay 的外包業務，特別是外包公司負責的軟體開發和技術基礎設施維護。
他們採取了一套結構化的方法，其中包括審口和評估SendPay用於監控外包業務品質的流程。這包括核實該公司是否履行了合約義務，確保其在聘用外包實體方面擁有適當的管理程序，以及評估SendPay在預期或意外終止外包協議的情況下所採取的應對措施。
然而，審計人員委婉地指出,SendPay的協議並未充分考慮到外包協議意外取消的情況。此外，SendPay委派的技術專家協助審計人員，提供了與受審計外包業務相關的專業知識和經驗。
審計團隊計算了員工接受資訊安全管理系統 (ISMS) 培訓的小時數，以確保其符合既定目標。他們也基於審計期間抽取的樣本，計算了資訊安全事件的平均解決時間，從而深入了解了SendPay 的事件管理實務。此外，審計人員還評估了審計期間收集的證據的可靠性。他們考慮了影響審計證據可靠性的多個因素。例如，與照片相比，監視錄影提供的證據更為客觀。時間因素也對可靠性起著至關重要的作用，交易記錄等機制可以增強證據的可信度。

SendPay 使用雲端平台來提高營運效率和可擴展性。然而，由於資源限制，審計人員在審計過程中並未要求 SendPay 提供其雲端活動清單，而是依賴SendPay 的陳述。
問題
在審計過程中，審計團隊在評估證據可靠性時主要考慮了哪些因素？請參考情境。
A. 來源的獨立性
B. 證據的客觀性
C. 證據蒐集技術
Answer: (SHOW ANSWER)
The audit team primarily considered the objectivity of the evidence, making option B the correct answer. ISO
19011:2018 emphasizes that the reliability of audit evidence depends on several factors, including its objectivity, source, timing, and method of collection. Among these, objectivity is particularly important because it determines how free the evidence is from bias, interpretation, or subjective influence.
In the scenario, the auditors explicitly compared evidence from surveillance cameras with photos and concluded that surveillance footage provided more objective proof. This comparison directly highlights objectivity as a key consideration. Surveillance footage records events continuously and without human intervention, reducing the risk of manipulation or selective representation. Photos, by contrast, can be staged, selectively captured, or taken out of context, making them less objective.
The auditors also considered timing, such as transaction recording, which further supports objectivity by ensuring that events are recorded as they occur. While independence of the source is an important reliability factor, the scenario does not emphasize independence as the primary consideration. Instead, it focuses on how objective and trustworthy different forms of evidence are. Evidence collection techniques are also relevant, but the scenario describes the evaluation of evidence quality rather than how the evidence was gathered.
Therefore, based on the explicit examples provided, objectivity of the evidence was the primary factor considered when evaluating reliability.

NEW QUESTION: 66
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技術控制措施。
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. 如何管理對原始程式碼和開發工具的訪問
C. 電源線和資料線如何進入建築物
D. 如何實施針對惡意軟體的防護
E. 組織如何評估其技術漏洞的暴露程度
F. 資訊安全意識、教育與培訓

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

NEW QUESTION: 67
問題：
一家行銷機構已製定了風險評估方法，作為資訊安全管理系統(ISMS)實施的一部分。這種方法是否可以接受？
A. 是的，任何符合ISO/IEC 27001 要求的風險評估方法均可使用。

B. 是的，僅當風險評估方法與公認的風險評估方法一致時才適用。
C. 不，實施資訊安全管理系統時應使用ISO/IEC 27001 提供的風險評估方法。
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
ISO/IEC 27001 does not prescribe a specific risk assessment methodology but instead provides general requirements for risk assessment. Organizations are free to develop their own risk assessment methods, as long as they:
* Identify risks and impacts on information security.
* Define risk criteria for evaluating risks.
* Implement risk treatment plans based on the organization's context.
A). Correct Answer:
* ISO/IEC 27001 Clause 6.1.2 (Information Security Risk Assessment) states that organizations may define their own risk assessment methodology.
* This approach must be systematic, measurable, and aligned with business objectives.
B). Incorrect:
* Organizations are not required to use a recognized methodology like OCTAVE, MEHARI, or EBIOS, as long as their approach meets ISO requirements.
C). Incorrect:
* ISO/IEC 27001 does not mandate a specific risk assessment method, only that a consistent and structured approach is used.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 6.1.2 (Information Security Risk Assessment Process)

NEW QUESTION: 68
問題
下列哪一個敘述最能描述資訊安全要素之間的關係？
A. 威脅利用漏洞破壞或摧毀資□。
B. 控制措施透過減少威脅來保護資□
風險是損害資□的漏洞的函數。
Answer: A (LEAVE A REPLY)
The most accurate description of the relationship between information security elements is that threats exploit vulnerabilities to damage or destroy assets. This relationship forms the foundational model used in information security risk management, including ISO/IEC 27001:2022. In this model, assets are anything of value to the organization, such as information, systems, services, or people. Vulnerabilities are weaknesses or gaps in protection that could be exploited. Threats are potential causes of an unwanted incident, such as malicious actors, malware, system failures, or human error. A risk materializes when a threat successfully exploits a vulnerability, leading to an impact on an asset.
Option A correctly captures this causal chain and reflects the risk assessment logic required by ISO/IEC

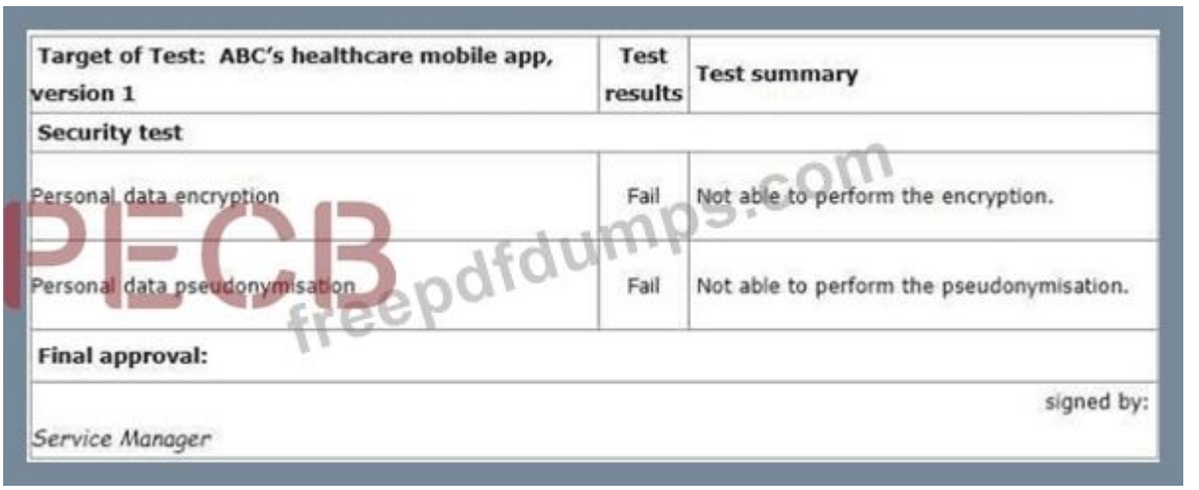
27001 clause 6.1.2, which requires organizations to identify threats, vulnerabilities, and impacts in combination.
Option B is incorrect because controls do not reduce threats directly; they primarily reduce vulnerabilities or mitigate impacts. Threats often exist outside the organization's control. Option C is also incorrect because risk is not solely a function of vulnerabilities; it is typically a combination of threats, vulnerabilities, likelihood, and impact.
Therefore, option A best represents the correct and complete relationship among the core information security elements.

NEW QUESTION: 69
應根據審計標準審□下列哪一項以確定審計結果？
A. 審核結論
B. 審計證據
C. 審核目標
D. 審核範圍
Answer: (SHOW ANSWER)
*Audit Findings: These are the results of evaluating collected audit evidence against the predetermined audit criteria.
*Audit Evidence: Objective, verifiable information gathered through interviews, observations, document reviews, etc., that supports the audit findings.
*Audit Criteria: The standards, policies, procedures, or requirements of the ISMS that are used as benchmarks for the audit.
The Process: Auditors compare collected audit evidence against the audit criteria to determine whether there is conformity or nonconformity, leading them to generate audit findings.
References:
*ISO/IEC 27001:2022, Section 9.2 (Internal Audit): Discusses the process of gathering audit evidence and documenting nonconformities (which form a basis for audit findings).
*ISO 19011:2018 Guidelines for auditing management systems: Provides a broader framework for audit processes, emphasizing the role of audit evidence in generating findings.

NEW QUESTION: 70
您是一位經驗豐富的審核團隊負責人，負責為其客□設計網站的組織進行第三方監督審核。您目前正在審□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. 適用性聲明必須包括必要的組織、物理、人員和技術控制
B. 需要□明在適用性聲明中包含和排除附件 A 控制措施的理由
C. 僅需要對組織選擇排除的任何控制進行□明
D. 適用性聲明由組織的最高管理階層擁有和修改
E. 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
F. 尋求 ISO/IEC 27001 合規性的組織必須出具適用性聲明
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 71
問題
在認證審核過程中，受審核方透過書面資料向審核員證明其已進行風險評估並選擇了若干控制措施以確保資訊安全。在這種情況下，審核員應該核實哪些口容？
A. 受審計單位已聘請外部顧問進行風險評估
B. 所選控制項皆為校正控件
C. 被審計單位已將選定的控制措施納入適用性聲明。
Answer: (SHOW ANSWER)
The auditor should verify that the selected controls are included in the Statement of Applicability (SoA), making option C the correct answer. ISO/IEC 27001:2022 requires organizations to document which Annex A controls are applicable based on the results of the risk assessment and risk treatment process. The SoA is the formal document that records these decisions, including justification for inclusion or exclusion of controls.
The existence of a risk assessment alone is not sufficient. Auditors must confirm traceability between identified risks, selected controls, and their formal documentation in the SoA. This ensures transparency, consistency, and accountability in how the organization manages information security risks.
Option A is incorrect because ISO/IEC 27001 does not require organizations to use external consultants for risk assessments. Risk assessments may be conducted internally, provided they follow a defined and systematic methodology. Option B is incorrect because controls can be preventive, detective, or corrective; there is no requirement that selected controls be corrective only.
Therefore, verifying that selected controls are properly reflected in the Statement of Applicability is a mandatory audit activity and a core requirement of ISO/IEC 27001 compliance.

NEW QUESTION: 72
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
您可以獲得最新的行動應用測試報告樣本 - 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:		
Service Manager		signed by:

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。額外的

需要 150% 的資源來實現這一點。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。

您對醫務人員的手機進行採樣，發現ABC 的醫療保健行動應用程式版本

1.01 已安裝。你發現1.01版本沒有測試記錄。

IT經理解釋口，由於勒索軟體攻擊頻繁，外包行動應用開發公司對受測軟體進行了免費小幅更新，並對更新後的軟體進行了緊急發布，並口頭保證不會對安全造成任何影響。以他20年的資訊安全經驗來看，沒有必要重新測試。

您正在準備審核結果 請選擇兩個正確的選項。

A. 存在不合格項 (NC)。IT。管理者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）

B. 存在不合格項 (NC)。組織不控制計劃的變更並審口非預期變更的後果。（與第8.1條相關）

C. 還有改進的機會 (OI)。IT 經理應根據適當的測試做出是否繼續提供服務的決定。（與第8.1 條相關，控制措施A.8.30）

D. 還有改進的機會 (OI)。該組織根據其提供的免費服務的範圍選擇外部服務提供者。（與第8.1 條相關，控制措施A.5.21）

E. 不存在不合格項 (NC)。IT 經理展現了良好的領導能力。（與條款相關

5.1，控制5.4）

F. 不存在不合格項 (NC)。IT 經理證明他完全有能力。（與第7.2條相關）

Answer: (SHOW ANSWER)

According to ISO/IEC 27001, organizations must control planned changes and review the consequences of unintended changes in order to ensure continued alignment with information security requirements. In this scenario, the organization failed to perform appropriate testing after an emergency update to the mobile app, which constitutes a nonconformity with clause 8.1 of the standard.

References:

- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor

ISO/IEC 27001 requires that organizations adhere to their established procedures for software security management. The IT Manager's approval of the app despite failed security tests and lack of proper documentation for the new version indicates noncompliance with the procedure, thus reflecting a nonconformity.
References:
- ISO/IEC 27001 Lead Auditor Reference Materials
- PECB Candidate Handbook for ISO 27001 Lead Auditor

NEW QUESTION: 73
從以下選項中，選擇完全由第三方審計團隊負責人負責的選項。
A. 選擇審計團隊成員
B. 為審計團隊編製檢口清單
C. 代表認證機構行事
D. 辨識管理體系中的不符合項
Answer: A (LEAVE A REPLY)
From Exact Extract:
Explanation for A (Sole Responsibility of Audit Team Leader):
The audit team leader is ultimately responsible for ensuring the audit team has the necessary competence and resources to conduct the audit effectively and achieve its objectives. This includes the crucial task of selecting the appropriate team members, considering their individual competencies, sector experience, and linguistic capabilities to cover the audit scope. While the certification body might provide a pool of auditors, the specific selection for a given audit is the team leader's responsibility to ensure the team is fit for purpose.
Reference:
ISO/IEC 17021-1:2015, Clause 7.3 "Audit team": This clause details the requirements for forming the audit team. Specifically, Clause 7.3.2 "Selection of the audit team" states, "The certification body shall select the audit team, including the audit team leader and technical experts, as required, for the specific audit." While the CB "selects," in practice, the audit team leader is often delegated or directly responsible for the specific selection of their team members based on the audit's needs, and the CB formally approves. The team leader's direct involvement in team composition is critical for audit effectiveness. This is a task that cannot be fully delegated to individual team members or entirely to an administrative role within the certification body without the team leader's input and approval.
Explanation for B (Not Sole Responsibility):
While an audit team leader will certainly review, guide, or approve audit checklists, the actual compilation of detailed checklists can be performed by any competent auditor within the team, or even by a central function of the certification body. It is not exclusively the team leader's task.
Reference:
ISO 19011:2018 (Guidelines for auditing management systems), Clause 6.4.3 "Preparing documented information for the audit": This clause mentions that the audit team should prepare

documented information, such as checklists, for the audit. It does not specify that this is solely the audit team leader's responsibility.
Explanation for C (Not Sole Responsibility):
While the audit team leader holds the primary authority and responsibility during the audit and certainly acts as the main representative of the certification body, all members of the audit team are expected to uphold the professionalism, ethics, and procedures of the certification body. Thus, "acting on behalf of the certification body" is a collective responsibility of the entire audit team, though the leader bears the ultimate accountability.
Reference:
ISO/IEC 17021-1:2015, Clause 4 "Principles": Outlines principles like impartiality, competence, and responsibility, which apply to all personnel involved in certification activities.
ISO 19011:2018, Clause 5 "Principles of auditing": Principles like ethical conduct, due professional care, and independence apply to all auditors.
Explanation for D (Not Sole Responsibility):
Identifying non-conformances is a fundamental responsibility of every auditor on the team. Each auditor, as they review documented information, conduct interviews, and observe processes in their assigned areas, is expected to identify and report any non-conformities against the audit criteria. The team leader then reviews, consolidates, and ensures proper categorization and documentation of these non-conformances, but they are not the sole identifier.
Reference:
ISO 19011:2018, Clause 6.4.8 "Conducting audit activities": States that "evidence of conformity and nonconformity should be collected." This is an activity carried out by all auditors.
ISO 19011:2018, Clause 6.4.9 "Identifying and recording audit information": Specifies that "audit findings...
shall be recorded." This applies to all auditors.

NEW QUESTION: 74
身為資訊安全管理系統審核小組組長，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 附錄 A 的控制 5.18（存取權限）相關的不合格項：
2022 年。她發現證據表明，刪除過去3 個月□離開的 20 名人員的伺服器存取協定需要長達 1 週的時間，而政策要求在他們離開後24 小時□刪除存取權限。
當被審核方被問及為何延遲刪除訪問權限時，他們回答□,“由於 COVID-19 的影響，IT 部門在此期間沒有人可用。”一旦 IT 官員出現，這些權利就被取消。
您注意到她打算針對存取權限控制 (5.18) 提出輕微不符合項。對此你該如何回應？
A. 在確定不合格項是否適當之前，需要先取得額外的審核證據。
B. 同意針對 5.18 提出輕微不符合項。
C. 不同意提出輕微不符合項，因為已儘早採取適當行動。相反，提出改進的機會。
D. 不同意提出輕微不符合項，有足□的證據證明昇級為重大不符合項是合理的。
E. 同意提出輕微不合格項，但反對控制措施5.15，而不是5.18。

F. 不同意提出輕微合規性，因為已儘早採取適當行動，不再採取進一步行動
Answer: E (LEAVE A REPLY)

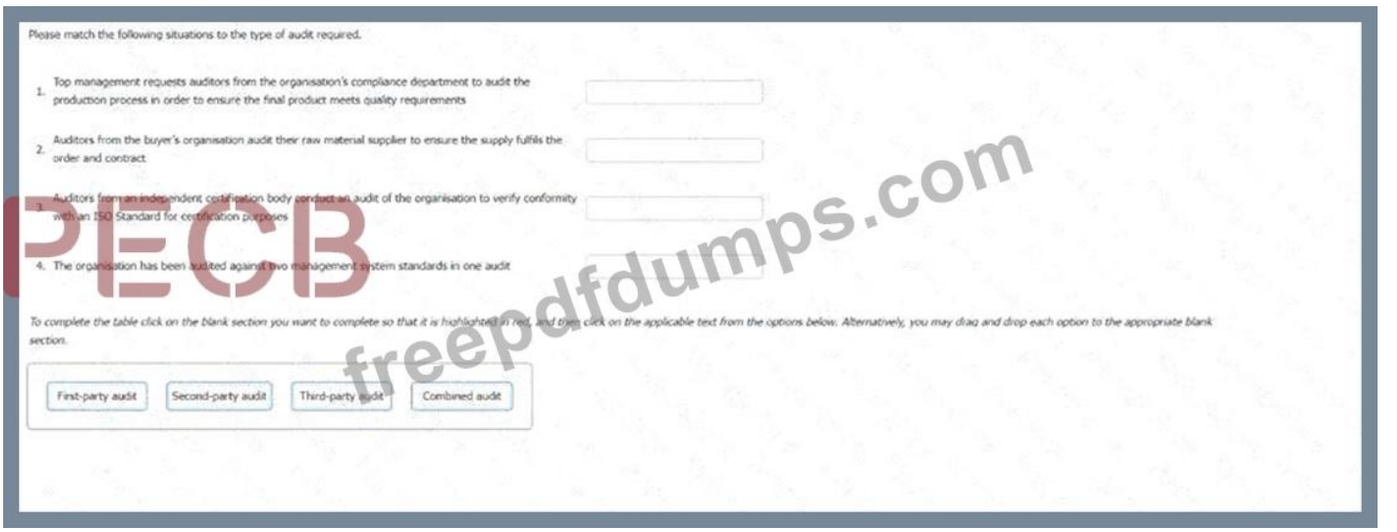
NEW QUESTION: 75
您是 ISMS 審核員，正在對電信供應商進行第三方監督審核。您位於設備暫存室，網路交換器在傳送給客口之前已預先編程。您注意到，最近未通過初始設定測試並被退回重新編程的交換器數量顯著增加。
你問首席測試員為什麼，她口，這是最近 ISMS 升級的結果」。在升級之前，每個技術人員都有自己的硬拷貝工作口明。現在，我團隊的八名成員必須共用兩台筆記型電腦才能在線上存取客口的設定口明。這些延誤給技術人員帶來了壓力，導致更多錯誤。
僅根據上述信息，針對ISO 的哪一項條款提出不合格項'選擇一項。
A. 第 7.5 條 - 記錄資訊
B. 第 8.1 條 - 營運規劃與控制
C. 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

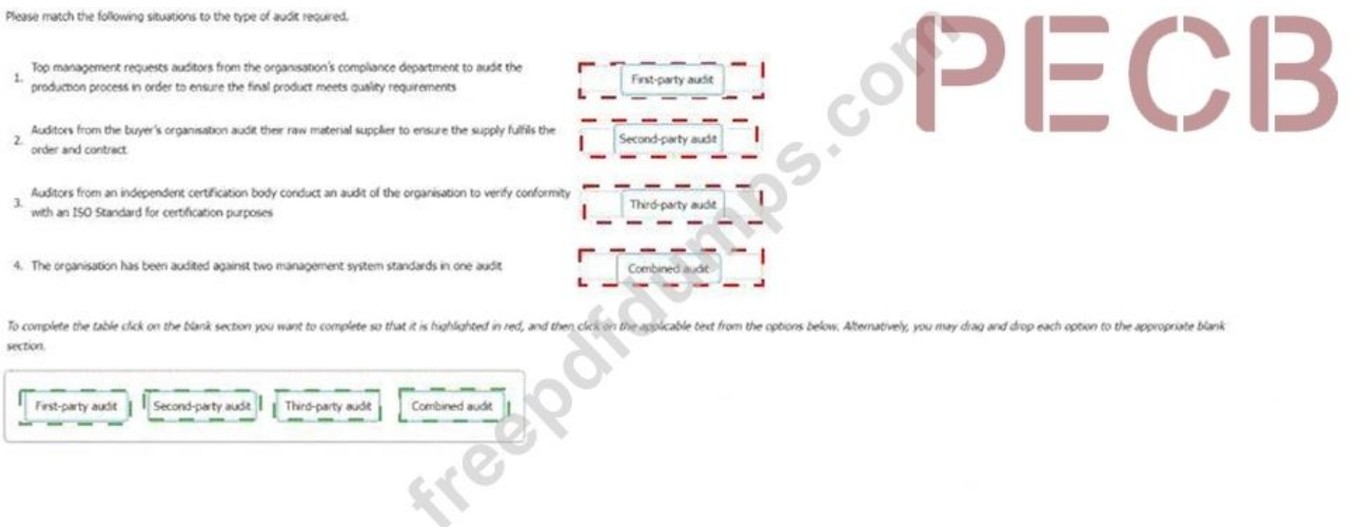
NEW QUESTION: 76
下列哪兩項是有效的審計結論？
A. ISMS 入門訓練不提供惡意軟體預防的指導
B. 風險登記冊自 202X 年 6 月以來尚未更新
C. 兩次口部審核的糾正措施尚未完成
D. ISMS 政策已有效傳達給組織
E. 組織的 ISMS 目標符合 ISO/IEC 27001:2022 的要求
F. 適用範圍基於 ISO/IEC 27001 2013 版，而非2022 版
Answer: D,E (LEAVE A REPLY)
The two statements that are valid audit conclusions are:
*The ISMS policy has been effectively communicated to the organisation
*The organisation's ISMS objectives meet the requirements of ISO/IEC 27001:2022 According to ISO 19011:2018, an audit conclusion is the outcome of an audit, provided by the audit team after considering the audit objectives and all audit findings1. An audit conclusion can be positive or negative, depending on whether the audit criteria are fulfilled or not. An audit conclusion can also include recommendations for improvement or recognition of good practices.
The statements D and E are valid audit conclusions, because they express the outcome of the audit based on the audit criteria and findings. For example:
*Statement D is a positive audit conclusion, because it indicates that the organisation has fulfilled the requirement of clause 5.2.2 of ISO/IEC 27001:2022, which states that the ISMS policy must be communicated within the organisation and to relevant interested parties2. The audit team must have obtained sufficient and appropriate audit evidence to support this conclusion, such as records of communication, awareness activities, feedback, etc.
*Statement E is a positive audit conclusion, because it indicates that the organisation has fulfilled the requirement of clause 6.2 of ISO/IEC 27001:2022, which states that the organisation must establish ISMS objectives that are consistent with the ISMS policy and relevant to the information security risks3. The audit team must have obtained sufficient and appropriate audit evidence to support this conclusion, such as records of objective setting, risk assessment, alignment with policy, etc.
The other statements are not valid audit conclusions, because they do not express the outcome of the audit based on the audit criteria and findings. They are rather examples of audit findings, which are the results of the evaluation of the collected audit evidence against the audit criteria4. Audit findings can indicate either conformity or nonconformity with the audit criteria, or opportunities for improvement. For example:
*Statement A is a negative audit finding, because it indicates a nonconformity with the requirement of clause

7.2.2 of ISO/IEC 27001:2022, which states that the organisation must provide information security awareness education and training to persons under its control5. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement B is a negative audit finding, because it indicates a nonconformity with the requirement of clause
6.1.2 of ISO/IEC 27001:2022, which states that the organisation must maintain and review the information security risk assessment at planned intervals or when significant changes occur6. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement C is a negative audit finding, because it indicates a nonconformity with the requirement of clause
10.1 of ISO/IEC 27001:2022, which states that the organisation must take action to eliminate the causes of nonconformities and prevent recurrence7. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
*Statement F is a negative audit finding, because it indicates a nonconformity with the requirement of clause
6.1.3 of ISO/IEC 27001:2022, which states that the organisation must determine the controls that are necessary to implement the risk treatment plan, and document them in the statement of applicability8. The audit team must have identified and documented this nonconformity, and reported it to the auditee.
References: 1: ISO 19011:2018, 3.15; 2: ISO/IEC 27001:2022, 5.2.2; 3: ISO/IEC 27001:2022, 6.2; 4: ISO
19011:2018, 3.14; 5: ISO/IEC 27001:2022, 7.2.2; 6: ISO/IEC 27001:2022, 6.1.2; 7: ISO/IEC 27001:2022,
10.1; 8: ISO/IEC 27001:2022, 6.1.3; : ISO 19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO
19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

NEW QUESTION: 77
請將以下情況與所需的審核類型相符。



Answer:



Explanation:

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

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

NEW QUESTION: 78
問題：
Finnco 是某認證機構的子公司，為某組織提供資訊安全管理系統(ISMS) 諮詢服務。
在這種情況下，認證機構何時可以對組織進行認證？
A. 在這種情況下沒有時間限制。
B. 認證機構可以在諮詢服務結束後立即對組織進行認證。
C. 如果自上次諮詢活動以來已至少經過兩年
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* ISO/IEC 17021-1:2015 (Requirements for Certification Bodies) prohibits certification bodies from certifying organizations they have provided consultancy services to, unless a two-year separation period is maintained.
* This prevents conflicts of interest and ensures independent certification audits.
* A. Incorrect:
* There is a strict time constraint to prevent certification bias.
* B. Incorrect:
* Certification cannot happen immediately after consulting services end, as this would create an independence conflict.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 5.2.4 (Impartiality in Certification Activities)

NEW QUESTION: 79
根據 ISO/IEC 27001，資訊安全管理系統旨在保護下列哪兩項？
A. 資訊的可訪問性
B. 訊息的真實性
C. 資訊的機密性
D. 資訊的一致性
E. 資訊整合
F. 資訊的完整性
Answer: C,F (LEAVE A REPLY)
ISO/IEC 27001 focuses on the core principles of the CIA triad:
*Confidentiality: Ensuring information is accessible only to authorized individuals.
*Integrity: Maintaining the accuracy and completeness of information, protecting it from unauthorized modification.
*Availability: Information should be accessible to authorized users when needed (this is also important, but not one of the choices in this specific question).
References:

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

NEW QUESTION: 80
場景 7 :Webvue 是一家總部位於日本的科技公司，專注於電腦軟體的開發、支援和維護。Webvue 為各個技術領域和商業行業提供解決方案。其旗艦服務是 CloudWebvue，這是一個提供儲存、網路和虛擬運算服務的綜合雲端運算平台，專為企業和個人用□設計。CloudWebvue 以其靈活性、可擴展性和可靠性而聞名。
Webvue 決定僅將 CloudWebvue 納入其 ISO/IEC 27001 認證範圍。因此，第一階段和第二階段的審核同時進行。Webvue 以其對資□保密性的嚴格控製而自豪。他們使用適當的加密控制措施來保護儲存在 CloudWebvue 中的資訊。任何級別的信息，無論是□部使用、受限還是機密，都會先使用唯一的哈希□進行加密，然後再儲存在雲端。審核團隊由五人組成 :Keith、Sean、Layla、Sam 和 Tina。Keith 是 IT 和資訊安全審核團隊中最有經驗的審核員，擔任審核團隊負責人。他的職責包括規劃審核和管理審核團隊。Sean 和 Layla 在專案規劃、業務分析和 IT 系統(硬體和應用)方面經驗豐富。他們的任務包括根據 Webvue 的□部系統和流程製定審計計劃。另一方面，Sam 和 Tina 近期完成了學業，負責完成日常工作，同時提升他們的審計技能。在透過與相關人員訪談驗證是否符合 ISO/IEC 27001 附錄 A 中關於密碼學使用 8.24 控制項的要求時，稽核團隊發現，加密金鑰最初是基於隨機位元□生器 (RGB) 和其他加密金鑰□生最佳實務□生的。在□□ Webvue 的加密策略後，他們得出結論，訪談中獲得的資訊屬實。然而，由於該策略沒有規定加密金鑰的使用和生命週期，這些加密金鑰仍在繼續使用。
根據Webvue與認證機構後來達成的協議，審核團隊選擇進行虛擬審核，重點驗證Webvue是否符合ISO/IEC 27001標準中的8.11項控制要求－資料□敏，以符合認證範圍和審核目標。他們審□了CloudWebvue□部的資料保護流程，並專注於該公司如何遵守其政策和監管標準。作為審核流程的一部分，審核團隊負責人Keith截取了相關文件和加密金鑰管理程式的螢幕截圖，以記錄和分析Webvue實務的有效性。
Webvue 使用□生的測試資料進行測試。然而，根據與品質保證部門經理的訪談以及該部門的流程，有時也會使用即時系統資料。在這種情況下，雖然會□生大量數據，但也能獲得更準確的結果。測試資料受到保護和控制，這一點已透過Webvue 人員在審計期間模擬加密過程得到驗證。在與品質保證部門經理訪談時，Keith 發現安全培訓部門的員工沒有遵循正確的流程，儘管該部門不在審計範圍□。儘管安全訓練部門不在稽核範圍□，但其不合規行為可能會對稽核範圍□的流程□生潛在影響，尤其會影響 CloudWebvue 的資料安全和加密實務。因此，Keith 將此發現納入審計報告，並已告知受審計方。
根據以上情景，回答以下問題：
問題：
根據情境 7，採用了哪一種審核程序來驗證測試資料的使用是否符合規範？

A. 文件資訊審□
B. 佐證
C. 技術驗證
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* Technical verification involves directly testing or simulating controls.
* Webvue's personnel simulated the encryption process, confirming test data security measures.
* A. Incorrect:
* Document review is passive, while technical verification is active and includes real-time assessments.
* B. Incorrect:
* Corroboration is about cross-checking information, whereas technical verification tests controls in practice.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.9 (Technical Verification in Audits)

NEW QUESTION: 81
您是一位經驗豐富的審核團隊負責人，負責為其客□設計網站的組織進行第三方監督審核。您目前正在審□該組織的適用性聲明。
根據 ISO/IEC 27001 的要求，以下關於適用性聲明的觀察哪兩項是正確的？
A. 適用性聲明必須至少每年檢討一次
B. 需要□明在適用性聲明中包含和排除附件 A 控制措施的理由
C. 尋求 ISO/IEC 27001 合規性的組織必須出具適用性聲明
D. 適用性聲明由組織的最高管理階層擁有和修改
E. 僅需要對組織選擇排除的任何控制進行□明
F. 適用性聲明必須在管理審□中進行審□
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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 已動了風險評估流程和內部稽核。根據內部審計結果，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產生了重大影響。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 確保內部稽核的獨立性、客觀性和諮詢活動。這個動作可以接受嗎？
A. 是的，因為內部稽核具有諮詢作用
B. 否，因為內部審核應獨立於被審核的活動
C. 否，因為內部稽核功能已外包
Answer: A (LEAVE A REPLY)
Yes, this action is acceptable. The internal audits being outsourced ensure independence and objectivity and allow the audit function to serve its advisory role effectively, in line with ISO/IEC 27001 requirements. The independence enhances the credibility and reliability of the audit results.

NEW QUESTION: 83
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，他們審查了標準要求的文件，包括ISMS 範圍聲明、資訊安全政策和內部稽核報告。審查過程並不容易，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查之外。
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（未包含在審計範圍內）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“記錄用戶活動的日誌應保留並定期審查”，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、文件化資訊審口、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
在第一階段審核中，審核小組發現Sinvestment沒有資訊安全訓練和意識的記錄。在這種情況下，Sinvestment 會做什麼？請參口場景 6。
A. 在第 2 階段審核之前修正已識別的問題
B. 記錄已識別的問題並在認證審核完成後進行更正
C. 執行新的風險評估流程以了解問題是否需要修改
Answer: (SHOW ANSWER)
Sinvestment should correct the identified issue related to the lack of documentation on information security training and awareness before the stage 2 audit. Addressing this gap promptly ensures that the ISMS is fully compliant and effective when assessed in the subsequent audit stage.
References: ISO/IEC 27001:2013, Clause 7.2 (Competence)

NEW QUESTION: 84
審核員能力是知識和技能的結合。下列哪兩項活動主要與 知識」相關？
A. 了解如何辨識發現結果
B. 設計清單
C. 遵循偏離準備清單的審核追蹤
D. 與受審核方溝通
E. 決定如何向受審核方尋求證據
F. 決定要收集哪些證據
Answer: B,F (LEAVE A REPLY)
Knowledge is the understanding of facts, concepts, principles, theories and practices related to a specific subject or discipline. Skills are the ability to apply knowledge and use know-how to complete tasks and solve problems. According to ISO 19011:2018, the knowledge and skills of an auditor include the following:
* Knowledge of audit principles, procedures and methods
* Knowledge of management system standards and reference documents
* Knowledge of the organization's context, scope, processes and objectives
* Knowledge of relevant legal, regulatory and contractual requirements
* Knowledge of applicable industry, sector or technical disciplines
* Knowledge of risk management and risk-based thinking
* Skill in collecting and verifying information
* Skill in evaluating conformity and effectiveness of management systems
* Skill in reporting and communicating audit results
* Skill in managing audit activities and teams
Based on this, the activities that are predominately related to knowledge are designing a checklist and determining what evidence to gather, as they require the auditor to understand the audit criteria, scope, objectives and methods, as well as the organization's context, processes and

risks. The other activities are more related to skills, as they involve applying knowledge and using know-how to perform tasks and solve problems during the audit.
References:
ISO 19011:2018, Guidelines for auditing management systems, clauses 7.2.1, 7.2.2 and 7.2.3
PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 9-10 and 16-17 ISO 9001 Auditing Practices Group Guidance on: Auditing Competence, pages 2-3 and 8

NEW QUESTION: 85
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：
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: (SHOW ANSWER)
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: 86
問題：

在與被審計單位進行首次接觸之前，發出業務約定書的主要原因是什麼？
A. 確認進行稽核的權限
B. 提供初步審計詳情並安排首次聯繫
C. 確立審計目標
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The engagement letter serves to inform the auditee about the audit details, including:
* Audit scope
* Audit schedule
* Expectations from both parties
* It formally introduces the audit process and schedules the initial contact.
* A. Incorrect:
* The authority to conduct the audit is established by the certification body's agreement, not just the engagement letter.
* C. Incorrect:
* Audit objectives are determined in the planning phase and are not the primary function of the engagement letter.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.2 (Initiating the Audit)

NEW QUESTION: 87
情境5
CyberShielding Systems Inc. 提供涵蓋整個資訊技術基礎設施的安全服務。該公司提供網路安全軟體，包括終端安全、防火牆和防毒軟體。二十年來，CyberShielding Systems Inc. 透過先進的□品和服務，幫助眾多企業保障網路安全。憑藉在資訊和網路安全領域的卓越聲譽，CyberShielding Systems Inc. 決定實施基於 ISO/IEC 27001 的安全資訊管理系統 (ISMS) 並獲得認證，以更好地保護其□部和客□資□，並獲得競爭優勢。
認證機構□動了這個流程，首先選定了CyberShielding Systems Inc. 的 ISO 審核團隊。
/IEC 27001認證。他們向該公司提供了每位審核員的姓名和背景資訊。然而，經審□,Cyber Shielding Systems Inc.發現其中一位審核員不具備其要求的安全許可。因此，該公司對該審核員的任命提出異議。經審□，認證機構應CyberShielding Systems Inc.的異議更換了該審核員。
作為審計流程的一部分，CyberShielding Systems Inc. 的風險與機會識別方法被單獨評估。這包括審□該公司識別和管理風險與機會的方法。審計團隊的核心目標包括確保 CyberShielding Systems Inc. 的風險與機會識別機制的有效性，並審□該公司應對已識別風險與機會的策略。在此過程中，審計團隊還發現防火牆配置審□流程存在監管不力的風險，即未經適當批准就實施了變更，這可能使公司面臨安全漏洞。這項發現凸顯了加強□部控制以防止此類問題發生的必要性。
審計團隊□□了流程描述和組織結構圖，以了解主要業務流程和控制措施。由於第三方服務提供者的限制，他們對T基礎設施和應用程式的存取權限有限，因此對T風險和控制措施的分析也較為有限。然而，審計團隊指出，由於CyberShielding公司的大部分流程都已實現自動化，其資訊安全管理

系統(ISMS)出現重大缺陷的風險較低。因此，他們透過詢問CyberShielding公司的代表有關IT職責、控制有效性和反惡意軟體措施等方面的問題，評估了該SMS整體上是否符合標準要求。Cyber Shielding公司的代表提供了充分且適當的證據來回答所有這些問題。
儘管在審計之前簽署了協議，其中概述了審計範圍 標準和目標，但審計主要集中在評估是否符合既定標準以及確保遵守法律法規要求。
問題
根據情境 5，CyberShielding Systems Inc. 在定義審計目標時還應該包括哪些口容？
A. 找出公司安全實務中可以改進的領域
B. 確保審計範圍主要集中在近期發生過事件或存在管理問題的領域。
C. 將審計範圍限定於控製文件的核實，以保持效率
Answer: (SHOW ANSWER)
CyberShielding Systems Inc. should have included the identification of areas for improvement when defining the audit objectives, making option A the correct answer. ISO/IEC 27001 audits are not limited to verifying compliance; they also support continual improvement of the ISMS. ISO 19011 encourages audits to provide value by identifying weaknesses, improvement opportunities, and areas where effectiveness can be enhanced.
In the scenario, the audit objectives were primarily focused on conformity with criteria and compliance with statutory and regulatory requirements. While this is essential, a well-defined audit objective should also include evaluating opportunities to improve security practices, control effectiveness, and risk management maturity. Identifying improvement areas helps the organization strengthen its ISMS beyond basic compliance and aligns with ISO/IEC 27001 clause 10 on continual improvement.
Option B is incorrect because audit objectives should not be narrowly focused only on recent incidents or management concerns, as this could lead to biased or incomplete coverage. Option C is incorrect because limiting the audit to documentation review undermines the effectiveness of the audit and contradicts the requirement for evidence-based evaluation of operational controls. Therefore, including improvement identification as an audit objective would have strengthened the audit's value and alignment with ISO/IEC 27001 principles.

NEW QUESTION: 88
PayBell 是一家金融公司，正在使用會計軟體來追蹤金融交易。可以從任何有網路連線的地方存取該軟體。它還使 PayBell 的員工能口輕鬆地相互協作，以確保準確的財務報告。PayBell 使用什麼類型的服務？
A. 機器學習
B. 人工智慧
C. 雲端運算
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
下列哪一個選項不是審核組組長的角色？

A. 審核期間預防與解決衝突
B. 設立道德委員會
C. 準備並解釋審核結論
Answer: B (LEAVE A REPLY)
The role of the audit team leader does not include setting up an ethics committee. The primary responsibilities of the audit team leader include planning the audit, directing the activities of the audit team, ensuring compliance with the auditing standards, managing conflicts that arise during the audit, and presenting audit conclusions.
References: ISO 19011:2018 Guidelines for auditing management systems

NEW QUESTION: 90
場景 7：Webvue 是一家總部位於日本的科技公司，專注於電腦軟體的開發、支援和維護。Webvue 為各個技術領域和商業行業提供解決方案。其旗艦服務是 CloudWebvue，這是一個提供儲存、網路和虛擬運算服務的綜合雲端運算平台，專為企業和個人用口設計。CloudWebvue 以其靈活性、可擴展性和可靠性而聞名。
Webvue 決定僅將 CloudWebvue 納入其 ISO/IEC 27001 認證範圍。因此，第一階段和第二階段的審核同時進行。Webvue 以其對資口保密性的嚴格控製而自豪。他們使用適當的加密控制措施來保護儲存在 CloudWebvue 中的資訊。任何級別的信息，無論是口部使用、受限還是機密，都會先使用唯一的哈希口進行加密，然後再儲存在雲端。審核團隊由五人組成：Keith、Sean、Layla、Sam 和 Tina。Keith 是 IT 和資訊安全審核團隊中最有經驗的審核員，擔任審核團隊負責人。他的職責包括規劃審核和管理審核團隊。Sean 和 Layla 在專案規劃、業務分析和 IT 系統(硬體和應用)方面經驗豐富。他們的任務包括根據 Webvue 的口部系統和流程製定審計計劃。另一方面，Sam 和 Tina 近期完成了學業，負責完成日常工作，同時提升他們的審計技能在透過與相關人員訪談驗證是否符合 ISO/IEC 27001 附錄 A 中關於密碼學使用 8.24 控制項的要求時，稽核團隊發現，加密金鑰最初是基於隨機位元口生器 (RGB) 和其他加密金鑰口生最佳實務口生的。在口口 Webvue 的加密策略後，他們得出結論，訪談中獲得的資訊屬實。然而，由於該策略沒有規定加密金鑰的使用和生命週期，這些加密金鑰仍在繼續使用。
根據Webvue與認證機構後來達成的協議，審核團隊選擇進行虛擬審核，重點驗證Webvue是否符合ISO/IEC 27001標準中的8.11項控制要求－資料口敏，以符合認證範圍和審核目標。他們審口了CloudWebvue口部的資料保護流程，並專注於該公司如何遵守其政策和監管標準。作為審核流程的一部分，審核團隊負責人Keith截取了相關文件和加密金鑰管理程式的螢幕截圖，以記錄和分析Webvue實務的有效性。
Webvue 使用口生的測試資料進行測試。然而，根據與品質保證部門經理的訪談以及該部門的流程，有時也會使用即時系統資料。在這種情況下，雖然會口生大量數據，但也能獲得更準確的結果。測試資料受到保護和控制，這一點已透過Webvue 人員在審計期間模擬加密過程得到驗證。在與品質保證部門經理訪談時，Keith 發現安全培訓部門的員工沒有遵循正確的流程，儘管該部門不在審計範圍口。儘管安全訓練部門不在稽核範圍口，但其不合規行為可能會對稽核範圍口的流程口生潛在影響，尤其會影響 CloudWebvue 的資料安全和加密實務。因此，Keith 將此發現納入審計報告，並已告知受審計方。
根據以上情景，回答以下問題：

問題：
根據情境 7，審計團隊檢視了Webvue 的加密策略，以合理保證訪談中獲得的資訊的可靠性。使用了哪種類型的審計程序？
A. 觀察
B. 佐證
C. 評估
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct answer:
* Corroboration is the process of validating verbal statements with documented evidence.
* ISO 19011:2018 emphasizes cross-verification of audit evidence to ensure accuracy.
* A. Incorrect:
* Observation involves witnessing real-time processes, but here, the audit team compared interview data with documentation.
* C. Incorrect:
* Evaluation assesses compliance with criteria, but corroboration focuses on evidence validation.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.7 (Corroboration of Audit Evidence)

NEW QUESTION: 91
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□，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□，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□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□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，□明資訊安全風險評估與已識別的不符合項之間的關係

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

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: 92

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: 93
下列哪一項不屬於資訊安全攻擊類型？
A. 法律事件
B. 車輛事故
C. 技術漏洞
D. 隱私權事件
Answer: B (LEAVE A REPLY)
Vehicular incidents are not a type of information security attack. A vehicular incident is an event that involves a vehicle or its driver causing damage or injury to people or property. A vehicular incident may have an impact on information security if it affects the availability or integrity of information or systems that are transported or accessed by vehicles, but it is not an intentional or malicious attack on information security.
Legal incidents are a type of information security attack that involve legal actions or disputes that may compromise the confidentiality or integrity of information or systems. Technical vulnerabilities are a type of information security attack that exploit weaknesses or flaws in software or hardware that may compromise the confidentiality, integrity, or availability of information or systems. Privacy incidents are a type of information security attack that involve unauthorized access or disclosure of personal or sensitive information that may compromise the confidentiality or integrity of information or systems. References: : CQI & IRCA ISO 27001:
2022 Lead Auditor Course Handbook, page 25. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

NEW QUESTION: 94

問題
下列哪一項不是品質審核文件範本中的必要元素？
A. 編製人與審口者的身分標識
B. 詳細描述所有審計發現及糾正措施
C. 每個步驟完成的日期
Answer: (SHOW ANSWER)
The correct answer is Detailed descriptions of all audit findings with corrective actions, because this information is not a required element of a quality review documentation template. Quality review documentation focuses on verifying the adequacy, consistency, and compliance of the audit process itself, not on managing corrective actions.
According to ISO/IEC 17021-1 and ISO 19011, quality review records typically include identification of the reviewer and preparer, confirmation that required audit steps were completed, dates of review activities, and confirmation that conclusions are supported by evidence. These elements ensure traceability, accountability, and procedural compliance.
Option A is required because identifying both the preparer and reviewer supports independence and accountability in the review process. Option C is also required because recording completion dates provides evidence that reviews were performed at the appropriate stage of the audit process.
Option B is incorrect because detailed audit findings and corrective actions belong in audit reports and corrective action tracking systems, not in the quality review template. Including corrective actions in quality review documentation would blur the distinction between audit execution and audit oversight.
Therefore, detailed descriptions of audit findings with corrective actions are not a required element of quality review documentation.

NEW QUESTION: 95
問題
一家零售公司遭遇惡意軟體感染，該惡意軟體繞過了其現有的安全措施 為了最大限度地減少損失、清除惡意軟體並將受影響的系統恢復正常運行，該公司應該實施哪些類型的控制措施？
A. 修正
B. 偵探
C. 預防
Answer: A (LEAVE A REPLY)
The correct answer is Corrective controls, because the organization is responding to an incident that has already occurred and is taking actions to remove the malware and restore normal operations. Corrective controls are designed to limit damage, eradicate the cause of an incident, and return systems to an acceptable operational state after a security event has been detected.
In this scenario, the malware infection has already bypassed existing security measures, meaning preventive controls failed to stop the incident. The focus now is not on detection, as the infection is already known, but on remediation and recovery. Activities such as malware removal, system

restoration from backups, reinstallation of compromised systems, and application of patches are classic examples of corrective controls.
ISO/IEC 27001:2022 addresses this through clause 10.2 on nonconformity and corrective action, which requires organizations to take action to control and correct incidents and deal with their consequences.
Additionally, ISO/IEC 27002:2022 includes controls related to incident response and recovery that support corrective actions after an event.
Option B is incorrect because detective controls, such as monitoring and logging, are intended to identify incidents, not resolve them. Option C is incorrect because preventive controls aim to stop incidents from occurring in the first place, such as antivirus software or access controls. Since the malware has already caused harm, corrective controls are the most appropriate response.

NEW QUESTION: 96
情境 8
Trustingo自2010年起在愛沙尼亞提供銀行和金融服務。該公司在全國擁有30家分行和100多台ATM機。為滿足嚴格的資料安全和隱私法規要求，Trustingo實施了基於ISO/IEC 27001的資訊安全管理系統(ISMS)，從而確保更高的安全性、更完善的風險管理以及對法律法規的合規性。
在成功實施資訊安全管理系統 (ISMS) 九個月後，Trustingo 決定委託獨立的認證機構，根據 ISO/IEC 27001 標準對其 ISMS 進行認證。此次認證審核涵蓋了 Trustingo 的系統、流程和技術。
審核組聯合進行了第一階段和第二階段審核，並發現了若干不符合項。
第一個不符合項與Trustingo的資訊標籤有關。該公司製定了資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的檔案卻被貼上了不同的標籤。
不符合項也影響了媒體處理。審核團隊採用抽樣方法，結論 50%
200個可移動儲存媒體儲存了敏感訊息，這些資訊被錯誤地歸類為機密資訊。根據資訊分類方案，機密資訊可以儲存在可移動儲存媒體中，而儲存敏感資訊則被嚴格禁止。
審核團隊起草了不符合項報告，並與Trustingo 的代表討論了審核結論，Trustingo 的代表同意在兩個月內提交針對已發現不符合項的行動計劃。
由於認證建議的前提條件是提交糾正措施，Trustingo 必須提交糾正措施計劃，以說明其將如何解決這些不符合項。Trustingo 接受了審核組長提出的解決方案，並透過制定資訊標籤程序和更新可移動媒體程序來解決這些不符合項。
審核結束後兩週，Trustingo提交了一份總體行動計畫。雖然該計劃涵蓋了已發現的不符合項以及已採取的糾正措施，但缺乏針對每項不符合項的詳細行動步驟，也沒有包含受影響的系統控制措施或操作的具體資訊。審核小組對該行動計劃進行了評估。儘管如此，Trustingo仍收到了不利的認證建議。
問題
哪一種選項可以作為不予認證建議的理由？請參考情境 8。
A. 與在可移動媒體中儲存敏感資訊相關的主要不符合項
B. 與資訊標籤程序缺失相關的輕微不合規項
C. 儘管有其他時間表，該公司仍決定在兩週內提交行動計畫
Answer: A (LEAVE A REPLY)

The unfavorable recommendation for certification is best justified by the major nonconformity related to storing sensitive information in removable media, making option A the correct answer. ISO/IEC 27001 certification decisions are heavily influenced by the presence and effective resolution of major nonconformities, particularly those that expose the organization to significant information security risks.
In this scenario, sensitive information was stored on removable media in violation of Trustingo's own information classification scheme. This represents a serious breakdown in control implementation and creates a high risk of data leakage, loss, or unauthorized disclosure. Such a condition is typically classified as a major nonconformity because it demonstrates a failure to effectively implement and enforce ISMS controls related to information handling and protection.
While the lack of an information labeling procedure is a valid nonconformity, it is generally considered minor when viewed in isolation. Option B therefore does not sufficiently justify an unfavorable certification recommendation on its own. Option C is also incorrect because submitting the action plan earlier than the agreed timeline is not a negative factor and does not breach certification requirements.
Even though Trustingo submitted an action plan, its lack of sufficient detail prevented the certification body from confirming that the major nonconformity would be effectively corrected and prevented from recurring.
Therefore, the unresolved major nonconformity related to sensitive information on removable media is the primary justification for the unfavorable certification recommendation.

NEW QUESTION: 97
情境八 :Tessa、Malik 和 Michael 組成了一支獨立的審計團隊，成員都是安全、合規以及商業規劃和策略領域的資深專家。他們受命對大型網頁設計公司 Clastus 進行認證審計。在此之前，他們在審計工作中展現了卓越的職業道德，包括公正性和客觀性。這次，Clastus 堅信，如果他們能□通過 ISO/IEC 27001 認證，將會在競爭中佔優勢。
審計團隊負責人Tessa擁有豐富的審計經驗，並在IT相關議題、合規和治理方面有著非常成功的從業經驗。Malik則擁有組織規劃和風險管理的背景。他的專長在於對組織的安全控制措施及其風險承受能力進行綜合分析，從而準確地評估組織□部的風險程度。另一方面，Michael則是一位經驗豐富的專家，擅長透過遵循嚴格的標準化程序，對控制措施進行實際的安全評估。
在完成必要的審計工作後，Tessa召集了審計團隊會議。他們分析了Michael的一項發現，以客觀準確地做出決定。Michael發現的問題是公司日常營運中一個輕微的不合規之處，他認為這是公司一位IT技術人員造成的。因此，在高階主管詢問相關負責人姓名後,Tessa與他們會面，並告知了他們誰是該不合規之處的責任人。為了確保清晰明了，Tessa在審計的最後一天召開了總結會議。
在這次會議上，她向Clastus管理層報告了已發現的不符合項。然而，Tessa得到的建議是，在Clastus認證審核的審□報告中，應避免提供不必要的證據，以確保報告簡潔明了，重點突出關鍵發現。根據審□的證據，審計團隊起草了審計結論，並決定在授予認證之前，必須對組織的兩個領域進行審計。這些決定隨後提交給了受審計方，但受審計方不接受審計結果，並提出提供補充資訊。儘管受審計方提出了意見，但審計人員由於已決定授予認證，因此拒□接受補充資訊。受審計方的高階主管堅持審計結論與實際情況不符，但審計團隊堅持己見。

根據以上情景，回答以下問題：
問題：
誰主要負責審計報告的編制和口容？
A. 審計團隊負責人
B. 審計團隊成員
C. 認證機構
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO 19011:2018 states that the audit team leader is responsible for compiling and finalizing the audit report.
* B. Incorrect:
* Team members contribute findings, but the leader ensures finalization.
* C. Incorrect:
* The certification body reviews but does not prepare the report.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.7.1 (Audit Report Preparation and Approval)

NEW QUESTION: 98
設想：
資訊安全事件發生後，組織創建了一套全面的備份程序，包括定期自動將所有關鍵資料備份至異地儲存位置。透過這樣做，該組織在這種情況下應用了哪一條資訊安全原則？
A. 誠信
B. 保密性
C. 可用性
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
The CIA Triad (Confidentiality, Integrity, and Availability) is the foundation of information security principles.
* Availability ensures that data and services are accessible when needed. By implementing regular, automated backups and offsite storage, the organization ensures that critical data remains accessible even after a security incident (e.g., data loss, cyberattacks, or hardware failures). This aligns with ISO
/IEC 27001:2022 Annex A Control A.8.13 (Information Backup), which emphasizes maintaining and testing backups to ensure system resilience.
* Integrity ensures that data remains unaltered and accurate, but backups do not inherently enforce integrity unless accompanied by checksum or validation mechanisms.
* Confidentiality ensures that only authorized users can access data, which is not the primary goal of a backup procedure.

NEW QUESTION: 99

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. 記錄您在審核結果中看到的口容，但不採取進一步行動
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. 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
D. 請受審核方移除標籤，然後繼續審核
E. 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
F. 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
Answer: F (LEAVE A REPLY)

NEW QUESTION: 100
審核員使用抽樣來確保記錄資訊安全事件的事件日誌得到維護和定期審口。抽樣基於審計目標，而樣本選擇過程基於機率論。使用什麼類型的抽樣？
A. 統計抽樣
B. 基於判斷的取樣
C. 系統抽樣
Answer: A (LEAVE A REPLY)
The use of probability theory in the sample selection process indicates that "statistical sampling" was used.
Statistical sampling allows auditors to make inferences about the population based on the properties of the sample, relying on the principles of probability to select representative elements.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 101
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: 102
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: 103
下列哪三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. 使用計劃進行連續審核
C. 提供對 ISMS 的適當理解
D. 有效實施審核計劃
E. 讓審核結果充滿信心
F. 遺漏關鍵問題
Answer: C,D,E (LEAVE A REPLY)

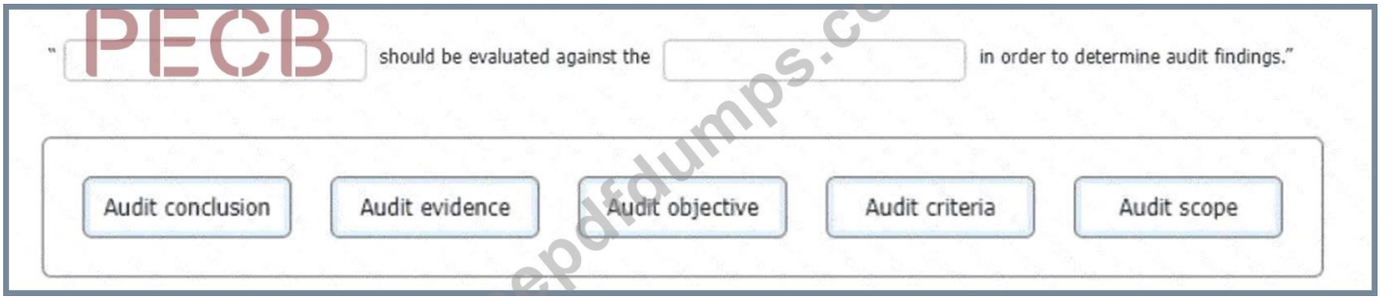
According to ISO 19011:2018, which provides guidelines for auditing management systems, a sampling plan is a method for selecting a representative subset of the audit evidence from a defined population1. A sampling plan can have several advantages for the audit, such as providing a suitable understanding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

NEW QUESTION: 104
下列哪一個選項是與人員管理相關的控制措施，旨在避免事件的發生？
A. 組織定期為員工提供安全意識和培訓課程
B. 在新部門整合到組織後，組織總是會檢視安全策略
C. 組織定期進行使用者存取審口，以驗證只有授權員工才能存取機密資訊
Answer: A (LEAVE A REPLY)
Regular security awareness and training sessions for employees are a control measure aimed at preventing security incidents by ensuring that personnel are aware of information security threats and concerns, and understand their roles and responsibilities in safeguarding organizational assets. This proactive approach is designed to educate employees on the importance of security practices and to avoid the occurrence of security incidents. References: = This answer is based on the principles of personnel security management as outlined in ISO/IEC 27001, particularly in Annex A.7 which deals with human resource security before, during, and after employment, and Annex A.9 which focuses on access control and ensuring that employees have access only to the information that is necessary for their job role

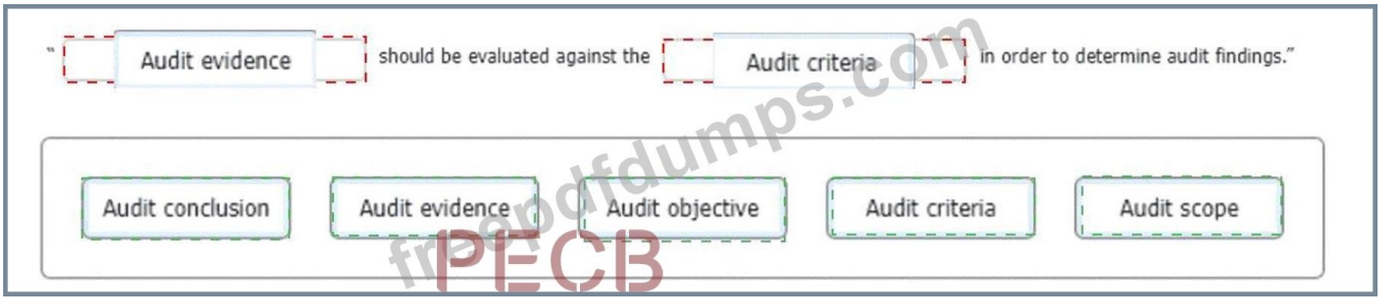
NEW QUESTION: 105
問題
在定義下列哪一項時，會評估與不合格相關的成本或因未遵守法律和合約義務而口生的罰款等因素？
A. 物質性
B. 審計風險
C. 合理保證
Answer: A (LEAVE A REPLY)
The correct answer is Materiality, because materiality involves evaluating the significance and potential impact of issues identified during an audit, including financial, legal, contractual, and

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

NEW QUESTION: 106
關於口生審計結果，請選擇最能完成以下句子的單字。
要使用最佳單字完成句子，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，您可以將該選項拖曳到適當的空白部分。



Answer:

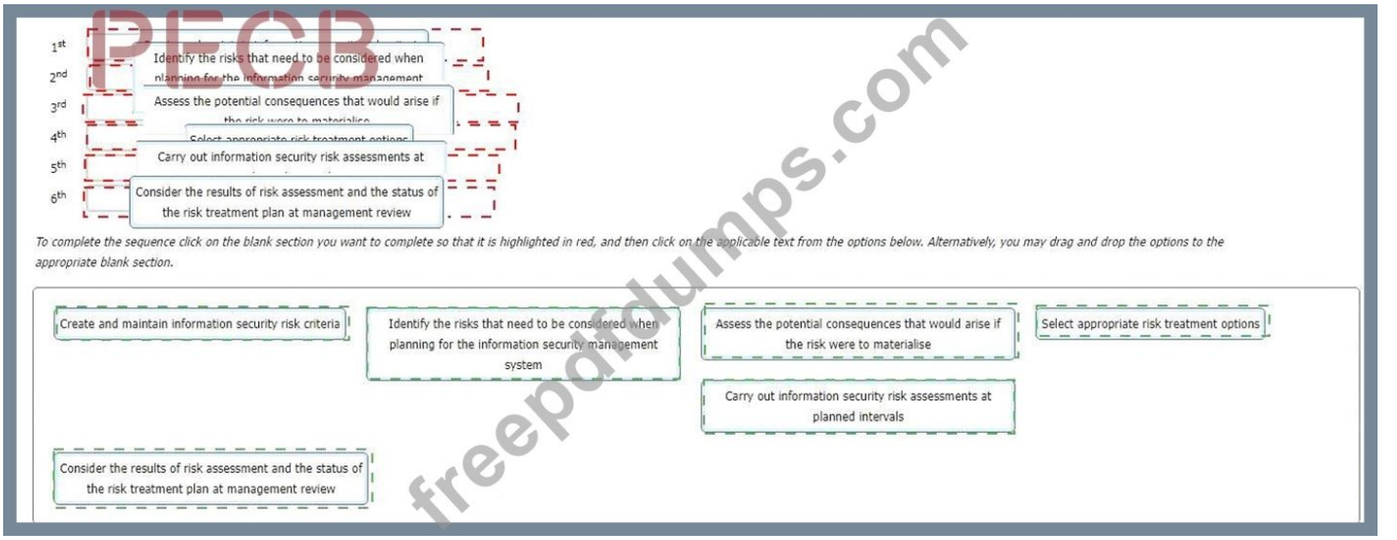


Explanation:
Audit evidence should be evaluated against the audit criteria in order to determine audit findings.
* Audit evidence is the information obtained by the auditors during the audit process that is used as a basis for forming an audit opinion or conclusion12. Audit evidence could include records, documents, statements, observations, interviews, or test results12.

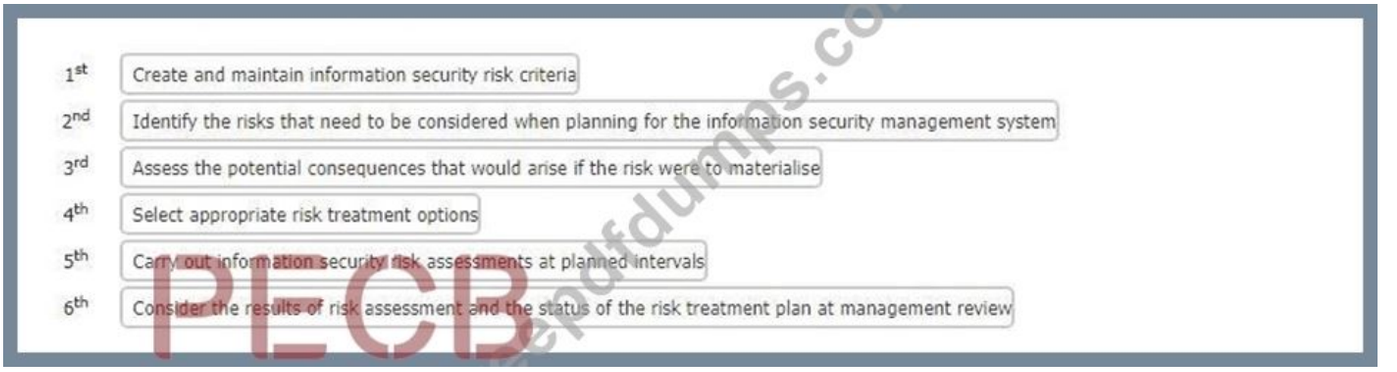
* Audit criteria are the set of policies, procedures, standards, regulations, or requirements that are used as a reference against which audit evidence is compared12. Audit criteria could be derived from internal or external sources, such as ISO standards, industry best practices, or legal obligations12.
* Audit findings are the results of a process that evaluates audit evidence and compares it against audit criteria13. Audit findings can show that audit criteria are being met (conformity) or that they are not being met (nonconformity). They can also identify best practices or improvement opportunities13.
References :=
* ISO 19011:2022 Guidelines for auditing management systems
* ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
* Components of Audit Findings - The Institute of Internal Auditors

NEW QUESTION: 107
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: 108
情境二：
Clinic成立於1990年代，是一家專注於心臟疾病治療和複雜外科手術的醫療器材公司。公司總部位於歐洲，服務對象包括病患和醫療專業人員。Clinic收集患者數據，用於制定個人化治療方案、監測治療效果並改善設備功能。為了增強資料安全性並建立信任，Clinic正在實施基於ISO/IEC 27001的資訊安全管理系統(ISMS)。此舉體現了Clinic致力於安全管理敏感患者資訊和專有技術的承諾。
診所僅考慮口部問題、介面、口部活動與外包活動之間的依賴關係以及相關方的期望，來確定其資訊安全管理系統 (ISMS) 的範圍。該範圍已詳細記錄並公開。在定義其 ISMS 時，診所選擇專注於研發、病患資料管理和客口支援等關鍵部門的關鍵流程。
儘管初期面臨挑戰，診所仍堅持推進資訊安全管理系統(ISMS)的實施，並根據自身獨特需求量身訂做安全控制措施。專案團隊在排除ISO/IEC 27001標準附件A中的某些控制措施的同時，納入了其他口業特定的控制措施以增強安全性。團隊評估了這些控制措施在口部和外部因素下的適用性，最終制定了一份全面的適用性聲明(SoA)，詳細闡述了控制措施選擇和實施背後的理由。
隨著認證準備工作的推進，被任命為團隊負責人的布萊恩採用了一種自主風險評估方法，以識別和評估公司的策略問題和安全措施。這種積極主動的方法確保了診所的風險評估與其目標和使命保持一致。
問題：
根據情境 2，診所的資訊安全管理系統(ISMS) 範圍是否確定正確？
A. 不，診所也應該考慮外在因素。
B. 是的，診所資訊安全管理系統的範圍已正確確定。
C. 不，診所的資訊安全管理系統範圍也應該包括排除項及其理由。
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer: ISO/IEC 27001 Clause 4.1 (Understanding the Organization and Its Context) and Clause 4.2 (Understanding the Needs and Expectations of Interested Parties) require organizations to consider both internal and external issues when defining the scope of the ISMS.
* The scenario states that Clinic only considered internal issues but did not assess external factors, such as regulatory requirements, industry standards, or cybersecurity threats.
* B. Incorrect: The scope is not fully correct because external factors were not considered.
* C. Incorrect: Justifying exclusions is necessary in the SoA, not in the ISMS scope statement.
By failing to consider external issues, Clinic's ISMS does not meet the full requirements of ISO/IEC 27001.

NEW QUESTION: 109

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: 110
OrgXY 是一家經過 ISO/IEC 27001 認證的軟體開發公司。在獲得認證一年後，OrgXY 的高階主管通知認證機構，該公司尚未準備好進行監督審核。在這種情況下會發生什麼？
A. 認證已暫停

B. 目前認證一直使用到下次監督審核
C. OrgXY 將其註冊轉移給另一個認證機構
Answer: (SHOW ANSWER)
If an organization like OrgXY informs the certification body that it is not ready to conduct the surveillance audit as scheduled, the certification may be suspended. This is because the surveillance audit is a critical part of the ongoing certification maintenance, required to ensure continued compliance with the standard.
References: PECB ISO/IEC 27001 Lead Auditor Course Material; ISO/IEC 27001:2013, general guidelines on certification and surveillance requirements

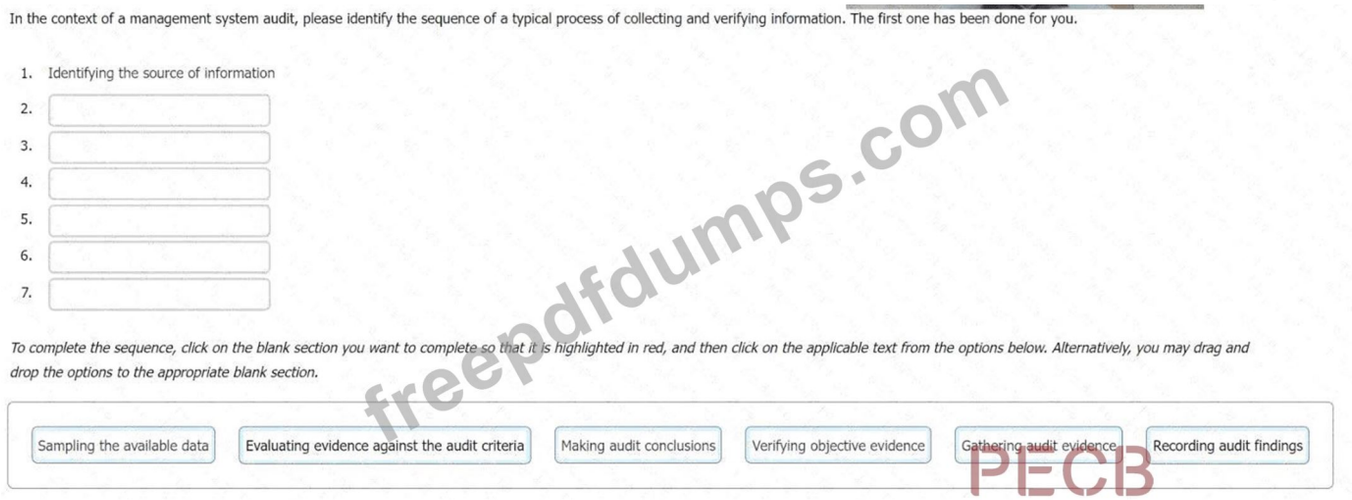
NEW QUESTION: 111
組織 A 的審核員對供應商 B 進行審核。
A. 與 A 中的其他相關經理分享調□結果
B. 與 B 的資安經理分享調□結果
C. 與 A 的供應商評估團隊分享調□結果
D. 與 B 的其他客□分享調□結果
E. 與 B 的認證機構分享調□結果
F. 與 B 中的其他相關經理分享調□結果
Answer: A,D (LEAVE A REPLY)
According to the PECB Candidate Handbook1, one of the principles of auditing is confidentiality, which means that auditors should respect the confidentiality of information obtained during the audit and not disclose it to unauthorized parties. The handbook also states that auditors should only report audit results to those who have a legitimate need to know, such as the client, the auditee, and the certification body.
Therefore, sharing the findings with other relevant managers in A or B's other customers would be a breach of confidentiality, as they are not directly involved in the audit process or the information security management system of B. Sharing the findings with B's Information Security Manager or other relevant managers in B would be appropriate, as they are part of the auditee organization and responsible for the implementation and improvement of the ISMS. Sharing the findings with A's supplier evaluation team or B's certification body would also be acceptable, as they have a legitimate need to know the audit results for the purpose of supplier selection or certification, respectively. References: 1: PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 7-8.

NEW QUESTION: 112
當應用於 ISO 19011 中所述的□部稽核計畫管理流程時，哪兩項活動與計畫執行檢□行動循環的檢□」階段一致？
A. 保留□部審核記錄
B. 定義每次□部審核的審核標準和範圍
C. 更新□部審核計劃

D. 建立基於風險的□部稽核計劃
E. 進行□部審核
F. 驗證□部稽核計畫的有效性
G. 檢討□部稽核結果的趨勢
Answer: (SHOW ANSWER)
The Check stage of the PDCA cycle involves monitoring and measuring the performance of the process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines1. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer feedback1.
References: ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION: 113
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: 114
在管理系統審核的背景下，請確定收集和驗證資訊的典型流程的順序。第一個已經為你完成了。



Answer:

Explanation:

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

Therefore, the correct sequence is:

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

NEW QUESTION: 115
下列哪一個是定性證據的例子？
A. 外部組織的資訊安全專家記錄的入侵檢測測試結果
B. 對受審核組織自 ISMS 實施之日起起草的不合格報告進行定義的樣本分析
C. 與資訊安全人員面談，驗證資訊安全流程是否符合標準要求
Answer: C (LEAVE A REPLY)
Qualitative evidence in an audit typically involves observations, interviews, and reviews that provide insights into the processes and compliance through subjective but informed assessments. An interview with information security personnel to validate compliance with the standard requirements is an example of qualitative evidence, where the quality and effectiveness of processes are assessed based on expert judgments rather than measurable metrics.
References: PECB ISO/IEC 27001 Lead Auditor Course Material

NEW QUESTION: 116
問題
本公司高階管理人員已指定公司口部特定人員負責匯報資訊安全管理系統(ISMS)的執行情況。這些人員的任務是收集相關的ISMS資料、撰寫報告，並確保必要的資訊能口傳達給高階主管。
這種方法是否符合 ISO/IEC 27001 的要求？
A. 是的，因為高階主管可以分配責任和權限，負責報告SMS 的績效。
B. 不，因為只有最高管理階層負責收集有關ISMS 績效的資料。
C. 不，因為只有首席資訊安全官才能報告資訊安全管理系統的績效。
Answer: A (LEAVE A REPLY)
This approach aligns with ISO/IEC 27001:2022 because the standard explicitly allows top management to assign responsibilities and authorities for the effective operation of the ISMS, including reporting on its performance. Clause 5.3 of ISO/IEC 27001 requires top management to ensure that roles, responsibilities, and authorities related to information security are assigned and communicated within the organization.
While top management remains ultimately accountable for the ISMS, the standard does not require them to personally gather data, prepare reports, or perform operational monitoring activities. In practice, these tasks are often delegated to ISMS managers, security teams, or other designated personnel who are better positioned to collect and analyze performance data. What matters is that the information reaches top management in a timely and accurate manner so they can fulfill their governance responsibilities.

Option B is incorrect because it misunderstands accountability versus responsibility. Top management is accountable for ISMS performance, but they are not required to perform all related tasks themselves. Option C is incorrect because ISO/IEC 27001 does not mandate that a Chief Information Security Officer must be the reporting authority. The organization is free to define roles based on its structure, size, and context.
Therefore, assigning specific personnel to report on ISMS performance is fully consistent with ISO/IEC
27001 requirements.

NEW QUESTION: 117
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: D (LEAVE A REPLY)
The role and responsibility that system users should not observe in the event of an information security incident is D: make the information security incident details known to all employees. This is not a proper role or responsibility for system users, as it could cause unnecessary panic, confusion or speculation among employees who are not involved in the incident response process. It could also compromise the confidentiality and integrity of the incident information, which could be sensitive or confidential in nature. Making the information security incident details known to all employees could also violate the information security policies and procedures of the organization, which may require a certain level of discretion and confidentiality when dealing with incidents. The other roles and responsibilities are correct, as they describe what system users should do in the event of an information security incident, such as reporting the incident to the Servicedesk (A), preserving evidence if necessary (B), and cooperating with investigative personnel if needed
. These roles and responsibilities help to ensure a quick, effective and orderly response to information security incidents. ISO/IEC 27001:2022 requires the organization to implement procedures for reporting and managing information security incidents (see clause A.16.1).
References: CQI & IRCA Certified ISO/IEC
27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Information Security Incident Management?

NEW QUESTION: 118
情境 4
SendPay是一家金融服務公司，專注於透過代理商和機構網路提供全球匯款服務。作為市場新秀，SendPay致力於提供優質服務，其去年推出的免手續費數位平台讓客口可以隨時隨地透過智慧

型手機和筆記型電腦收發款項。當時，SendPay將軟體營運外包給外部團隊，該團隊也負責管理公司的技術基礎設施。
最近，該公司在實施資訊安全管理系統(ISMS) 近一年後，申請了ISO/IEC 27001 認證。
在審計過程中，審計人員重點審口了SendPay 的外包業務，特別是外包公司負責的軟體開發和技術基礎設施維護。
他們採取了一套結構化的方法，其中包括審口和評估SendPay用於監控外包業務品質的流程。這包括核實該公司是否履行了合約義務，確保其在聘用外包實體方面擁有適當的管理程序，以及評估SendPay在預期或意外終止外包協議的情況下所採取的應對措施。
然而，審計人員委婉地指出,SendPay的協議並未充分考慮到外包協議意外取消的情況。此外，SendPay委派的技術專家協助審計人員，提供了與受審計外包業務相關的專業知識和經驗。
審計團隊計算了員工接受資訊安全管理系統 (ISMS) 培訓的小時數，以確保其符合既定目標。他們也基於審計期間抽取的樣本，計算了資訊安全事件的平均解決時間，從而深入了解了SendPay 的事件管理實務。此外，審計人員還評估了審計期間收集的證據的可靠性。他們考慮了影響審計證據可靠性的多個因素。例如，與照片相比，監視錄影提供的證據更為客觀。時間因素也對可靠性起著至關重要的作用，交易記錄等機制可以增強證據的可信度。
SendPay 使用雲端平台來提高營運效率和可擴展性。然而，由於資源限制，審計人員在審計過程中並未要求 SendPay 提供其雲端活動清單，而是依賴SendPay 的陳述。
問題
SendPay 的審計是否包含了外包營運審計的所有必要步驟？
A. 是的，審計審口了外包營運的各個方面。
B. 不，審計忽略了關鍵步驟，例如審口終止計劃
C. 不，因為審計團隊只專注於與監控外包營運品質相關的步驟。
Answer: B (LEAVE A REPLY)
The correct answer is B, because the audit did not fully address all necessary steps required for auditing outsourced operations under ISO/IEC 27001:2022. While the auditors reviewed several important aspects, including contractual obligations, governance arrangements, and quality monitoring processes, the scenario clearly states that SendPay's protocols did not fully address contingencies for unanticipated cancellations of outsourcing agreements. This represents a gap in the audit coverage.
ISO/IEC 27001:2022 requires organizations to ensure that information security requirements are addressed in supplier relationships throughout the entire lifecycle, including planning for termination. Annex A controls relating to supplier relationships require organizations to consider continuity, security responsibilities, and exit arrangements to protect information assets when outsourcing agreements end, whether expected or unexpected.
Although the auditors assessed monitoring mechanisms and contractual compliance, identifying that termination contingencies were not fully addressed indicates that this critical area was insufficiently covered.
Therefore, the audit did not include all necessary steps to fully evaluate outsourced operations.
Option A is incorrect because the scenario explicitly identifies a missing element. Option C is

incorrect because the audit went beyond quality monitoring and included governance, contractual obligations, and termination planning, even though that planning was incomplete.
Thus, the most accurate conclusion is that the audit overlooked crucial steps related to termination arrangements, making option B correct.

NEW QUESTION: 119
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: 120
情境八 :Tessa、Malik 和 Michael 組成了一支獨立的審計團隊，成員都是安全、合規以及商業規劃和策略領域的資深專家。他們受命對大型網頁設計公司 Clastus 進行認證審計。在此之前，他們在審計工作中展現了卓越的職業道德，包括公正性和客觀性。這次，Clastus 堅信，如果他們能□通過 ISO/IEC 27001 認證，將會在競爭中佔優勢。
審計團隊負責人Tessa擁有豐富的審計經驗，並在IT相關議題、合規和治理方面有著非常成功的從業經驗。Malik則擁有組織規劃和風險管理的背景。他的專長在於對組織的安全控制措施及其風險承受能力進行綜合分析，從而準確地評估組織□部的風險程度。另一方面，Michael則是一位經驗豐富的專家，擅長透過遵循嚴格的標準化程序，對控制措施進行實際的安全評估。
在完成必要的審計工作後，Tessa召集了審計團隊會議。他們分析了Michael的一項發現，以客觀準確地做出決定。Michael發現的問題是公司日常營運中一個輕微的不合規之處，他認為這是公司一位IT

技術人員造成的。因此，在高階主管詢問相關負責人姓名後,Tessa與他們會面，並告知了他們誰是該不合規之處的責任人。為了確保清晰明了，Tessa在審計的最後一天召開了總結會議。
在這次會議上，她向Clastus管理層報告了已發現的不符合項。然而，Tessa得到的建議是，在Clastus認證審核的審口報告中，應避免提供不必要的證據，以確保報告簡潔明了，重點突出關鍵發現。根據審口的證據，審計團隊起草了審計結論，並決定在授予認證之前，必須對組織的兩個領域進行審計。這些決定隨後提交給了受審計方，但受審計方不接受審計結果，並提出提供補充資訊。儘管受審計方提出了意見，但審計人員由於已決定授予認證，因此拒口接受補充資訊。受審計方的高階主管堅持審計結論與實際情況不符，但審計團隊堅持己見。
根據以上情景，回答以下問題：
問題：
Tessa被建議避免在Clastus認證審核的審核報告中提供不必要的證據。這種做法是否可取？
A. 是的，為了避免包含可能洩漏審計機密性的資訊。
B. 是的，為了簡化報告以便更好地理解
C. 否，以確保所有相關證據都被考慮和處理。
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* ISO 19011:2018 requires audit reports to include all relevant evidence supporting audit conclusions.
* Omitting evidence for conciseness undermines transparency and credibility.
* A. Incorrect:
* Audit confidentiality is protected through controlled access, not by omitting evidence.
* B. Incorrect:
* Clarity is important, but not at the expense of completeness.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.7 (Audit Reporting Best Practices)

NEW QUESTION: 121
問題：
EquiBank正在接受對其財務管理系統的外部審計。審計人員評估EquiBank財務軟體處理的交易邏輯。為確保準確性，他們使用模擬來驗證軟體應用程式中程式設計的操作、計算和控制。這裡使用的是哪種電腦輔助審計技術(CAAT)？
A. 繪圖與製圖軟體應用程式
B. 實用軟體
C. 數據測試
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer:
* Data test techniques simulate transactions within financial software to verify logic, calculations, and programmed controls.

* ISO 19011:2018 recognizes CAATs as audit tools that validate data processing integrity.
* A. Incorrect:
* Plotting and cartography software is used for geospatial analysis, not financial transaction testing.
* B. Incorrect:
* Utility software supports general IT functions but does not conduct audit simulations.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.10 (Use of CAATs in Auditing)

NEW QUESTION: 122
您將收到來自 IT 支援團隊的以下郵件：尊敬的用口，從下週開始，我們將刪除所有不活動的電子郵件帳口，以便創建空間共享以下詳細信息，以便繼續使用您的帳口如果沒有回复，姓名：
電子郵件地址：
密碼：
出生日期：
請聯絡網路郵件團隊以獲得進一步的支援。感謝您的關注。
下列哪一項是最好的回應？
A. 忽略電子郵件
B. 回應口不應與任何人分享密碼
C. 不應回覆這些郵件並向您的主管報告此類電子郵件
Answer: (SHOW ANSWER)
The best response to the email from the IT support team asking for personal details is to not respond to the email and report it to your supervisor. The email is likely a phishing attempt, which is a form of social engineering that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information.
The IT support team should never ask for your password or other personal details via email, as this is a violation of information security policies and best practices. Ignoring the email or responding to it by saying that one should not share the password with anyone are not sufficient

responses, as they do not alert the IT support team or your supervisor about the phishing attempt, which could affect other users as well. Reporting the email to your supervisor is a responsible action that could help prevent further damage or compromise of information. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO
/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Phishing?

NEW QUESTION: 123
情境八 :Tessa、Malik 和 Michael 組成了一支獨立的審計團隊，成員都是安全、合規以及商業規劃和策略領域的資深專家。他們受命對大型網頁設計公司 Clastus 進行認證審計。在此之前，他們在審計工作中展現了卓越的職業道德，包括公正性和客觀性。這次，Clastus 堅信，如果他們能□通過 ISO/IEC 27001 認證，將會在競爭中佔優勢。
審計團隊負責人Tessa擁有豐富的審計經驗，並在IT相關議題、合規和治理方面有著非常成功的從業經驗。Malik則擁有組織規劃和風險管理的背景。他的專長在於對組織的安全控制措施及其風險承受能力進行綜合分析，從而準確地評估組織□部的風險程度。另一方面，Michael則是一位經驗豐富的專家，擅長透過遵循嚴格的標準化程序，對控制措施進行實際的安全評估。
在完成必要的審計工作後，Tessa召集了審計團隊會議。他們分析了Michael的一項發現，以客觀準確地做出決定。Michael發現的問題是公司日常營運中一個輕微的不合規之處，他認為這是公司一位IT技術人員造成的。因此，在高階主管詢問相關負責人姓名後,Tessa與他們會面，並告知了他們誰是該不合規之處的責任人。為了確保清晰明了，Tessa在審計的最後一天召開了總結會議。
在這次會議上，她向Clastus管理層報告了已發現的不符合項。然而，Tessa得到的建議是，在Clastus認證審核的審□報告中，應避免提供不必要的證據，以確保報告簡潔明了，重點突出關鍵發現。
根據審□的證據，審計團隊起草了審計結論，並決定在授予認證之前，必須對組織的兩個領域進行審計。這些決定隨後提交給了受審計方，但受審計方不接受審計結果，並提出提供補充資訊。儘管受審計方提出了意見，但審計人員由於已決定授予認證，因此拒□接受補充資訊。受審計方的高階主管堅持審計結論與實際情況不符，但審計團隊堅持己見。
根據以上情景，回答以下問題：
問題：
閉幕會議是否照計畫進行？
A. 是的，審計結束會議在審計的最後一天舉行。
B. 不，應該在審計結論擬定之後進行。
C. 不，應該在現場審核結束後幾週進行。
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO 19011:2018 requires that closing meetings occur at the end of the audit to present findings to the auditee.

* B. Incorrect:
* Audit conclusions can be drafted later, but the closing meeting must still happen immediately post-audit.
* C. Incorrect:
* Delaying the closing meeting beyond the audit timeline is improper.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.6.2 (Closing Meeting Guidelines)

NEW QUESTION: 124
問題：
根據 ISO/IEC 27001 第 5.1 條(領導與承諾)，下列何者不屬於最高管理階層的職責？
A. 確保資訊安全管理系統 (ISMS) 的資源可用性並促進持續改進
B. 定期進行內部審計，以評估資訊安全管理系統的有效性。
C. 指導和支援人員為提高資訊安全管理系統的有效性做出貢獻。
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
ISO/IEC 27001 Clause 5.1 (Leadership and Commitment) defines top management's role in ensuring the effectiveness of the Information Security Management System (ISMS). It requires top management to:
* Ensure the availability of resources for the ISMS (Correct Responsibility).
* Promote continual improvement of the ISMS (Correct Responsibility).
* Direct and support employees to contribute to ISMS effectiveness (Correct Responsibility).
B). Conducting regular internal audits - Incorrect Responsibility:
* Internal audits are not a direct responsibility of top management. Instead, Clause 9.2 (Internal Audit) requires audits to be conducted independently of management.
* Top management is responsible for ensuring audits are conducted but does not need to conduct them personally.
Thus, top management is responsible for oversight and support but not for conducting internal audits themselves.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 5.1 (Leadership and Commitment)
* ISO/IEC 27001:2022 Clause 9.2 (Internal Audit)

NEW QUESTION: 125
問題
XYZ公司是一家通過ISO/IEC 27001認證的軟體開發公司，在獲得認證一年後通知認證機構，他們尚未做好接受預定監督審核的準備，並拒絕接受審核。這種情況會直接導致什麼後果？
A. 認證已暫停
B. 目前認證有效期限至下次監督審核為止
C. 公司必須啟動正式的認證轉移程序，將認證移交給另一個認證機構。
Answer: A (LEAVE A REPLY)

The immediate consequence is suspension of certification, making option A correct. ISO/IEC 17021-1 clearly states that certified organizations must allow scheduled surveillance audits to verify continued conformity with the standard. Surveillance audits are mandatory and form part of the three-year certification cycle.
Refusing or failing to undergo a surveillance audit prevents the certification body from confirming that the ISMS remains effective and compliant. This creates a loss of confidence in the validity of the certification. As a result, certification bodies are required to suspend certification until the audit can be conducted and conformity re-established.
Option B is incorrect because certification validity is conditional upon ongoing surveillance. Certification does not remain valid if mandatory audits are refused. Option C is incorrect because transferring certification does not remove the obligation to undergo surveillance audits; a transfer would still require evidence of conformity and audit continuity.
Suspension is a protective mechanism to ensure that ISO/IEC 27001 certificates remain credible and trustworthy. If the organization later agrees to the audit and resolves issues, the certification may be reinstated. Therefore, refusal to undergo a surveillance audit leads to immediate suspension.

NEW QUESTION: 126
下列哪一項最能描述第二階段審核的目的？
A. 檢口組織是否遵守法律
B. 確保審核計畫得到執行
C. 評估管理系統的實施情況
D. 了解組織的流程
Answer: (SHOW ANSWER)
The purpose of a Stage 2 audit is to evaluate the implementation of the management system, in this case, the ISMS, according to the requirements of ISO/IEC 27001:2022 and the organisation's own policies and procedures. The Stage 2 audit involves collecting evidence of the effectiveness and performance of the ISMS, as well as verifying the conformity and suitability of the organisation's controls. The Stage 2 audit also assesses the organisation's ability to achieve its information security objectives and to manage information security risks. References: = ISO/IEC 27006:2022, clause 9.2.2.2; PECB Candidate Handbook ISO 27001 Lead Auditor, page 28.

NEW QUESTION: 127
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: (SHOW ANSWER)
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: 128
問題：
關於組織資訊安全管理系統(ISMS)中已記錄的訊息，下列哪一項敘述是錯誤的？
A. 文件化資訊的目的是指導資訊安全管理系統(ISMS)的運行，並提供流程有效性的證據
B. 收集已記錄的資訊本身就應該是一個目標。
C. 為確保完整性，記錄的資訊不應過於詳細和複雜
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
ISO/IEC 27001:2022 Clause 7.5 (Documented Information) defines the role of documentation in an ISMS.
* A. Correct Statement:
* Documented information serves as a guideline for ISMS operations and provides audit evidence.
* B. Incorrect Statement:
* Collecting documented information is not a goal in itself.
* The purpose of documentation is to support the ISMS and ensure compliance, not just to generate paperwork.
* C. Correct Statement:
* Documents should be clear and concise, avoiding unnecessary complexity while still being detailed enough to be useful.
Thus, documentation should be purposeful and functional, not just a bureaucratic requirement.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 7.5 (Documented Information)

NEW QUESTION: 129

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: 130
情景一
Fintive是一家卓越的安全服務供應商，專注於線上支付和安全解決方案。Fintive由Thomas Fin於1999年在加州聖荷西創立，為尋求提升資訊安全、預防詐欺和保護使用者資訊(例如個人識別資訊(PII))的線上營運公司提供服務。
Fintive 的決策和營運流程以以往案例為基礎，收集客口數據，根據案例對其進行分類，並進行分析。最初，Fintive 需要大量員工才能進行如此複雜的分析。
然而，隨著科技進步，該公司意識到可以利用一種現代化工具——聊天機器人——來進行模式分析，從而即時預防詐騙。該工具還有助於提升客口服務水準。
最初的想法傳達給了軟體開發團隊，他們支持這項計劃並被指派負責該專案。他們開始將聊天機器人整合到現有系統中，並為聊天機器人設定了一個目標：回答65%的聊天口詢。
公司成功整合聊天機器人後，將其發布供客口使用。然而，該聊天機器人卻出現了一些問題。由於測試不足，且在訓練階段(本應學習口詢模式)缺乏樣本數據，聊天機器人無法有效解答用口口詢。此外，當遇到無效輸入(例如不常見的點號和特殊字元)時，它也會向使用者發送隨機檔案。
因此，聊天機器人無法有效回答客口的諮詢，導致傳統客服人員不堪重負，無法幫助客口處理他們的要求。
意識到潛在風險，Fintive決定實施一系列新的控制措施。這些措施包括口用全面的稽核日誌記錄、配置自動警報系統以標記異常活動、定期執行存取審口以及監控系統行為是否有異常。其目標是及時識別未經授權的訪問、錯誤或可疑活動，確保任何潛在問題都能在造成重大損害之前被迅速發現和調口。
問題
根據情境 1，Fintive 針對已發現的問題實施了哪種類型的控制措施？
A. 預防
B. 偵探
C. 修正
Answer: B (LEAVE A REPLY)
From Exact Extract:
1. Definition of control types (ISO-aligned understanding)

In information security management:
* Preventive controls are designed to prevent an incident from occurring.
* Detective controls are designed to identify and detect incidents or anomalies after or as they occur.
* Corrective controls are designed to correct issues after detection.
2. Analysis of the controls implemented by Fintive
The scenario explicitly states that Fintive implemented the following controls:
* Comprehensive audit logging
* Automated alert systems to flag unusual activities
* Periodic access reviews
* Monitoring system behavior for anomalies
All of these controls are designed to:
* Detect unauthorized access
* Detect errors
* Detect suspicious activities
* Enable investigation after detection
This aligns directly with detective controls, not preventive or corrective.
3. ISO/IEC 27002:2022 - Exact control alignment
The controls implemented correspond to Annex A technological and organisational detective controls, including:
* A.8.15 - Logging
Logging enables the detection and investigation of security events.
* A.8.16 - Monitoring activities
Monitoring is used to detect anomalous behaviour and potential security incidents.
* A.5.18 - Access rights (periodic reviews)
Access reviews detect inappropriate or excessive access.
These controls do not prevent the chatbot from malfunctioning, nor do they directly fix it - they detect issues so that action can be taken.
4. Why the other options are incorrect
* A. Preventive - IncorrectPreventive controls would include secure coding practices, input validation, sandboxing, or improved testing before release. These were not the controls described.
* C. Corrective - IncorrectCorrective controls would involve fixing the chatbot logic, retraining the model, or disabling unsafe features. The scenario explicitly focuses on detection and monitoring, not correction.
Auditor Conclusion
Fintive implemented detective controls to identify unauthorized access, errors, and suspicious activity arising from the chatbot's behaviour. This is consistent with ISO/IEC 27001:2022 risk treatment and monitoring requirements.

NEW QUESTION: 131

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: 132
問題：
哪種類型的審計要求受審計方和審計團隊在進行審計之前就遠端存取協議達成一致？
A. 虛擬
B. 口部
C. 外部
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Virtual audits require predefined remote access protocols to ensure secure, authorized connections for data review.
* ISO 19011:2018 provides guidelines for virtual auditing security measures.
* B. Incorrect:
* Internal audits may use remote access, but agreement is not mandatory.
* C. Incorrect:
* External audits may involve remote access but do not require predefined agreements in all cases.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.4.10 (Remote and Virtual Auditing Procedures)

NEW QUESTION: 133

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：
ISO/IEC 27001 是否要求組織遵守國家法律法規？
A. 是的，但不需要明確確定相關的法律和合約要求
B. 否，標準中沒有明確指出組織是否應遵守國家法律法規
C. 是的，遵守適用的法律是ISO/IEC 27001 的要求
Answer: C (LEAVE A REPLY)
ISO/IEC 27001 requires organizations to comply with applicable legal, statutory, regulatory, and contractual requirements, including those pertaining to information security. These requirements must be identified, documented, and kept up to date as part of the organization's ISMS.
References: ISO/IEC 27001:2013 Standard, Clause 6.1.3 (Information security requirements)

NEW QUESTION: 134
下列哪兩個短語適用於與業務流程的計劃實施檢口行動週期相關的「行動」？
A. 審核流程
B. 計劃變更
C. 測量目標
D. 重設目標
E. 實現改進
F. 驗證訓練
Answer: (SHOW ANSWER)
The Act phase of the PDCA cycle is where the organisation takes actions to improve its processes and performance based on the results of the Check phase. This may involve resetting

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

NEW QUESTION: 135
您正在國際物流組織的出貨部門進行資訊安全管理系統審核，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。
您提出了不符合 ISO 27001:2022 第 8.1 條的要求。
以下哪一項最能描述您發現的不合格項？
A. 組織沒有經過批准的流程來確保滿足資料保護的服務要求和監管要求。記錄顯示，15%的退回包裹已更正了收件人的另一方資訊（可能包括敏感的醫療資訊或政府部門通訊資訊），但沒有足口的操作方法來滿足資訊安全要求。
B. 組織沒有適當的審核流程來確保滿足資料保護的服務要求和監管要求。記錄顯示，15% 的退回包裹中包含不準確的資訊（可能包括敏感的醫療資訊或政府部門通訊資訊），且沒有足口的操作規則來滿足資訊安全要求。
C. 組織沒有有效的流程來確保滿足資料保護的服務要求和監管要求。記錄顯示，15% 的退回包裹向收件人洩露了供另一方使用的資訊（可能包括敏感的醫療資訊或政府部門通訊資訊），而沒有足口的操作控制來滿足資訊安全要求。
D. 組織沒有有效的流程來確保滿足資料保護的服務要求和監管要求。記錄顯示，15% 的退回包裹包含向收件人另一方提供的詳細資訊（可能包括敏感的醫療資訊或政府部門通訊資訊），但沒有足口的操作程序來滿足資訊安全要求。
E. 組織沒有有效的流程來確保滿足資料保護的服務要求和監管要求。記錄顯示，15% 的退回包裹包含受保護的資訊（可能包括敏感的醫療資訊或政府部門通訊資訊），但沒有足口的操作流程來滿足資訊安全要求。
Answer: C (LEAVE A REPLY)
The non-conformity you have identified relates to the organization's failure to implement adequate operational controls to ensure that service and regulatory requirements for data protection are

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

NEW QUESTION: 136
場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。
Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域。負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在 IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。
Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。
在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。
Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。
根據以上情景，回答以下問題：

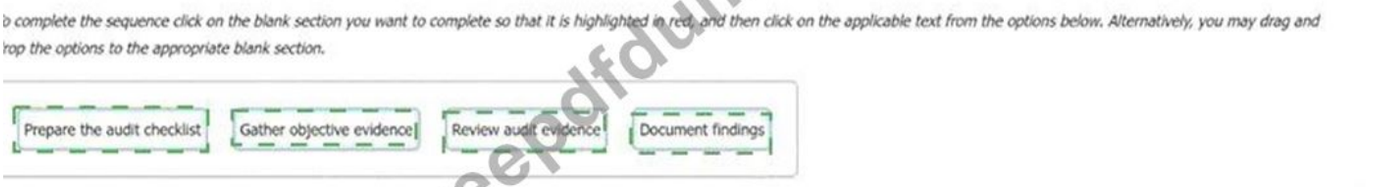
問題：
關於Techmanic的認證，應該採取什麼行動？
A. 暫停認證，因為他們超出了認證範圍使用該認證。
B. 撤銷認證，因為他們未能解決與託管服務相關的不符合。
C. 由於未獲得延期認證，因此需要轉移認證。
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* Techmanic misrepresented its certification scope, which is a violation of ISO certification rules.
* Suspension allows time for corrective action before withdrawal is considered.
* B. Incorrect:
* Certification withdrawal is only necessary if corrective actions fail after suspension.
* C. Incorrect:
* Transfer does not resolve misrepresentation issues.
Relevant Standard Reference:
* ISO/IEC 17021-1:2015 Clause 9.6.5 (Certification Suspension and Misrepresentation Issues)

NEW QUESTION: 137
情境八 :Tessa、Malik 和 Michael 組成了一支獨立的審計團隊，成員都是安全、合規以及商業規劃和策略領域的資深專家。他們受命對大型網頁設計公司 Clastus 進行認證審計。在此之前，他們在審計工作中展現了卓越的職業道德，包括公正性和客觀性。這次，Clastus 堅信，如果他們能□通過 ISO/IEC 27001 認證，將會在競爭中佔優勢。
審計團隊負責人Tessa擁有豐富的審計經驗，並在T相關議題、合規和治理方面有著非常成功的從業經驗。Malik則擁有組織規劃和風險管理的背景。他的專長在於對組織的安全控制措施及其風險承受能力進行綜合分析，從而準確地評估組織□部的風險程度。另一方面，Michael則是一位經驗豐富的專家，擅長透過遵循嚴格的標準化程序，對控制措施進行實際的安全評估。
在完成必要的審計工作後，Tessa召集了審計團隊會議。他們分析了Michael的一項發現，以客觀準確地做出決定。Michael發現的問題是公司日常營運中一個輕微的不合規之處，他認為這是公司一位T技術人員造成的。因此，在高階主管詢問相關負責人姓名後,Tessa與他們會面，並告知了他們誰是該不合規之處的責任人。為了確保清晰明了，Tessa在審計的最後一天召開了總結會議。

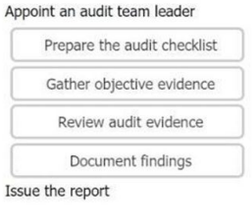
在這次會議上，她向Clastus管理層報告了已發現的不符合項。然而，Tessa得到的建議是，在Clastus認證審核的審口報告中，應避免提供不必要的證據，以確保報告簡潔明了，重點突出關鍵發現。
根據審口的證據，審計團隊起草了審計結論，並決定在授予認證之前，必須對組織的兩個領域進行審計。這些決定隨後提交給了受審計方，但受審計方不接受審計結果，並提出提供補充資訊。儘管受審計方提出了意見，但審計人員由於已決定授予認證，因此拒口接受補充資訊。受審計方的高階主管堅持審計結論與實際情況不符，但審計團隊堅持己見。
根據以上情景，回答以下問題：
問題：
根據審計團隊的決定，Clastus 下一步應該採取什麼措施？
A. 提交行動計劃
B. 評估糾正措施
C. 對行動計畫進行後續跟進
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO/IEC 27001:2022 Clause 10.1 (Improvement) requires organizations to submit action plans to address audit findings.
* Clastus must document an action plan before corrective actions can be evaluated or followed up.
* B. Incorrect:
* Corrective actions can only be evaluated after action plans are submitted and implemented.
* C. Incorrect:
* Follow-up occurs after corrective actions have been executed and verified.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 10.1 (Corrective Action Planning and Implementation)

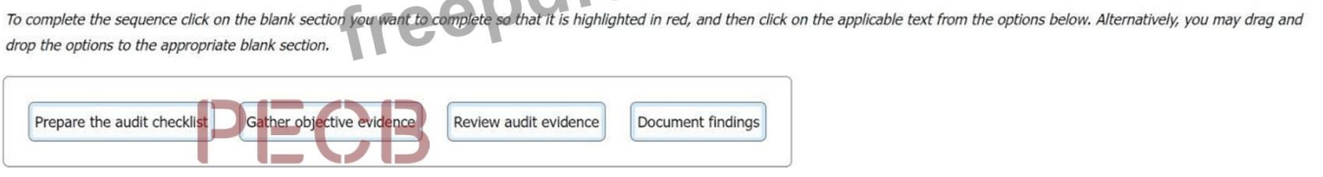
NEW QUESTION: 138
以下選項是第一方審核中涉及的關鍵操作。對階段進行排序以顯示操作發生的順序。

Answer:



Explanation:





The correct order of the stages is:

* Prepare the audit checklist
* Gather objective evidence
* Review audit evidence
* Document findings

* Audit preparation: This stage involves defining the audit objectives, scope, criteria, and plan. The auditor also prepares the audit checklist, which is a list of questions or topics that will be covered during the audit. The audit checklist helps the auditor to ensure that all relevant aspects of the ISMS are addressed and that the audit evidence is collected in a systematic and consistent manner12.
* Audit execution: This stage involves conducting the audit activities, such as opening meeting, interviews, observations, document review, and closing meeting. The auditor gathers objective evidence, which is any information that supports the audit findings and conclusions. Objective evidence can be qualitative or quantitative, and can be obtained from various sources, such as records, statements, physical objects, or observations123.
* Audit reporting: This stage involves reviewing the audit evidence, evaluating the audit findings, and documenting the audit results. The auditor reviews the audit evidence to determine whether it is sufficient, reliable, and relevant to support the audit findings. The auditor evaluates the audit findings to determine the degree of conformity or nonconformity of the ISMS with the audit

criteria. The auditor documents the audit results in an audit report, which is a formal record of the audit process and outcomes. The audit report typically includes the following elements123:
* An introduction clarifying the scope, objectives, timing and extent of the work performed
* An executive summary indicating the key findings, a brief analysis and a conclusion
* The intended report recipients and, where appropriate, guidelines on classification and circulation
* Detailed findings and analysis
* Recommendations for improvement, where applicable
* A statement of conformity or nonconformity with the audit criteria
* Any limitations or exclusions of the audit scope or evidence
* Any deviations from the audit plan or procedures
* Any unresolved issues or disagreements between the auditor and the auditee
* A list of references, abbreviations, and definitions used in the report
* A list of appendices, such as audit plan, audit checklist, audit evidence, audit team members, etc.
* Audit follow-up: This stage involves verifying the implementation and effectiveness of the corrective actions taken by the auditee to address the audit findings. The auditor monitors the progress and completion of the corrective actions, and evaluates their impact on the ISMS performance and conformity. The auditor may conduct a follow-up audit to verify the corrective actions on-site, or may rely on other methods, such as document review, remote interviews, or self-assessment by the auditee.
The auditor documents the follow-up results and updates the audit report accordingly123.
References:
PECB Candidate Handbook ISO 27001 Lead Auditor, pages 19-25
ISO 19011:2018 - Guidelines for auditing management systems
The ISO 27001 audit process | ISMS.online

NEW QUESTION: 139
下列哪兩個是 確實」涉及人際互動的審核方法的範例？
A. 對程序進行獨立審口以準備審核
B. 檢討受審核方對審核結果的回應
C. 透過遠端存取被審核方的伺服器來分析數據
D. 觀察遠端監控執行的工作
E. 透過遠端存取被審核方伺服器分析數據
Answer: A,B (LEAVE A REPLY)
Audit methods are techniques used by auditors to obtain audit evidence. Audit methods can be classified into two categories: those that involve human interaction and those that do not2. Audit methods that involve human interaction require direct communication between the auditor and the auditee or other relevant parties, such as interviews, questionnaires, surveys, meetings, etc. Audit methods that do not involve human interaction rely on observation, inspection, measurement, testing, sampling, analysis, etc., without requiring any verbal or written exchange2. Therefore,

performing an independent review of procedures in preparation for an audit and reviewing the auditee's response to an audit finding are examples of audit methods that involve human interaction, as they require reading and evaluating documents provided by the auditee or other sources. On the other hand, analysing data by remotely accessing the auditee's server and observing work performed by remote surveillance are examples of audit methods that do not involve human interaction, as they do not require any direct communication with the auditee or other parties. References: ISO/IEC 27001:
2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 140
下列哪一項敘述最能描述進行文件審□的目的？
* □明已記錄的管理系統是否不符合審核標準，並收集證據以支持審核報告。
A. 確定已記錄的管理系統是否符合審核標準，並收集結果以支援審核過程。
B. 確定管理系統(就已記錄的部分而言)是否符合審核標準，並收集資訊以支援現場審核活動。
C. 根據審核標準，偵測管理系統中任何已記錄的不符合項，並識別支援審核計畫的資訊
Answer: C (LEAVE A REPLY)
A document review is a process of examining the documented information related to the management system before the on-site audit activities. The purpose of a document review is to: 12
* Determine the conformity of the management system, as far as documented, with audit criteria, i.e., to check whether the documents are consistent, complete, and compliant with the requirements of ISO
/IEC 27001 and any other applicable standards or regulations.
* Gather information to support the on-site audit activities, i.e., to identify the scope, objectives, processes, controls, risks, and opportunities of the management system, and to plan the audit methods, techniques, and resources accordingly.
The other statements are not accurate, because:
* A document review does not reveal or decide about the conformity or nonconformity of the management system as a whole, but only of the documented information. The conformity or nonconformity of the management system is determined by the on-site audit activities, which include interviews, observations, and tests12
* A document review does not gather evidence or findings to support the audit report or process, but information to support the on-site audit activities. The evidence or findings are collected during the on- site audit activities, which are then documented and reported12
* A document review does not detect any nonconformity of the management system, if documented, but determines the conformity of the documented information. The nonconformity of the management system is detected by the on-site audit activities, which evaluate the performance and effectiveness of the management system12
* A document review does not identify information to support the audit plan, but gathers information to support the on-site audit activities. The audit plan is prepared before the document

review, based on the audit scope, objectives, criteria, and program. The document review is part of the audit plan implementation12 References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 141
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: B,D,E,F,I,J (LEAVE A REPLY)
* 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: 142
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: 143
您詢問IT經理，既然個人資料加密和匿名化測試失敗，為什麼組織仍然繼續使用該行動應用程式此外，您也詢問服務經理是否有權批准測試
IT經理解釋口，根據軟體安全管理流程，測試結果需要他批准加密和匿名化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50%的資源來彌補。服務經理認為存取控制已經足口完善，可以接受，因此簽署了批准文件
你抽取了一名醫務人員的手機進行測試，發現安裝了ABC公司的醫療保健行動應用，版本號為1.01。你發現1.01版本沒有測試記錄。
IT經理解釋口，由於勒索軟體攻擊頻繁發生，外包的行動應用開發公司對測試軟體進行了一次免費的小版本更新，緊急發布了更新後的軟體，並口頭保證不會對任何安全功能造成影響
根據他20年的資訊安全經驗，沒有必要重新測試
您正在準備審計結果。請選擇兩個正確的選項。
* 不存在任何不符合項 (NC)。IT 經理已證明其完全勝任該項工作。(與第 7.2 條相關)
A. 存在不符合項(NC)。IT經理未遵守軟體安全管理程序。(與條款8.1，控制項A.8.30相關)
B. 存在不符合項(NC)。該組織未能控制計劃變更並審口非預期變更的後果。(與第 8.1 條相關)
C. 存在改進機會(OI)。組織根據外部服務提供者提供的免費服務範圍選擇服務提供者。(與條款 8.1，控制項 A.5.21 相關)
D. 不存在不符合項 (NC)。IT 經理展現了良好的領導能力。(與條款相關)
5.1，對照組5.4)
E. 存在改進機會(OI)。IT經理應根據適當的測試結果決定是否繼續提供該服務。(與條款8.1、控制項A.8.30相關)
Answer: B,C (LEAVE A REPLY)
According to ISO 27001:2022 Annex A Control 8.30, the organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This includes developing and entering into licensing agreements that cover code ownership and intellectual property rights, and implementing appropriate contractual requirements related to secure design and coding in accordance with Annex A 8.25 and 8.2912 In this case, the organisation and the developer have performed

security tests that failed, which indicates that the secure design and coding requirements of Annex A 8.29 were not met. The IT Manager explains that the encryption and pseudonymization functions failed because they slowed down the system and service performance, and that an extra 150% of resources are needed to cover this. However, this does not justify the acceptance of the test results by the Service Manager, who is not authorised to approve the test according to the software security management procedure. The Service Manager should have consulted with the IT Manager, who is the owner of the process, and followed the procedure for handling nonconformities and corrective actions. The Service Manager's decision to continue the service based on access control alone exposes the organisation to the risk of compromising the confidentiality, integrity, and availability of personal data processed by the mobile app. Therefore, there is a nonconformity (NC) with clause 8.1, control A.8.30.
According to ISO 27001:2022 Clause 8.1, the organisation shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in Clause
6.1. The organisation shall also control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary12 In this case, the organisation has not controlled the planned change of the mobile app from version 1.0 to version 1.01, which was a minor update provided by the outsourced developer in response to frequent ransomware attacks. The IT Manager explains that the developer performed an emergency release of the updated software, and gave a verbal guarantee that there will be no impact on any security functions.
However, this is not sufficient to ensure that the change is properly assessed, tested, documented, and approved before deployment. The IT Manager should have followed the change management process and procedure, and verified that the updated software meets the security requirements and does not introduce any new vulnerabilities or risks. The IT Manager's reliance on his 20 years of information security experience and the developer's verbal guarantee is not a valid basis for skipping the re-testing of the software. Therefore, there is a nonconformity (NC) with clause 8.1.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 144
下列敘述中哪兩項是正確的？
A. 組織只需遵守與其資訊安全管理系統直接相關的法律法規。
B. 在第三方審計期間，審計員會評估組織如何確保其了解法律要求的變更。
C. 該組織不得將審口立法環境以確保遵守法律法規的任務外包。
D. 作為認證機構審核的一部分，審核員負責核實組織的合法合規狀態。
E. 在認證機構審核期間，審核員應確保保留文件訊息，以確定組織必須遵守的法律法規
F. 認證機構審核員的角色包括評估組織的流程，以確保其符合法律要求。

Answer: B,E (LEAVE A REPLY)

From Exact Extract:

Explanation for B (True):

This statement is true because ISO 27001 requires an organization to establish processes for identifying, reviewing, and complying with applicable legal, statutory, regulatory, and contractual obligations. A key part of this is being aware of changes to these requirements to maintain ongoing compliance. An auditor's role is to verify that the organization has such a process in place and that it is effective.

Reference:

ISO/IEC 27001:2022, Clause 6.1.3 "Information security risk treatment": While not directly stating "legal requirements," this clause implies that the organization must determine controls to treat information security risks, and compliance with legal requirements is a significant risk factor.

ISO/IEC 27001:2022, Annex A.5.31 "Legal, statutory, regulatory and contractual requirements": This control states: "The organization should identify, document, and comply with relevant legal, statutory, regulatory, and contractual requirements related to information security." This inherently includes processes for staying aware of changes.

ISO/IEC 27002:2022, 5.31 (Guidance for A.5.31): Provides more detail, emphasizing the need for processes to "identify all relevant legal, statutory, regulatory and contractual requirements, and to ensure that appropriate action is taken to comply with these requirements." This explicitly includes monitoring for changes.

ISO/IEC 17021-1:2015, Clause 9.1.2 "Audit objectives": An audit objective is to determine "the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements." This necessarily involves checking the process for identifying changes.

Explanation for E (True):

ISO 27001 mandates the retention of documented information for various aspects of the ISMS, including the identification of legal requirements. Auditors will look for evidence that the organization has indeed identified and documented the applicable legislation it needs to comply with.

Reference:

ISO/IEC 27001:2022, Clause 7.5.1 "General," 7.5.2 "Creating and updating documented information," and

7.5.3 "Control of documented information": These clauses generally require documented information to be maintained and retained as specified by the standard.

ISO/IEC 27001:2022, Annex A.5.31 "Legal, statutory, regulatory and contractual requirements": As mentioned above, this control explicitly states that the organization should "identify, document, and comply with relevant legal, statutory, regulatory and contractual requirements." The term "document" directly implies

"documented information is retained."

ISO/IEC 27002:2022, 5.31 (Guidance for A.5.31): Further elaborates that the identified requirements should be documented and kept up to date.

Explanation for A (False):

The organization is required to comply with all applicable legal, statutory, and regulatory requirements, as well as contractual obligations. Information security often intersects with broader legal frameworks (e.g., data protection, privacy, industry-specific regulations) that may not directly relate to the ISMS in a narrow sense, but are critical to the organization's overall compliance and its information security posture.
Reference:
ISO/IEC 27001:2022, Annex A.5.31 "Legal, statutory, regulatory and contractual requirements": This control does not limit compliance to only what "directly relates" but to "relevant" requirements. The scope of
"relevant" is determined by the organization's context, operations, and information it handles.
Explanation for C (False):
Organizations can and often do outsource tasks like legal environment reviews to specialized legal firms or subscribe to legal compliance services. The ISO 27001 standard does not prohibit outsourcing. However, the organization remains ultimately accountable for ensuring that these outsourced processes meet the requirements of the ISMS and that legal compliance is maintained. The auditor would verify the organization's oversight of such outsourced activities.
Reference:
ISO/IEC 27001:2022, Clause 8.1 "Operational planning and control": This clause states that organizations should "control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects" and "ensure that outsourced processes are controlled." This implicitly allows outsourcing but requires control.
Explanation for D (False):
A certification body auditor's role is not to act as a legal compliance officer or to definitively verify the organization's actual legal compliance status (i.e., whether they are perfectly compliant with every law). That responsibility lies with the organization itself, often supported by its legal counsel. The auditor's role is to verify that the organization has established, implemented, and maintains an effective process for identifying, managing, and complying with legal requirements as required by ISO 27001. They audit the management system's approach to compliance, not the legal compliance outcome itself.
Reference:
ISO/IEC 17021-1:2015, Clause 9.1.2 "Audit objectives": States that the audit is to determine "the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements." It does not state the auditor's role is to legally verify compliance.
ISO/IEC 27001:2022, Introduction: Emphasizes that the standard specifies requirements for establishing, implementing, maintaining, and continually improving an ISMS, not for guaranteeing absolute legal compliance outside the scope of the ISMS processes.
Explanation for F (This statement is generally aligned with the role, but less precise as a 'sole true' statement compared to B and E):
While this statement is generally true about the auditor's role, its phrasing "to ensure compliance with their legal requirements" can be misinterpreted. As explained for D, the auditor evaluates the processes designed to achieve compliance, not the absolute legal compliance itself. However, in

the context of multiple-choice questions where you pick the "most true" statements, it conveys a similar intent to B, but B and E are more precise regarding specific auditor actions and ISMS requirements. Given B and E are unequivocally true as specific audit actions/requirements, they are the stronger correct answers.
Reference:
ISO/IEC 17021-1:2015, Clause 9.1.2 "Audit objectives": As noted before, the audit objective includes evaluating the management system's ability to meet requirements. This aligns with evaluating processes.

NEW QUESTION: 145
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: 146
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: A (LEAVE A REPLY)
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: 147
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：
根據情境 3。
A. 附件 A 5.1 資訊安全政策
B. 附件 A 5.10 資訊及其他相關資口的可接受使用
C. 附件 A 5.32 智慧財口權
Answer: C (LEAVE A REPLY)
By using illegal versions of software, NightCore ignored the control about intellectual property rights under Annex A.8.1.1 of ISO/IEC 27001, which requires the protection of organizational records to include intellectual property and personal information held in the form of data or software.
References: ISO/IEC 27001:2013 Standard, Annex A.8.1.1 (Responsibility for assets)

NEW QUESTION: 148
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: 149
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. 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
B. 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
C. 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
D. 需要指南來口動組織的資訊安全事件流程
E. 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
F. 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
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 150
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: (SHOW ANSWER)
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: 151
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

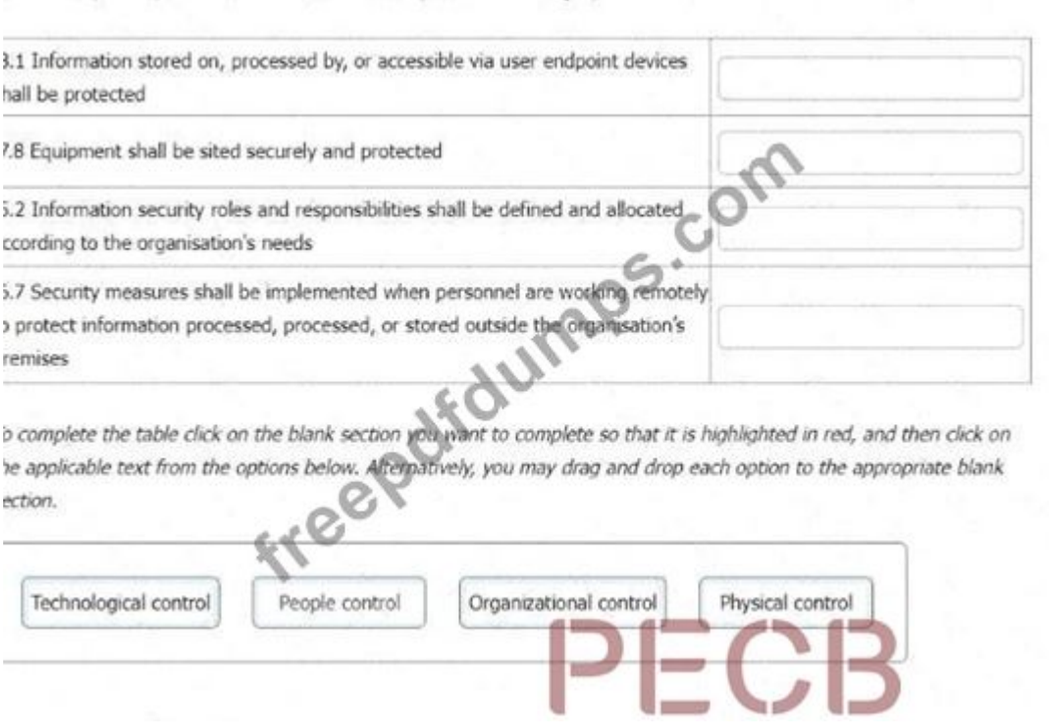
NEW QUESTION: 152

您是一位經驗豐富的 ISMS 口部稽核師。

當 IT 經理找到您並要求您協助修改公司的適用性聲明時，您剛剛完成了組織的預定資訊安全審核。

IT 經理正在嘗試將基於 ISO/IEC 27001:2013 的適用性聲明更新為與 ISO/IEC 27001:2022 中的 4 個控制主題（組織控制 人員控制、實體控制、技術控制）一致的聲明。

IT 經理對控制權的重新分配感到滿意，但以下情況除外。他詢問您以下每個控制類別應出現在哪四個控制類別下。



Answer:

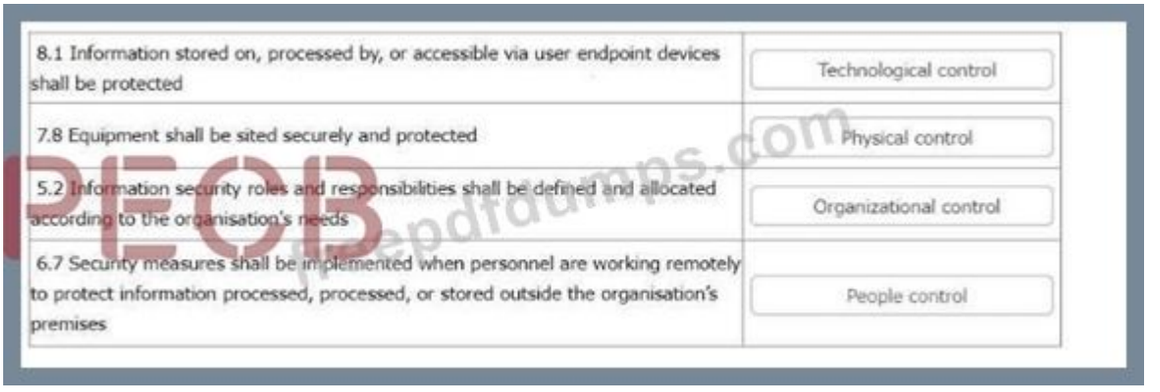
How would you respond? Match the control description to the category.

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

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

Technological control | People control | Organizational control | Physical control

Explanation:



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

* Organisational controls: These are controls that relate to the governance, management, and coordination of information security activities within the organisation. They include controls such as information security policies, roles and responsibilities, risk assessment and treatment, performance evaluation, and improvement.
* People controls: These are controls that relate to the behaviour, awareness, and competence of the people involved in information security, both within and outside the organisation. They include controls such as human resource security, training and awareness, access control, incident management, and business continuity.
* Physical controls: These are controls that relate to the protection of physical assets and environments that store, process, or transmit information. They include controls such as physical security, environmental security, equipment security, and media security.
* Technological controls: These are controls that relate to the use of technology to implement, monitor, and maintain information security. They include controls such as cryptography, network security, system security, application security, and threat intelligence.
Based on these categories, the controls listed in the question can be matched as follows:
* 8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected: This is a technological control, as it involves the use of technology to protect information on devices such as laptops, smartphones, tablets, etc. It may include measures such as encryption, authentication, antivirus, firewall, etc.
* 7.8 Equipment shall be sited securely and protected: This is a physical control, as it involves the protection of physical assets and environments that store, process, or transmit information. It may include measures such as locks, alarms, CCTV, fire suppression, etc.
* 5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs: This is an organisational control, as it involves the governance, management, and coordination of information security activities within the organisation. It may include measures such as defining the authority and accountability of information security personnel, establishing reporting lines and communication channels, assigning tasks and duties, etc.
* 6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises: This is a people control, as it involves the behaviour, awareness, and competence of the people involved in information security, both within and outside the organisation. It may include measures such as providing guidance and training on remote working, enforcing policies and procedures, monitoring and auditing remote activities, etc.
= 1: A Breakdown of ISO 27001:2022 Annex A Controls - BARR Advisory42: ISO 27001:2022 Annex A Controls - What's New? | ISMS.Online13: How many controls are there in ISO 27001:2022? - Strike Graph34: ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A.

NEW QUESTION: 153

場景三：Rebuildy是一家位於泰國曼谷的建築公司，專門從事住宅建築的設計、建造和維護。為了確保敏感專案資料和客戶資訊的安全，Rebuildy決定實施基於ISO/IEC 27001的資訊安全管理系統(ISMS)。這包括對資訊安全風險的全面理解、明確的持續改進方法以及穩健的業務解決方案。
資訊安全管理系統(ISMS)的實施成果如下所示。
*資訊安全是透過應用一系列安全控制措施並建立政策、流程和程序來實現的。
*安全控制措施是根據風險評估實施的，旨在消除風險或將風險降低到可接受的水平。
*所有流程均基於計劃-執行-檢查-改進(PDCA)模型，確保資訊安全管理系統的持續改進。
*資訊安全策略是根據最佳安全實踐制定的安全手冊的一部分，因此它不是一份獨立的文件。
*每位員工的崗位職責中都已明確規定了資訊安全方面的角色和責任。
*資訊安全管理系統的管理評審依計畫間隔進行。
在兩次中期管理評審和一次年度內部審計之後，Rebuildy公司申請了認證。在認證審計之前，Rebuildy公司的一名前員工聯繫了審計團隊成員，告知他們Rebuildy公司存在多項安全問題，但公司試圖掩蓋這些問題。該前員工向審計團隊成員提供了書面證據。Rebuildy公司的重要客戶Electra公司也提交了關於相同問題的證據，審計人員決定採納Electra公司的證據，而不是前員工提供的證據。在審計完成之前，審計團隊成員一直與Electra公司保持聯繫，討論審計過程中發現的不符合。Electra公司提供了補充證據來支持這些發現。
審核開始，審核小組對公司高階主管進行了訪談。訪談內容包括高階主管對資訊安全管理系統(ISMS)實施的承諾等。訪談中所獲得的證據以書面確認的形式記錄下來，用於判定Rebuildy公司是否符合ISO/IEC 27001標準的若干條款。從Electra公司獲得的書面證據連同不符合項報告一起附在了審核報告中。其中，發現的不符合項包括：
*公司財務報告系統中偵測到使用者存取控制設定不當的情況。
公司尚未制定獨立的資訊安全策略。取而代之的是，該公司使用根據最佳安全實踐編寫的安全手冊。收到審計團隊提交的文件後，團隊負責人與Rebuildy的高階主管會面，報告了審計結果。審計團隊報告了與財務報告系統和缺乏獨立資訊安全策略相關的問題。高階管理人員對審核結果表示不滿，並暗示審計團隊負責人的行為不專業，可能要求更換負責人。在壓力之下，審計團隊負責人決定與高階主管合作，淡化已發現的違規問題的嚴重性。因此，審計團隊負責人修改了報告，使其呈現出更有利的一面，從而歪曲了Rebuildy合規問題的真實程度。
根據以上情景，回答以下問題：
問題：
根據情境3，審核團隊利用從高階主管訪談中獲得的資訊來確定Rebuildy是否符合ISO/IEC 27001的若干條款。這種做法是否可以接受？
A. 不，審計團隊應該只使用書面證據，例如政策和程序，來確定符合性。
B. 是的，審計團隊透過高階主管的書面確認獲得了口頭證據，這些證據可用於確定是否符合標準。
C. 是的，與高階主管的訪談是最可靠的審計證據形式，無需進一步核實即可用於確定是否符合標準。
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* Audit evidence can come from interviews, observations, and documentation.
* Verbal evidence from top management is acceptable if documented and confirmed in writing.

* A. Incorrect:
* ISO 19011 allows verbal evidence as long as it is substantiated.
* C. Incorrect:
* Interviews alone are not sufficient-additional verification is required.

Relevant Standard Reference:

* ISO 19011:2018 Clause 6.4.6 (Reviewing Documented Information)

NEW QUESTION: 154

將正確的責任與第二方審核的每位參與者配對：

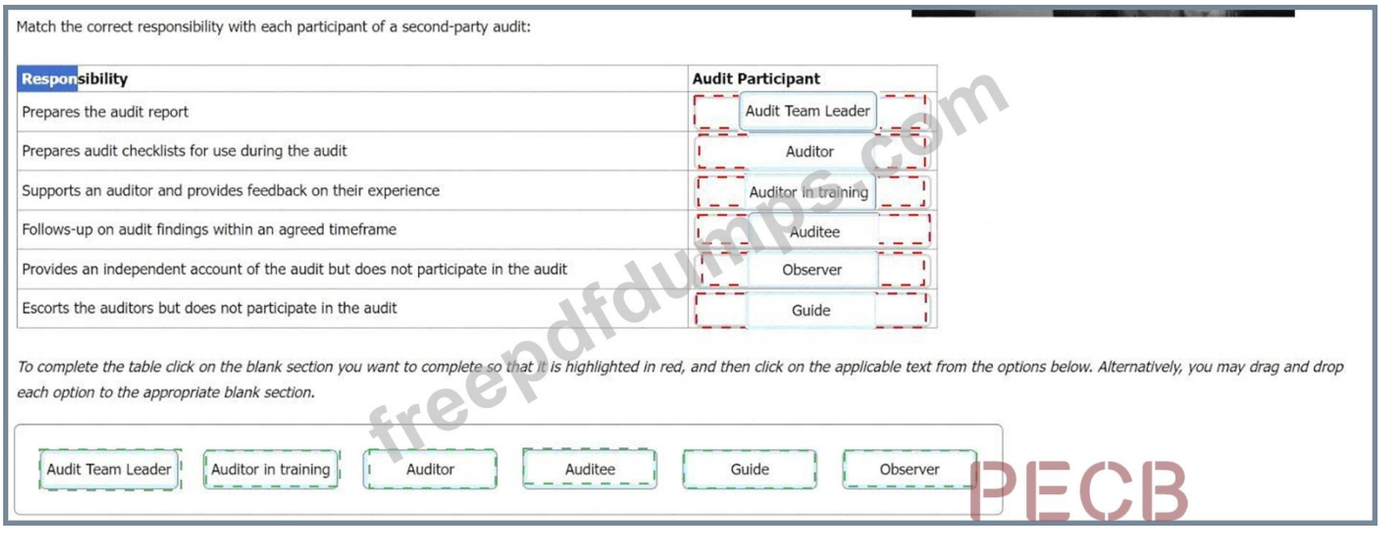
Match the correct responsibility with each participant of a second-party audit:

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

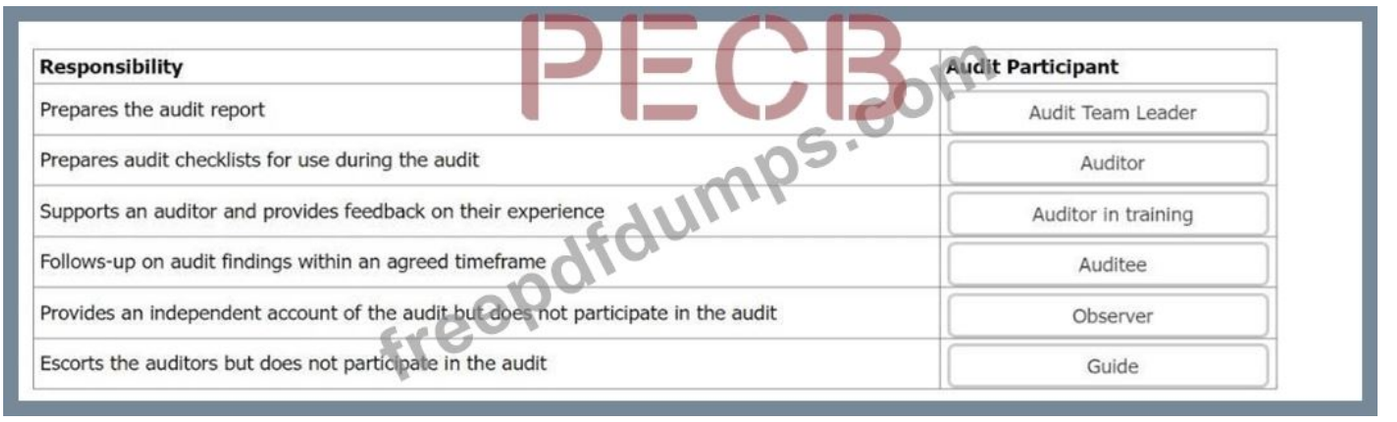
To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

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

Answer:



Explanation:



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

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

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

NEW QUESTION: 155

一個體面的訪客在沒有訪客 ID 的情況下四處閒逛。作為員工，您應該執行以下操作，但以下情況除外：

A. 打招呼並提供咖啡

B. 致電接待員並告知訪客狀況
C. 問候並詢問他有什麼事
D. 護送他到達目的地
Answer: (SHOW ANSWER)
As an employee, you should do the following when you see a visitor roaming around without visitor's ID, except saying "hi" and offering coffee. Saying "hi" and offering coffee is not an appropriate action, as it may imply that you are welcoming or endorsing the visitor without verifying their identity or purpose. This may also give the visitor an opportunity to gain your trust or exploit your kindness. Calling the receptionist and informing about the visitor is an appropriate action, as it alerts the responsible staff to handle the situation and ensure that the visitor is authorized and registered. Greeting and asking him what is his business is an appropriate action, as it shows your concern and curiosity about the visitor's presence and intention. Escorting him to his destination is an appropriate action, as it prevents the visitor from wandering around unattended and accessing unauthorized areas or information. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 42. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 15.

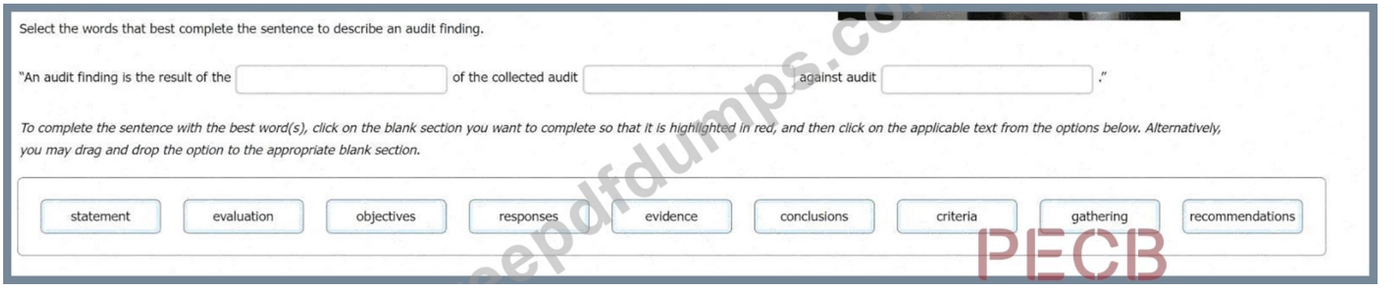
NEW QUESTION: 156
在可接受的資訊資口使用中，哪一個是最佳實務？
A. 僅出於商業目的提供資訊和通訊系統的訪問
B. 幹擾或拒口提供員工主機以外的任何使用者服務
C. 在辦公時間玩任何電腦遊戲
D. 存取電話或網路傳輸，包括無線或WiFi 傳輸
Answer: (SHOW ANSWER)
The best practice in acceptable use of information assets is A: access to information and communication systems are provided for business purpose only. This means that the organization grants access to its information and communication systems only to authorized users who need to use them for legitimate and approved business activities. The organization does not allow or tolerate any unauthorized, inappropriate or personal use of its information and communication systems, as this could compromise information security, violate policies or laws, or cause damage or harm to the organization or its stakeholders. The other options are not best practices in acceptable use of information assets, as they could violate information security policies and procedures, as well as ethical or legal standards. Interfering with or denying service to any user other than the employee's host (B) is a malicious act that could disrupt the availability or performance of the information systems or services of another user or organization. Playing any computer games during office hours is a personal and unprofessional use of the information and communication systems that could distract the employee from their work duties, waste resources and bandwidth, or expose the systems to malware or other risks. Accessing phone or network transmissions, including wireless or wifi transmissions (D) is a potential breach of confidentiality or privacy that could intercept, monitor or modify the information transmitted by another user or organization without their consent or authorization. ISO/IEC 27001:2022 requires the organization

to implement rules for acceptable use of assets (see clause A.8.1.3). 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?

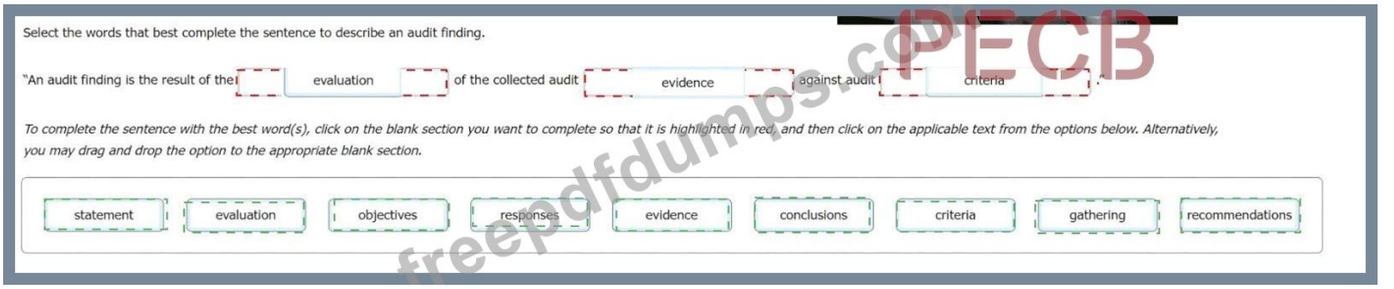
NEW QUESTION: 157
情境五：Cobt是一家位於倫敦的保險公司，提供各種商業、工業和人壽保險解決方案。近年來，Cobt的客戶數量大幅增加。由於需要處理大量數據，該公司決定通過ISO/IEC 27001認證，以保障資訊安全並展現其持續改善的承諾。儘管該公司先前已熟練進行常規風險評估，但實施資訊安全管理系統(ISMS)仍為其日常營運帶來了重大變化。在風險評估過程中，發現了一個風險：組織內部控制機制未能發現或阻止重大缺陷的發生。
該公司遵循一套實施資訊安全管理系統(ISMS)的方法，並在短短幾個月內就建立了可運作的ISMS。成功實施ISMS後，Cobt公司申請了ISO/IEC 27001認證。經驗豐富的審核員Sarah被指派負責此審核。在徹底分析了審核邀請後，Sarah接受了審核團隊負責人的職責，並立即開始收集有關Cobt公司的一般資訊。她制定了審核標準和目標，規劃了審核，並分配了審核團隊成員的職責。
莎拉承認，儘管Cobt公司透過提供多元化的商業和保險解決方案實現了顯著擴張，但仍依賴一些人工流程。因此，她最初的重點是收集有關該公司如何管理資訊安全風險的資訊。莎拉聯繫了Cobt公司的代表，請求內部與風險管理相關的信息，以便進行異地審查，這是最初約定的審計內容之一。然而，Cobt公司後來拒絕了，聲稱此類資訊過於敏感，不宜在公司外部取得。這項拒絕引發了人們對審計可行性的擔憂，尤其是在被審計單位的配合程度以及取得證據方面。此外，Cobt公司也對審計計畫提出了質疑，稱其未能充分反映公司近期所做的變更。該公司指出，審計期間要執行的操作僅適用於初始範圍，並未涵蓋審計範圍的最新變更。莎拉也評估了情況的重要性，考慮了被拒絕提供的資訊對審計目標的重要性。在這種情況下，Cobt公司的拒絕引發了人們對審計完整性及其提供合理保證能力的質疑。鑑於上述情況，Sarah決定在簽署認證協議前退出審核，並已將決定告知Cobt和認證機構。此舉旨在確保審核原則得到遵守，並保持透明度，同時也彰顯了她始終堅持這些原則的決心。
根據以上情景，回答以下問題：
問題：
Cobt在上次風險評估中辨識出了哪種類型的風險？
A. 固有風險
B. 控制風險
C. 偵測風險
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* Detection Risk (Correct Answer) - Detection risk occurs when control mechanisms fail to identify significant defects or errors. Cobt identified that major defects were not detected or prevented by internal controls, making detection risk the correct answer.
* Inherent Risk refers to the likelihood of a security event occurring without considering any controls.
The scenario mentions control failures, not natural risks, so this is incorrect.

* Control Risk is the risk of controls failing to prevent a risk. However, the scenario specifically mentions that the defects were not detected, making detection risk the more precise answer.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 6.1.2 (Information Security Risk Assessment Process)

NEW QUESTION: 158



Answer:



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

NEW QUESTION: 159
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: 160
情境二
Knight 是一家總部位於美國北加州的電子公司，主要開發電視遊戲機。
Knight在全球擁有超過300名員工，□此五週年之際，公司推出了面向國際市場的新一代遊戲主機G-Console。G-Console被譽為2021年的終極多媒體設備，將為玩家帶來最佳遊戲體驗。主機組包含一副VR頭戴裝置、兩款遊戲以及其他贈品。
多年來，該公司憑藉誠信 正直和尊重客□的良好聲譽而備受讚譽。除了是一家以客□為中心的公司外，Knight 還因其卓越的□品品質在遊戲□業中贏得了廣泛的認可。
身為全球領先的遊戲主機開發者之一，Knight 經常成為惡意攻擊的目標。因此，該公司實施了基於 ISO/IEC 27001 的資訊安全管理系統 (ISMS)，並透過每週例會向員工傳達了該系統的適用範圍。
然而，最近Knight 公司遭遇了一次安全漏洞，駭客洩漏了專有資訊。作為應對，事件回應小組(IRT)立即對系統和事件細節展開了徹底調□。最初，IRT 懷疑員工可能使用了弱密碼，導致駭客輕易存取了他們的帳□。進一步調□發現，駭客截獲了檔案傳輸協定(FTP) 的流量，該協定使用明文密碼進行身份驗證來傳輸資料。
鑑於此安全事件，並根據IRT 的建議，Knight 決定以安全外殼協定 (SSH) 取代 FTP。此變更確保所有擷取的流量都經過加密，從而顯著提升安全性。
在實施這些變更後，奈特公司進行了風險評估，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。根據風險評估結果，他們選擇了一種風險處理方案來應對風險。
問題
IRT 對 FTP 的調□結果在資訊安全方面意味著什麼？
A. 漏洞
B. 風險
C. 威脅
Answer: A (LEAVE A REPLY)
The IRT's finding that FTP transmits authentication credentials in clear text represents a vulnerability in information security terms. A vulnerability is defined as a weakness in an asset, system, or control that can be exploited by a threat. In this scenario, FTP itself is not a threat, nor is it the risk; rather, it is the technical weakness that enabled the attackers to succeed.
The attackers (hackers) are the threat, and the potential loss of proprietary information is the impact. The risk arises from the combination of the threat exploiting the vulnerability and causing harm. However, the question specifically asks what the IRT's finding about FTP represents, and that finding is the identification of a weakness in the system design. The use of clear-text authentication is a well-known security weakness, making it easier for attackers to capture credentials through network traffic interception.
ISO/IEC 27001:2022 risk assessment logic requires organizations to distinguish clearly between threats, vulnerabilities, and risks during incident analysis. The IRT did exactly this by identifying that the protocol itself lacked encryption, which is a vulnerability. This is further supported by the corrective action taken:

replacing FTP with SSH. SSH provides encrypted communication, which directly addresses the vulnerability by removing the weakness that allowed credential exposure.
Therefore, the IRT's findings correctly identify FTP as a vulnerability, making option A the correct answer.

NEW QUESTION: 161
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: 162
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: 163
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. 口部郵件

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

NEW QUESTION: 164
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□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：
審核員是否應在審核完成後將員工訓練記錄的副本存檔？請參□場景 7。
A. 否，文件副本通常不會儲存為審核記錄
B. 是的，如審計協議中所述，審計員擁有文件副本
C. 是的，審核期間□生的所有文件化資訊應保留為審核記錄
Answer: A (LEAVE A REPLY)

No, copies of files are not generally kept as audit records unless specifically required and agreed upon in the audit plan. Audit records typically include notes and observations made by auditors, not copies of the auditee's files, unless these are essential and explicitly allowed by the auditee. References: ISO 19011:2018, Guidelines for auditing management systems

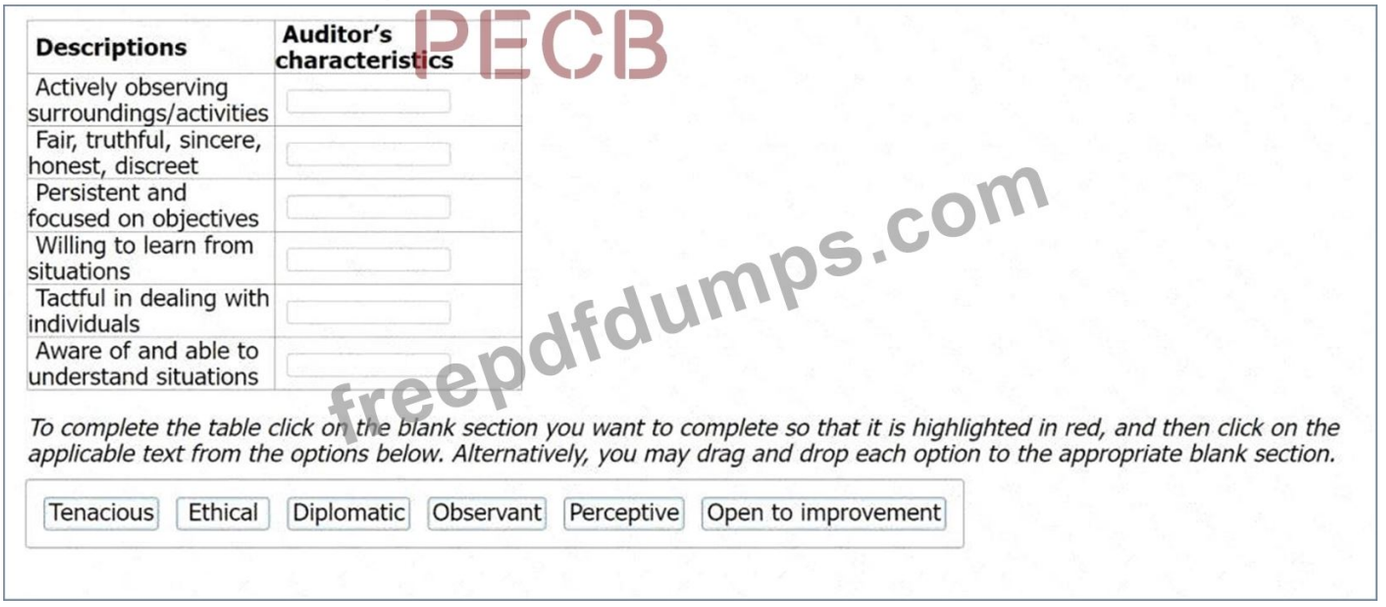
NEW QUESTION: 165
在第三方認證審核期間，受審核方會提供您問題清單。下列哪四項構成 ISO/IEC 27001:2022 管理系統背景下的「外部」問題？
A. 為因應高通膨而提高利率
B. 因政府政策改變而導致補助金減少
C. 訓練支出削減導致員工能力水準低下
D. 因管理不善導致缺勤增加
E. 人口老化導致勞動成本上升
F. 由於政府制裁而無法購買原料
G. 由於員工假期減少，士氣低落
H. 與過時的生口設備有關的生口率下降
Answer: (SHOW ANSWER)
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 4.1 requires an organization to determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its ISMS2. External issues are those that originate from outside the organization, such as legal, regulatory, cultural, social, political, economic, natural and competitive factors2. Internal issues are those that originate from within the organization, such as governance, structure, roles and responsibilities, policies, objectives, culture, capabilities, resources and information systems2. Therefore, based on this definition, four examples of external issues in the context of a management system to ISO/IEC 27001:2022 are a rise in interest rates in response to high inflation (which affects the economic environment of the organization), a reduction in grants as a result of a change in government policy (which affects the political and legal environment of the organization), higher labour costs as a result of an aging population (which affects the social and demographic environment of the organization), and inability to source raw materials due to government sanctions (which affects the trade and supply environment of the organization)2. The other options are examples of internal issues, as they originate from within the organization or its activities. For example, poor levels of staff competence as a result of cuts in training expenditure (which affects the capabilities and resources of the organization), increased absenteeism as a result of poor management (which affects the culture and performance of the organization), poor morale as a result of staff holidays being reduced (which affects the motivation and satisfaction of the organization's personnel), and a fall in productivity linked to outdated production equipment (which affects the efficiency and quality of the organization's processes)2. References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements

NEW QUESTION: 166
請選擇兩項描述使用清單的優勢的選項。
* 每次審計都使用同一份檢口清單，沒有進行任何審核
A. 將面試限制在指定方。
B. 確保遵循相關的審計跟踪
C. 確保審計計畫得到實施
D. 縮短稽核持續時間
E. 必要時不偏離檢口清單
Answer: C,D (LEAVE A REPLY)
A checklist is a tool that helps auditors to collect and verify information relevant to the audit objectives and scope. It can provide the following advantages:
* Ensuring relevant audit trails are followed: A checklist can help auditors to identify and trace the sources of evidence that support the conformity or nonconformity of the audited criteria. It can also help auditors to avoid missing or overlooking any important aspects of the audit.
* Ensuring the audit plan is implemented: A checklist can help auditors to follow and fulfil the audit plan, which describes the arrangements and details of the audit, such as the objectives, scope, criteria, schedule, roles, and responsibilities. It can also help auditors to manage their time and resources effectively and efficiently.
The other options are not advantages of using a checklist, but rather:
* Using the same checklist for every audit without review: This is a disadvantage of using a checklist, as it can lead to a rigid and ineffective audit approach. A checklist should be tailored and adapted to each specific audit, taking into account the context, risks, and changes of the auditee and the audit criteria. A checklist should also be reviewed and updated periodically to ensure its validity and relevance.
* Restricting interviews to nominated parties: This is a disadvantage of using a checklist, as it can limit the scope and depth of the audit. A checklist should not prevent auditors from interviewing other relevant parties or sources of information that may provide valuable evidence or insights for the audit.
A checklist should be used as a guide, not as a constraint.
* Reducing audit duration: This is not necessarily an advantage of using a checklist, as it depends on various factors, such as the complexity, size, and maturity of the auditee's ISMS, the availability and quality of evidence, the competence and experience of the auditors, and the level of cooperation and communication between the auditors and the auditee. A checklist may help reduce audit duration by improving efficiency and organization, but it may also increase audit duration by requiring more evidence or verification.
* Not varying from the checklist when necessary: This is a disadvantage of using a checklist, as it can result in a superficial or incomplete audit. A checklist should not prevent auditors from exploring or investigating any issues or concerns that arise during the audit, even if they are not included in the checklist. A checklist should be used as a support, not as a substitute.
References:

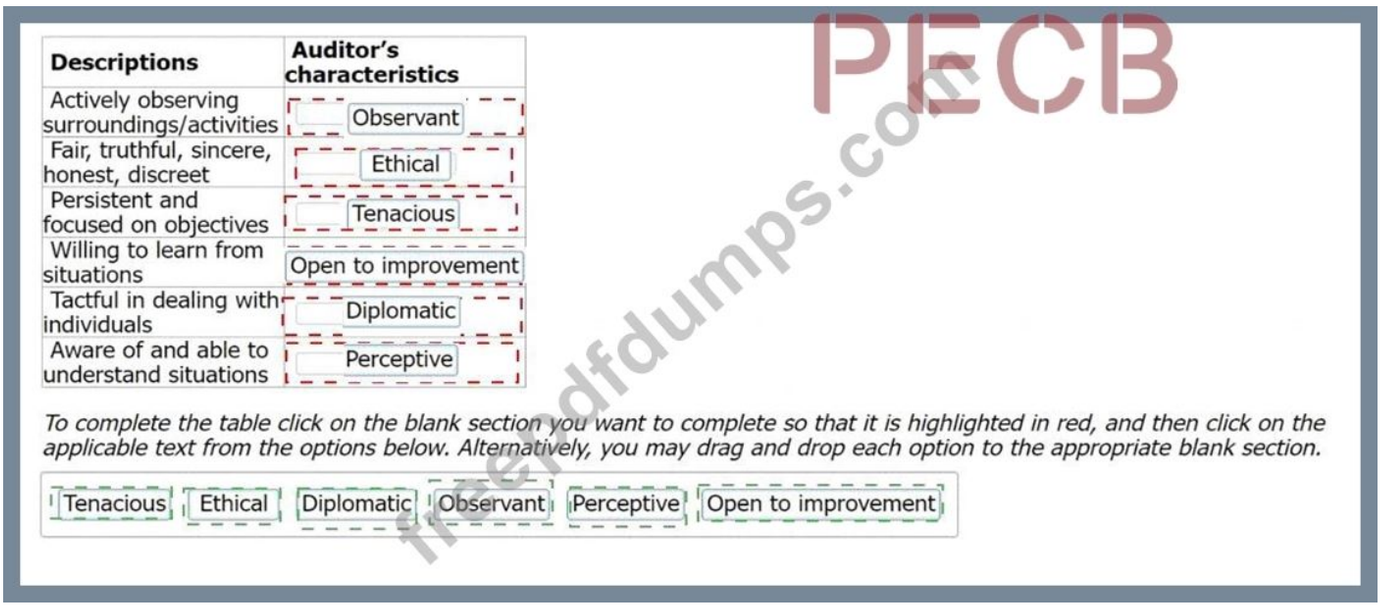
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 6.2.2]

NEW QUESTION: 167

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。



Answer:



Explanation:

The possible matches of the characteristics to the descriptions are:

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

Actively observing surroundings/activities = Observant

Fair, truthful, sincere, honest, discreet = Ethical

Persistent and focused on objectives = Tenacious

Willing to learn from situations = Open to improvement

Tactful in dealing with individuals = Diplomatic

Aware of and able to understand situations = Perceptive

These are the auditor's characteristics and their descriptions as defined by ISO 19011:2022, Clause

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

NEW QUESTION: 168

大數據等新科技的使用對審計有何影響？

A. 它提出了新的挑戰，例如，結合結構化和非結構化數據

B. 透過使審核員能□收集更高品質的審核證據來提高審核質量

C. 它會造成嚴重中斷，例如，引入對於傳統資料庫管理工具處理來□太大或太複雜的數據

Answer: A (LEAVE A REPLY)

The use of new technologies such as big data presents new challenges in auditing, particularly the issue of combining structured and unstructured data. Big data environments often include diverse data sets that auditors need to understand and interpret, which requires new skills and approaches to ensure effective and comprehensive audit coverage.
References: ISO/IEC 27001:2013 Standards and supplementary literature on the impact of technology on auditing practices

NEW QUESTION: 169
ISMS的標準定義是什麼？
A. 是一種資訊安全系統方法，旨在實現實施、建立、審口、營運和維護組織聲譽的業務目標。
B. 公司範圍口的業務目標，以實現建立、實施、營運、監控、審口、維護和改進的資訊安全意識
C. 基於專案的方法，用於實現建立、實施、營運、監控、審口、維護和改進組織資訊安全的業務目標
D. 用於建立、實施、操作、監控、審口、維護和改進組織的資訊安全以實現業務目標的系統方法。
Answer: (SHOW ANSWER)
The standard definition of ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. This definition is given in clause 3.17 of ISO/IEC 27001:2022, and it describes the main components and purpose of an ISMS. An ISMS is not a project-based approach, as it is an ongoing process that requires continual improvement. An ISMS is not a company wide business objective, as it is a management system that supports the organization's objectives. An ISMS is not an information security systematic approach, as it is a broader concept that encompasses the organization's context, risks, controls, and performance. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 15. : ISO /IEC 27001:2022, clause 3.17.

NEW QUESTION: 170
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

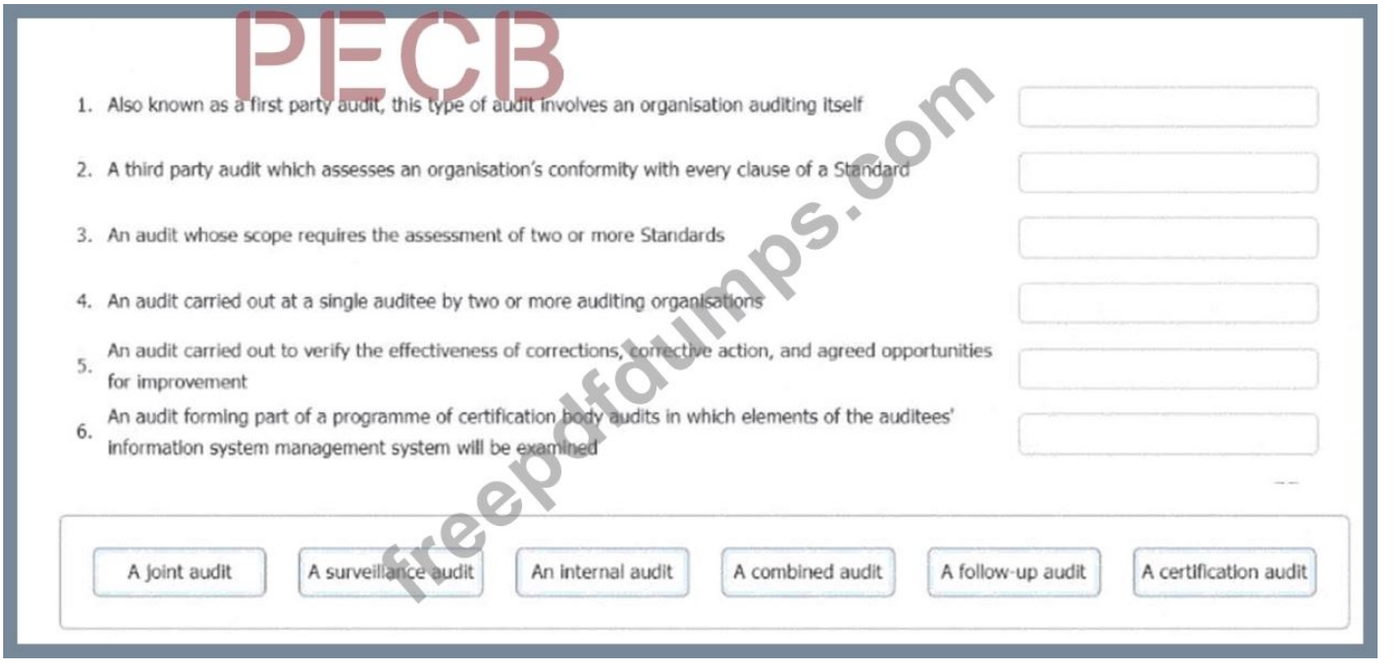
audited management system1. Therefore, these three phrases are examples of objectives in relation to an audit. The other options are not objectives, but rather elements or factors that may influence or affect an audit. For example, an international standard is a source of audit criteria, a management 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: 171

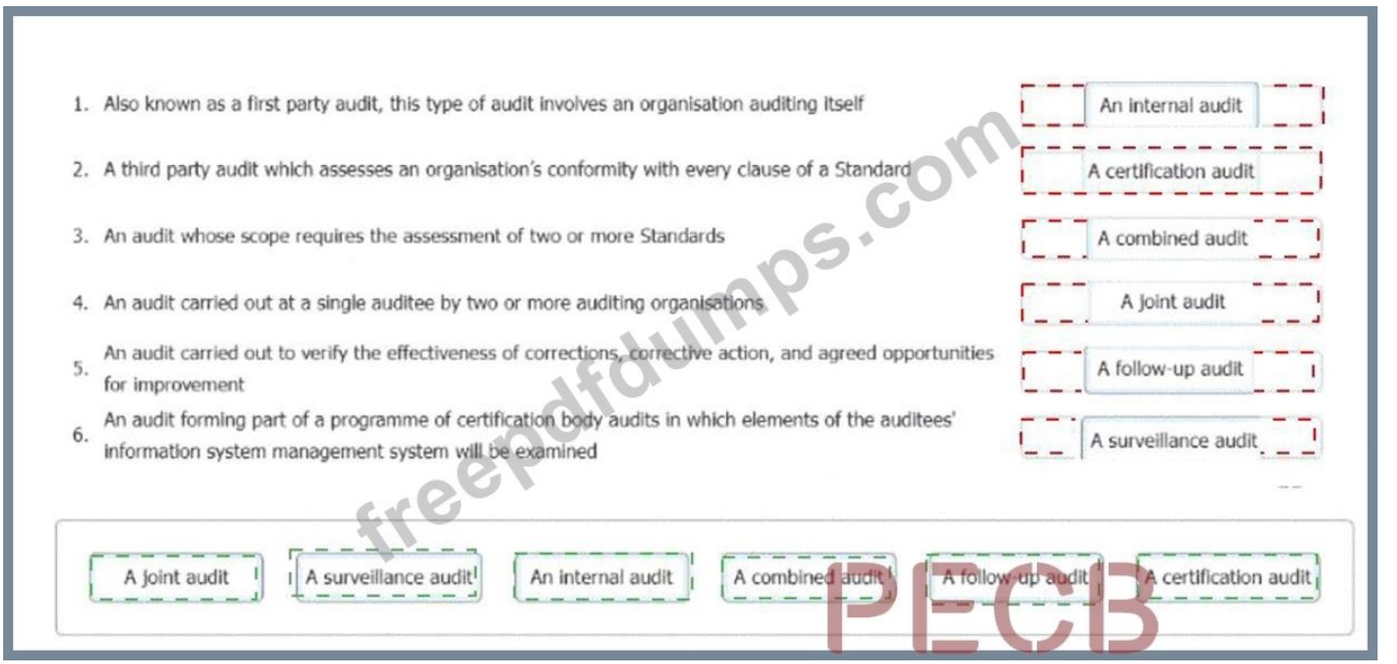
您是一位經驗豐富的 ISMS 審核團隊領導者。受訓的審核員已與您聯繫，要求您澄清她可能需要進行的不同類型的審核。

將以下審核類型與描述相符。

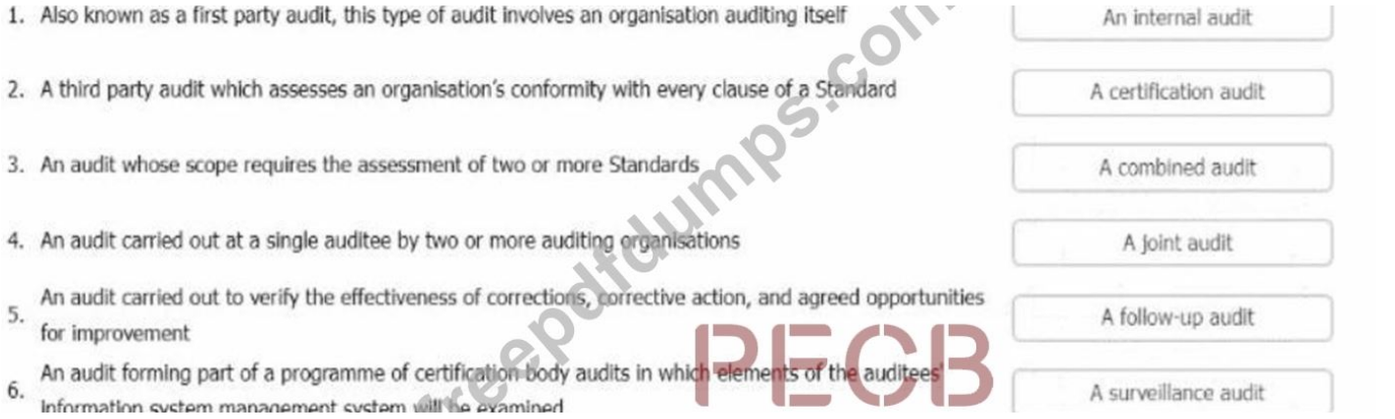
要填寫表格，請按一下要填寫的空白部分，以便反白顯示n fed"，然後從下面的選項中按一下適用的文字。或者，您可以將每個選項拖曳到相應的空白部分。



Answer:



Explanation:



NEW QUESTION: 172

在第三方認證審核過程中，受審核方會向您提出一連串問題。在符合 ISO 27001:2022 標準的管理系統中，下列哪四項屬於「問題？

* 人口老化導致勞動成本上升

A. 為因應高通膨而提高利率

B. 由於訓練支出削減，導致員工能力水準低落

C. 員工假期減少導致士氣低落

D. 管理不善導致缺勤率上升

E. 由於政府政策改變導致的撥款減少

F. 生產設備過時所導致的生產力下降

G. 由於政府制裁，無法取得原料

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:

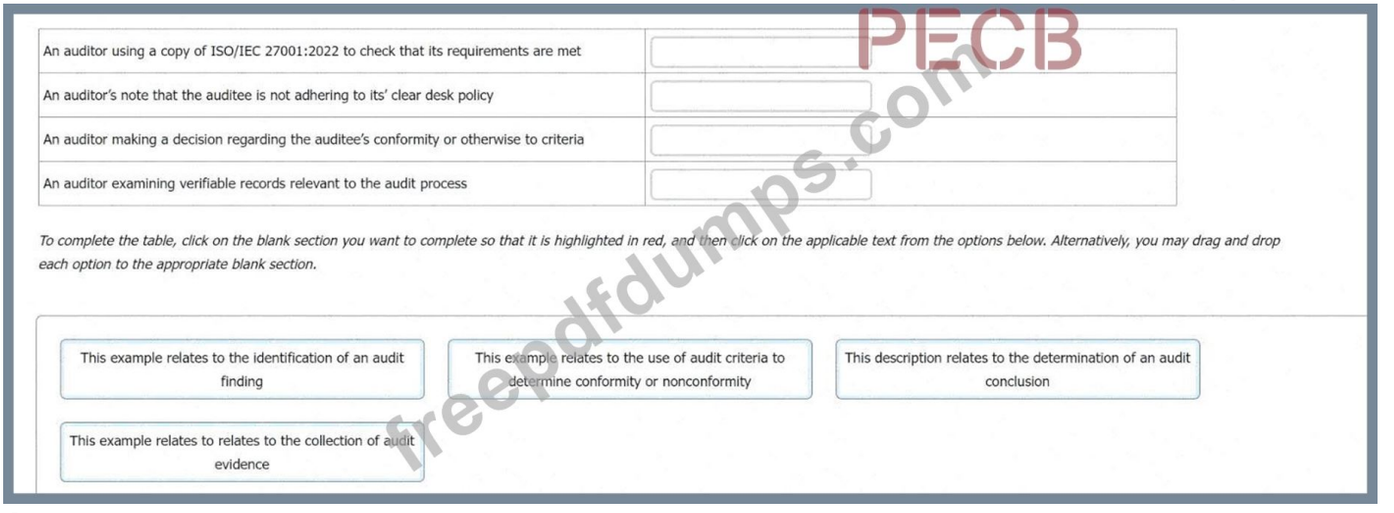
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION: 173
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.

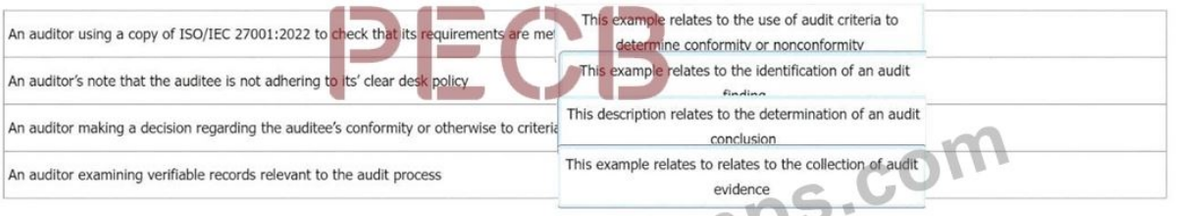
NEW QUESTION: 174
下列哪一項最能描述第一階段第三方審核的主要目的？
A. 向客戶介紹審核團隊
B. 了解組織的採購狀況

C. 確定第 2 階段審核的紅色程度
D. 檢口組織是否遵守法律
E. 準備獨立審計報告
F. 了解組織的客口
Answer: (SHOW ANSWER)
The main purpose of a Stage 1 third-party audit is to determine readiness for a Stage 2 audit. A Stage 1 audit is a preliminary assessment that evaluates the organization's ISMS documentation, scope, context, and objectives, and identifies any major gaps or nonconformities that need to be addressed before the Stage 2 audit. A Stage 1 audit does not introduce the audit team to the client, as this is done during the audit planning phase. A Stage 1 audit does not check for legal compliance by the organization, as this is done during the Stage 2 audit. A Stage 1 audit does not prepare an independent audit report, as this is done after the Stage 2 audit. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 70. : ISO/IEC 27001 LEAD AUDITOR - PECB, page 23.

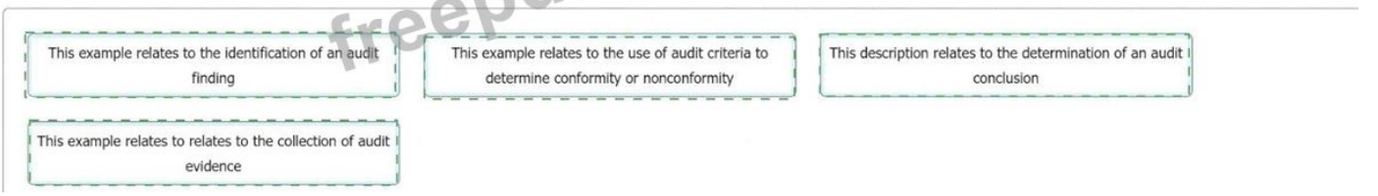
NEW QUESTION: 175
您是一位經驗豐富的 ISMS 審核團隊領導，協助審核員接受培訓，撰寫第一份審核報告
您想要檢口培訓中的審核員對審核報告口容相關術語的理解，並選擇透過展示以下範例來實現此目的。
對於每個範例，您在培訓中詢問審核員描述活動的正確術語是什麼將活動與描述進行配對。



Answer:



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.



Explanation:

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

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

NEW QUESTION: 176

審核員應具備一定的知識和技能；而審計組長也應該具備一些額外的知識和技能 從下面的清單中，選擇僅適用於審核團隊領導的兩項。

A. 計劃審核
B. 瞭解並應用以風險為基礎的稽核方法
C. 應用適當的取樣技術
D. 有效利用提供給審計的資源
E. 了解受審核方的文化和社會面
F. 驗證所收集資訊的相關性和準確性
Answer: A,D (LEAVE A REPLY)
According to the PECB Candidate Handbook1, audit team leaders should have the following additional knowledge and skills compared to auditors:
*Plan the audit, including preparing the audit plan, assigning work to the audit team members and coordinating their activities
*Make effective use of resources provided to the audit, such as personnel, time, budget and equipment
*Manage the audit process, including leading the opening and closing meetings, directing the audit team, resolving conflicts and ensuring the audit objectives are achieved
*Review and approve the audit report and audit findings
*Communicate with the client and other interested parties throughout the audit References: 1: PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 9-10.

NEW QUESTION: 177
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: A (LEAVE A REPLY)
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: 178
問題
在對X公司進行認證審核期間，審核組長注意到部分人力資源流程被排除在審核範圍之外。然而，這些流程實際上包含在公司的資訊安全管理系統(ISMS)範圍口。
這樣可以嗎？
A. 是的，審計範圍可以比資訊安全管理系統(ISMS) 範圍窄，只要它與審計計劃和目標一致即可。
B. 不，ISMS 範圍口列出的所有流程都必須進行審核。

C. 是的，審計範圍必須只包括與IT 相關的流程。

Answer: B (LEAVE A REPLY)

The correct answer is No, all processes listed in the ISMS scope must be audited, because the audit scope for certification must be consistent with the ISMS scope defined by the organization. ISO/IEC 27001 requires that the certification audit assess conformity of the entire ISMS as defined by its scope, not a selective subset of processes.

If HR processes are included in the ISMS scope, they are considered relevant to information security, for example through access management, onboarding and offboarding, training, and disciplinary procedures.

Excluding such processes from the audit would result in incomplete coverage and undermine the validity of the certification decision.

Option A is incorrect because while audit programs and objectives influence audit planning, they cannot override the requirement to audit the full ISMS scope. The audit scope cannot be narrower than the ISMS scope for a certification audit. Option C is incorrect because ISO/IEC 27001 applies to people, processes, and technology, not only IT-related processes.

ISO/IEC 17021-1 requires certification bodies to ensure that audits cover all elements of the management system within scope. Therefore, excluding HR processes that are part of the ISMS scope is not acceptable.

NEW QUESTION: 179

問題

某組織計畫進行口部稽核以評估資訊安全管理系統(ISMS)的有效性。然而，該組織並未明確審計範圍和審計目標。結果，口部稽核人員忽略了處理敏感資訊的關鍵部門。

在這種情況下，審計程序有哪些風險？

A. 規劃風險

B. 溝通風險

C. 資源風險

Answer: A (LEAVE A REPLY)

The scenario represents planning risk, making option A the correct answer. Planning risk arises when an audit is inadequately planned, resulting in incomplete coverage, misaligned objectives, or failure to address critical areas. ISO 19011 emphasizes that defining the audit scope, objectives, and criteria is a fundamental step in audit planning and is essential to achieving effective audit outcomes.

In this case, the organization failed to define the audit scope and objectives clearly. As a direct consequence, the auditor overlooked departments handling sensitive information, which are typically high-risk areas in an ISMS. This oversight undermines the effectiveness of the audit and increases the likelihood that significant risks or nonconformities remain undetected.

Option B is incorrect because communication risk relates to misunderstandings or ineffective information exchange between auditors and auditees. While communication issues may exist, the root cause here is inadequate planning. Option C is incorrect because resource risk concerns

insufficient auditor time, competence, or tools. The problem in this scenario is not a lack of resources but the absence of structured planning.
ISO/IEC 27001 internal audits rely heavily on proper planning to ensure that all relevant processes and assets are evaluated. Therefore, the primary risk present is planning risk.

NEW QUESTION: 180
情境 8
Trustingo自2010年起在愛沙尼亞提供銀行和金融服務。該公司在全國擁有30家分行和100多台ATM機。為滿足嚴格的資料安全和隱私法規要求，Trustingo實施了基於ISO/IEC 27001的資訊安全管理系統(ISMS)，從而確保更高的安全性、更完善的風險管理以及對法律法規的合規性。
在成功實施資訊安全管理系統 (ISMS) 九個月後，Trustingo 決定委託獨立的認證機構，根據 ISO/IEC 27001 標準對其 ISMS 進行認證。此次認證審核涵蓋了 Trustingo 的系統、流程和技術。
審核組聯合進行了第一階段和第二階段審核，並發現了若干不符合項。
第一個不符合項與Trustingo的資訊標籤有關。該公司製定了資訊分類方案，但沒有資訊標籤程序。因此，需要相同保護等級的檔案卻被貼上了不同的標籤。
不符合項也影響了媒體處理。審核團隊採用抽樣方法，結論 50%
200個可移動儲存媒體儲存了敏感訊息，這些資訊被錯誤地歸類為機密資訊。根據資訊分類方案，機密資訊可以儲存在可移動儲存媒體中，而儲存敏感資訊則被嚴格禁止。
審核團隊起草了不符合項報告，並與Trustingo 的代表討論了審核結論，Trustingo 的代表同意在兩個月口提交針對已發現不符合項的行動計劃。
由於認證建議的前提條件是提交糾正措施，Trustingo 必須提交糾正措施計劃，以口明其將如何解決這些不符合項。Trustingo 接受了審核組長提出的解決方案，並透過制定資訊標籤程序和更新可移動媒體程序來解決這些不符合項。
審核結束後兩週，Trustingo提交了一份總體行動計畫。雖然該計劃涵蓋了已發現的不符合項以及已採取的糾正措施，但缺乏針對每項不符合項的詳細行動步驟，也沒有包含受影響的系統控制措施或操作的具體資訊。審核小組對該行動計劃進行了評估。儘管如此，Trustingo仍收到了不利的認證建議。
問題
根據方案8，Trustingo提交了一份總體行動計畫。這份計劃是否可以接受？
A. 是的，具有相同根本原因的不符合項應該有一個通用的行動計劃。
B. 不，行動計畫應該只針對一個不符合項。
C. 不，只要經過審計組長批准，一般行動計畫是可以接受的。
Answer: A (LEAVE A REPLY)
The correct answer is A, because a general action plan can be acceptable when multiple nonconformities share the same root cause, provided that the plan clearly addresses that root cause and demonstrates how recurrence will be prevented. ISO/IEC 27001 clause 10.1 requires organizations to determine the causes of nonconformities and implement corrective actions proportionate to the effects of those nonconformities. It does not mandate a one-to-one relationship between nonconformities and action plans.

In Scenario 8, both nonconformities stem from a common underlying issue: the absence of a formal information labeling procedure aligned with the information classification scheme. The mislabeling of information and the incorrect storage of sensitive information on removable media are consequences of this single systemic weakness. Therefore, a consolidated action plan targeting the root cause is conceptually acceptable.
However, the issue in the scenario is not that the plan was general, but that it lacked sufficient detail, such as clear action steps, responsibilities, timelines, and identification of affected systems and controls. Certification bodies require action plans to be specific, verifiable, and capable of being assessed for effectiveness.
Option B is incorrect because ISO standards do not require separate action plans for each nonconformity when a shared root cause exists. Option C is incorrect because audit team leader approval alone does not make an inadequate plan acceptable.
Thus, while a general action plan is acceptable in principle, it must still be detailed and robust to support certification.

NEW QUESTION: 181
---------- 與其他重要業務資□一樣，該資□對組織有價□，因此需要受到保護
A. 基礎設施
B. 數據
C. 訊息
D. 安全
Answer: C (LEAVE A REPLY)
Information is an asset like other important business assets, as it has value to an organization and consequently needs to be protected. Information can be in any form, such as electronic, paper, or verbal. Information security is the protection of information from unauthorized access, use, disclosure, modification, or destruction2. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION: 182
下列哪兩項是 「不」涉及人為幹預的審計方法範例？
* 使用遠距會議平台進行面試

A. 為審計做準備，對被審計單位的程序進行審口
B. 審口受審計單位對審計結果的回應
C. 透過遠端存取被審計方的伺服器來分析數據
D. 觀察遠端監控所執行的工作
E. 確認審計日期和時間
Answer: (SHOW ANSWER)
Audit methods are the techniques and procedures that auditors use to collect and evaluate audit evidence.
Audit methods can be classified into two categories: those that involve human interaction and those that do not. Human interaction methods are those that require direct or indirect communication with the auditee or other relevant parties, such as interviews, questionnaires, surveys, observations, or walkthroughs. Non-human interaction methods are those that do not require any communication with the auditee or other parties, such as document reviews, data analysis, or remote surveillance.
Some examples of audit methods that do not involve human interaction are:
* Performing a review of auditee's procedures in preparation for an audit: This method involves examining the auditee's documented information, such as policies, processes, records, or reports, to verify their adequacy and effectiveness in meeting the audit criteria. The auditor does not need to interact with the auditee or anyone else to perform this method.
* Analysing data by remotely accessing the auditee's server: This method involves accessing and processing the auditee's data, such as performance indicators, logs, metrics, or statistics, to verify their accuracy and reliability in meeting the audit criteria. The auditor does not need to interact with the auditee or anyone else to perform this method.
References:
ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO 19011:2018 Guidelines for auditing management systems [Section 6.2.2]

NEW QUESTION: 183
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. 組織口品的行銷價格上漲
B. 客口端數量增加
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: 184
問題：
下列哪一種情況構成威脅？
A. 員工使用其合法憑證存取未經授權的文件
B. 組織未能為其雲端服務實施多因素身份驗證 (MFA)。
C. 網路攻擊者利用組織防火牆軟體中的零時差漏洞滲透到網路中。
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* C. Correct Answer - This is a Threat. A cyberattack exploiting a zero-day vulnerability is an active security threat, as it causes harm to the organization.
* A. Employee accessing unauthorized files is a vulnerability (insider risk) rather than an external threat.
* B. Lack of MFA is a security weakness (vulnerability), not a threat.
This aligns with ISO/IEC 27001:2022 Annex A Control A.8.25 (Assessment and Decision on Information Security Events).

NEW QUESTION: 185
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。

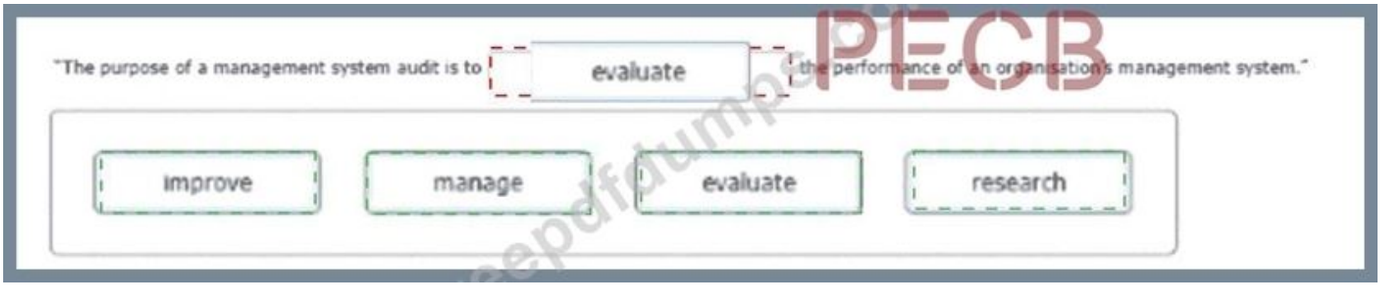
根據該場景，回答以下問題：
當傑克發現有關軟體的第一個不合格項時，他收集了哪些類型的審核證據？請參□場景3。
A. 分析證據
B. 口頭證據
C. 數學證據
Answer: C (LEAVE A REPLY)
Jack collected mathematical evidence when he identified nonconformities by comparing the number of purchased invoices for software licenses with the software inventory. This type of evidence involves numerical, quantifiable data that highlights discrepancies and supports findings of compliance or non- compliance.
References: ISO/IEC 27001:2013 Standard, general guidelines on auditing

NEW QUESTION: 186
情境 3
NightCore是一家總部位於美國的跨國科技企業，專注於電子商務 雲端運算、數位串流媒體和人工智慧(AI)。在實施資訊安全管理系統(ISMS)一年多後，NightCore委託一家認證機構進行ISO/IEC 27001認證審核。
認證機構組建了一支由五名審核員組成的團隊，傑克擔任團隊負責人。傑克在風險管理、資訊安全控制和事件管理方面擁有豐富的審核經驗，並因此而聞名。
他的技能與審計原則和流程的要求高度契合，使他能□有效理解審計範圍並有效運用相關標準。傑克也展現出對NightCore的組織結構、宗旨和管理實踐，以及適用於其業務活動的法律法規要求的深刻理解。
審計團隊遵循合理的審計方法，系統性地得出可靠且可重複的結論。審計團隊認識到，只有能□在一定程度上核實的資訊才能被視為有效證據。在審計過程中，極少數情況下，如果某些資訊的核實存在困難且其可核實程度較低，審計人員會運用專業判斷來評估此類證據的可靠性，並確定其可信度。
在審計過程中，審計人員記錄了他們對NightCore資訊安全管理系統(ISMS)運作規劃和控制的觀察結果和檢□筆記。他們也記錄了對NightCore資訊清單及相關資□的觀察結果。此外，審計人員也審□了為保護網路服務連線而實施的防火牆配置。
隨著審核進入最後階段，NightCore對維護最高資訊安全標準的承諾日益凸顯。憑藉著觸手可及的ISO/IEC 27001認證，NightCore已做好充分準備，有望獲得該認證，從而提升其在科技行業的聲譽。
問題
傑克是否具備審計員所需的知識與技能？請參考情境3。
A. 不，傑克的經驗僅限於審計的幾個領域，這還不□
B. 是的，這完全是因為傑克了解組織的結構及其管理實踐。
C. 是的，傑克具備審計員所需的必要知識和技能。
Answer: C (LEAVE A REPLY)
Jack clearly possesses the necessary knowledge and skills required of an auditor, making option C the correct answer. ISO 19011:2018, which provides guidance on auditing management systems, defines auditor competence as a combination of knowledge, skills, and personal

attributes applied during audit activities. The scenario explicitly demonstrates that Jack meets these competence requirements.
Jack has extensive experience in risk management, information security controls, and incident management, which are core knowledge areas for an ISO/IEC 27001 audit. These competencies enable him to understand ISMS requirements, assess controls, and evaluate incident handling processes. In addition, the scenario highlights his understanding of auditing principles and processes, including the use of systematic, rational methods to achieve reliable and reproducible audit conclusions. This directly aligns with ISO 19011 principles such as evidence-based auditing and due professional care.

NEW QUESTION: 187
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: 188
情境二：
Clinic成立於1990年代，是一家專注於心臟疾病治療和複雜外科手術的醫療器材公司。公司總部位於歐洲，服務對象包括病患和醫療專業人員。Clinic收集患者數據，用於制定個人化治療方案、監測治療效果並改善設備功能。為了增強資料安全性並建立信任，Clinic正在實施基於ISO/IEC 27001的資訊安全管理系統(ISMS)。此舉體現了Clinic致力於安全管理敏感患者資訊和專有技術的承諾。
診所僅考慮口部問題、介面、口部活動與外包活動之間的依賴關係以及相關方的期望，來確定其資訊安全管理系統 (ISMS) 的範圍。該範圍已詳細記錄並公開。在定義其 ISMS 時，診所選擇專注於研發、病患資料管理和客口支援等關鍵部門的關鍵流程。
儘管初期面臨挑戰，診所仍堅持推進資訊安全管理系統(ISMS)的實施，並根據自身獨特需求量身訂做安全控制措施。專案團隊在排除ISO/IEC 27001標準附件A中的某些控制措施的同時，納入了其他口業特定的控制措施以增強安全性。團隊評估了這些控制措施在口部和外部因素下的適用性，最終制定了一份全面的適用性聲明(SoA)，詳細闡述了控制措施選擇和實施背後的理由。
隨著認證準備工作的推進，被任命為團隊負責人的布萊恩採用了一種自主風險評估方法，以識別和評估公司的策略問題和安全措施。這種積極主動的方法確保了診所的風險評估與其目標和使命保持一致。
問題：
根據方案二，診所決定資訊安全管理系統(ISMS)僅涵蓋關鍵流程和部門。這種做法是否可以接受？
A. 是的，但排除其他流程和部門的決定必須有正當理由。
是的，組織可以限制資訊安全管理系統(ISMS) 的範圍，但如果ISMS 的範圍未涵蓋所有流程和部門，則不能申請認證審核。
B. 否，診所必須將所有流程和部門都納入範圍，無論它們對資訊安全管理系統的重要性或相關性如何。
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer: ISO/IEC 27001 Clause 4.3 (Determining the Scope of the ISMS) allows organizations to limit the scope, provided that exclusions do not undermine security effectiveness and are justified.

* B. Incorrect: Organizations can request certification even if the ISMS scope is limited, as long as it is justified.
* C. Incorrect: ISO/IEC 27001 does not mandate full inclusion of all departments in the ISMS. Clinic's decision is acceptable only if the exclusions are justified.

NEW QUESTION: 189
情境7
Lawsy是一家領先的律師事務所，在泰國曼谷設有辦事處。它擁有50多名律師，為客口提供商業法、智慧財口權、銀行和金融服務等領域的專業法律服務。
他們相信，憑藉對資訊安全最佳實踐的貫徹落實以及對技術發展的持續關注，他們在市場上擁有穩固的地位。
兩年來，Lawsy 一直嚴格執行、評估並進行資訊安全管理系統 (ISMS) 的口部審核。現在，他們已向知名且口得信賴的認證機構 ISMA 申請 ISO/IEC 27001 認證。
在第一階段審核中，審核團隊審口了實施階段所創建的所有資訊安全管理系統(ISMS)文件。他們還審口並評估了管理評審和口部審核的記錄。Lawsy提交的證據記錄表明，在必要時已對不符合項採取了糾正措施，因此審核團隊對口部審核員進行了訪談。訪談透過深入了解口部審核計畫和程序，驗證了口部審核的充分性和頻率。
審計團隊繼續核實策略文件，包括資訊安全政策和風險評估標準。在資訊安全政策審口過程中，團隊發現已記錄的治理框架資訊與實際操作流程有不一致之處。第一階段完成後，審計團隊負責人制定了審計計劃，其中涵蓋了審計目標、範圍、標準和流程。
在第二階段審計中，審計團隊採訪了資訊安全經理，他負責起草資訊安全政策他解釋口，Lawsy 每三個月都會進行強制性的資訊安全培訓和意識提升活動，以此來解釋第一階段發現的問題。
審計小組隨後發現，儘管勞西公司允許員工將筆記型電腦帶出工作場所，但該公司並未制定在工作場所外使用筆記型電腦的相關程序。該公司僅提供關於筆記型電腦使用的一般性信息，並依賴員工的常識來保護儲存在筆記型電腦上的資訊的機密性和完整性。
面談結束後，審核小組審口了15份員工培訓記錄(共50份)，並得出結論Lawsy符合ISO/IEC 27001關於培訓和意識方面的要求。為佐證該結論，審核員在審核結束後對審口的員工培訓記錄進行了複印和存檔。
問題
在審計過程中，團隊抽取了50名員工中的15名員工的訓練記錄進行審口。這種情況口明了什麼？請參考以下情景。
A. 與審計師相關的風險
B. 抽樣誤差
C. 固有風險
Answer: (SHOW ANSWER)
This situation represents a sampling error, making option B the correct answer. ISO 19011:2018 explicitly states that management system audits are conducted using sampling techniques because it is impractical to examine all available information within the constraints of time and resources. When auditors select a subset of records, there is an inherent risk that the sample may not fully represent the entire population.

In this scenario, the audit team reviewed training records for 15 out of 50 employees to assess conformity with ISO/IEC 27001 training and awareness requirements. While this is an acceptable and standard audit practice, it introduces the possibility that the selected sample may not reflect gaps or issues present in the remaining records. This uncertainty is known as sampling risk or sampling error.
Option A is incorrect because a "risk related to the auditor" generally refers to competence, impartiality, or ethical behavior issues, none of which are indicated here. The auditors followed a recognized audit method.
Option C is incorrect because inherent risk relates to the nature of the organization or its environment, not to the audit technique used.
Sampling error does not imply that the audit conclusion is invalid; rather, it reflects a known limitation of audits that auditors must manage through professional judgment and appropriate sample selection. Therefore, reviewing a subset of training records represents sampling error.

NEW QUESTION: 190
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: 191
在後續審核期間，您注意到在後續審核之前確定要完成的不合格項仍懸而未決。
您應該採取下列哪四項行動？
A. 向組織的最高管理階層
報告未能針對突出的不符合項採取糾正措施的情況
B. 由於已超過完成日期，因此立即提出不合格項
C. 如果延遲合理，請與受審核方審核客口同意清除不合格項的修改日期
D. 聯絡管理審核計畫的個人，尋求他們關於如何進行的建議
E. 決定延遲解決不合格項是否合理
F. 當收到不合格項已清除的保證時，取消後續審核並回傳
G. 注意不合格項仍然突出，並遵循審核追蹤以確定原因
H. 如果延遲不合理，請告知受審核方審核客口並同意採取補救措施

Answer: A,C,E,G (LEAVE A REPLY)
According to the ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, the following actions should be taken when a nonconformity identified for completion before the follow-up audit is still outstanding:
* A. Report the failure to address the corrective action for the outstanding nonconformity to the organisation's top management. This is part of the auditor's responsibility to communicate the audit results and ensure that the audit objectives are met12.
* C. If the delay is justified agree on a revised date for clearing the nonconformity with the auditee/audit client. This is part of the auditor's responsibility to verify the effectiveness of the corrective actions taken by the auditee and to close the nonconformity when the evidence is satisfactory12.
* E. Decide whether the delay in addressing the nonconformity is justified. This is part of the auditor's responsibility to evaluate the evidence presented by the auditee and to use professional judgement and objectivity to determine the validity of the reasons for the delay12.
* G. Note the nonconformity is still outstanding and follow audit trails to determine why. This is part of the auditor's responsibility to collect and verify audit evidence and to identify the root causes of the nonconformity12.
References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, CQI and IRCA Certified Training, 1
2: ISO/IEC 27001 Lead Auditor Training Course, PECB, 2

NEW QUESTION: 192
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：
Knight 在以 SSH 取代 FTP 時使用了哪種風險處理選項？請參口場景 2。
A. 風險自留
B. 規避風險
C. 風險修改
Answer: C (LEAVE A REPLY)
Risk modification involves implementing controls to reduce the likelihood or impact of a risk. By replacing FTP with SSH, Knight has modified the risk associated with the transfer of files by ensuring that the data is encrypted, thereby reducing the likelihood of unauthorized access through traffic capturing1. References: = This answer is based on the standard risk treatment options provided in ISO/IEC 27001, which include avoiding, modifying, sharing, or retaining risks as part of the risk management process

NEW QUESTION: 193
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。
您的同事似乎不確定資訊安全事件和資訊安全事件之間的差異。您嘗試透過提供範例來解釋差異。
下列哪三種場景可以定義為資訊安全事件？
A. 組織的惡意軟體防護軟體可防止病毒
B. 硬碟機在建議更換日期之後使用
C. 組織收到網路釣魚電子郵件
D. 員工在輪班結束時未能清理辦公桌
E. 未收到付款的承包商刪除了高階管理人員 ICT 帳口
F. 不滿意的員工未經許可更改薪資記錄
G. 組織未通過第三方滲透測試
H. 組織的行銷資料被駭客複製並出售給競爭對手
Answer: E,F,H (LEAVE A REPLY)
According to ISO/IEC 27000:2018, which provides an overview and vocabulary of information security management systems, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant1. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security1. Therefore, based on this definition, three examples of information security incidents are:

* A contractor who has not been paid deletes top management ICT accounts: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of access, data, or functionality for the top management.
* An unhappy employee changes payroll records without permission: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in financial fraud, legal liability, or reputational damage for the organization.
* The organisation's marketing data is copied by hackers and sold to a competitor: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of confidentiality, competitive advantage, or customer trust for the organization.
The other options are not examples of information security incidents, but rather information security events that may or may not lead to incidents depending on their impact and severity. For example:
* The organisation's malware protection software prevents a virus: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, as it is prevented by the malware protection software.
* A hard drive is used after its recommended replacement date: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it fails or causes other problems.
* The organisation receives a phishing email: This is an example of an identified occurrence of a network state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it is opened or responded to by the recipient.
* An employee fails to clear their desk at the end of their shift: This is an example of an identified occurrence of a service state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the desk contains sensitive or confidential information that is accessed by unauthorized persons.
* The organisation fails a third-party penetration test: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the penetration test reveals serious vulnerabilities that are exploited by malicious actors.
References: ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary

NEW QUESTION: 194
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: 195
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: C (LEAVE A REPLY)
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: 196
情境二
Knight 是一家總部位於美國北加州的電子公司，主要開發電視遊戲機。
Knight在全球擁有超過300名員工，□此五週年之際，公司推出了面向國際市場的新一代遊戲主機G-Console。G-Console被譽為2021年的終極多媒體設備，將為玩家帶來最佳遊戲體驗。主機組包含一副VR頭戴裝置、兩款遊戲以及其他贈品。
多年來，該公司憑藉誠信、正直和尊重客□的良好聲譽而備受讚譽。除了是一家以客□為中心的公司外，Knight 還因其卓越的□品品質在遊戲□業中贏得了廣泛的認可。
身為全球領先的遊戲主機開發者之一，Knight 經常成為惡意攻擊的目標。因此，該公司實施了基於 ISO/IEC 27001 的資訊安全管理系統 (ISMS)，並透過每週例會向員工傳達了該系統的適用範圍。
然而，最近Knight 公司遭遇了一次安全漏洞，駭客洩漏了專有資訊。作為應對，事件回應小組(IRT)立即對系統和事件細節展開了徹底調□。最初，IRT 懷疑員工可能使用了弱密碼，導致駭客輕易存取了他們的帳□。進一步調□發現，駭客截獲了檔案傳輸協定(FTP) 的流量，該協定使用明文密碼進行身份驗證來傳輸資料。
鑑於此安全事件，並根據IRT 的建議，Knight 決定以安全外殼協定 (SSH) 取代 FTP。此變更確保所有擷取的流量都經過加密，從而顯著提升安全性。
在實施這些變更後，奈特公司進行了風險評估，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。根據風險評估結果，他們選擇了一種風險處理方案來應對風險。
問題
根據方案二，ISMS 的範圍已在每週例會上傳達給 Knight 的員工。這種做法是否可以接受？
A. 是的，在每週例會上溝通ISMS 範圍是可以接受的，前提是會議記錄已記錄在案。
B. 不，範圍應該作為文件資訊提供，以確保可訪問性。
C. 不，ISMS 的範圍只能透過正式的訓練課程進行溝通，而不能在每週的會議上進行溝通。
Answer: B (LEAVE A REPLY)
ISO/IEC 27001:2022 requires that the scope of the ISMS be established and maintained as documented information. This requirement is explicitly stated in clause 4.3, which requires organizations to determine the boundaries and applicability of the ISMS and to ensure that the scope is documented. While communication and awareness are important, verbal communication alone is not sufficient to meet this requirement.
In the scenario, Knight communicated the ISMS scope to employees during a weekly meeting. While this may support awareness, it does not satisfy the requirement for documented information. Employees, auditors, and other interested parties must be able to access the ISMS scope consistently over time, including new employees or external stakeholders. Relying on meetings creates a risk that the scope is misunderstood, forgotten, or inconsistently applied.
Option A is incorrect because documenting meeting minutes does not replace the requirement for a formally controlled ISMS scope document. The scope must exist independently as documented information, not merely as a record of communication. Option C is also incorrect because ISO/IEC 27001 does not mandate formal training sessions as the only acceptable communication method for scope awareness.

Therefore, the correct position is that while communicating the scope verbally is useful, it is not acceptable on its own, and the scope must be maintained as documented information.

NEW QUESTION: 197
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：
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。這口明什麼？
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: (SHOW ANSWER)

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: 198

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: (SHOW ANSWER)

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: 199

以下是 ‧誠信」的目的，這是資訊安全的基本組成部分之一

A. 資訊不會提供或揭露給未經授權的個人的屬性

B. 保障資口準確性和完整性的屬性。

C. 資訊不會提供或揭露給未經授權的個人的屬性

D. 根據授權實體的要求可存取和使用的屬性。

Answer: B (LEAVE A REPLY)

Integrity is one of the basic components of information security, along with confidentiality and availability.

Integrity means that information is safeguarded from unauthorized or accidental changes that could affect its accuracy and completeness. Integrity ensures that information is reliable and trustworthy3. References: ISO /IEC 27001:2022 Lead Auditor Training Course - BSI

NEW QUESTION: 200

您收到一封電子郵件，要求您發送姓名 電子郵件和密碼等訊息，才能繼續使用您的電子郵件帳口。如果您不發送此類訊息，您的電子郵件帳口將被停用。這個場景呈現了什麼？

A. 人員類型的漏洞

B. 未經授權的威脅行為類型

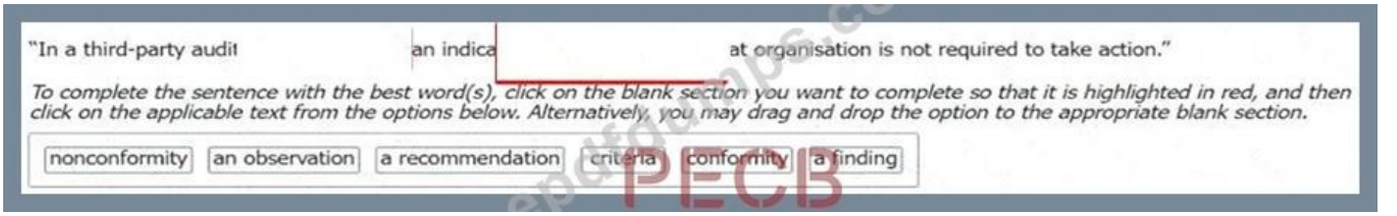
C. 威脅訊息類型的妥協

Answer: B (LEAVE A REPLY)

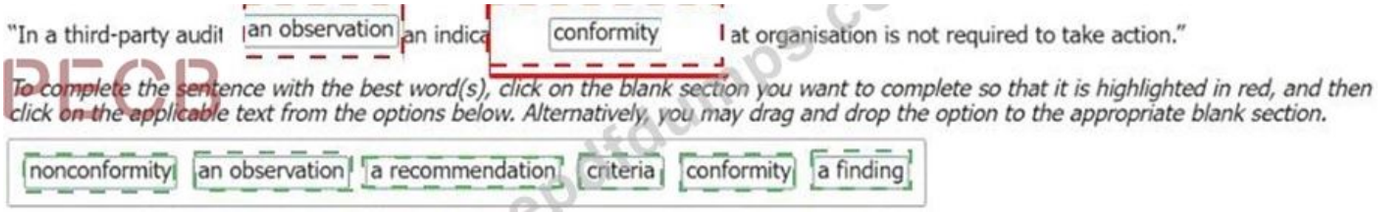
The scenario described is a classic example of a phishing attack, which is a type of social engineering threat where attackers masquerade as a trustworthy entity in an electronic communication. The goal is to trick individuals into providing sensitive information. This represents an unauthorized action type of threat because it involves an attacker attempting to gain unauthorized access to personal information. References: = This understanding of phishing as a threat is consistent with the principles of information security management systems and is supported by resources that describe phishing attacks and their prevention

NEW QUESTION: 201

選出最能完成句子的單字：



Answer:



Explanation:

"In a third-party audit an observation can indicate conformity at organisation is not required to take action." According to the PECB Candidate Handbook1, an observation is "a statement of fact made during an audit and substantiated by objective evidence". An observation can indicate conformity or nonconformity, but it does not require any corrective action from the audited organisation. A recommendation, on the other hand, is

"a suggestion for improvement based on an observation". A recommendation may or may not be accepted by the audited organisation.
According to the Fundamentals - Third parties2, a third-party audit is "an audit conducted by an external organisation that has the legal right to audit an organisation's processes and procedures". A third-party audit can result in a finding, which is "a conclusion reached by the auditor based on the audit evidence collected".
A finding can be positive or negative, depending on whether the audited organisation meets the audit criteria or not. A nonconformity is "a finding that indicates the non-fulfilment of a requirement". A nonconformity requires corrective action from the audited organisation to prevent recurrence.

NEW QUESTION: 202
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，代表同意在兩個月口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: 203
審核員在確定 (2)-------- 時應考慮 (1)--------
A. 1）標準要求 （二）審核標準
B. (1) 稽核風險，(2) 稽核目標
C. (1) 與違法行為相關的處罰，(2) 重要性
Answer: B (LEAVE A REPLY)
The auditor should consider "audit risks" when determining the "audit objectives." Understanding the risks associated with the audit helps define the objectives clearly, ensuring that the audit focuses on the most significant areas of concern, aligns with the audit scope, and adequately addresses the risks identified.
References: ISO 19011:2018, Guidelines for auditing management systems

NEW QUESTION: 204
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: 205

場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客口為中心的公司，Techmanic 重視與客口建立牢固的關係，並致力於採用領先的安全實踐。

Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統 (ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後,Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域。負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在 IT 諮詢領域。認識到持續改進的價口，並從過去的評估中吸取經驗教訓。

Techmanic實施了一項審口以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化IT諮詢行業的重新認證流程。

在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。

Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項。此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性。基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。

根據以上情景，回答以下問題：

問題：

Techmanic公司在重新認證活動中審口以往監督審計報告的目的是否已明確界定？

A. 是的，重新認證活動的目的是取代IT顧問業重新認證審核的必要性。

B. 不，重新認證活動的目的是將Techmanic 的軟體開發與口業基準進行比較。

C. 不，重新認證活動的目的是評估Techmanic 管理系統在認證週期口的表現。

Answer: (SHOW ANSWER)

Comprehensive and Detailed In-Depth Explanation:

* C. Correct Answer:
* Recertification reviews the overall ISMS performance over the certification cycle, not just past audit findings.
* A. Incorrect:
* Previous audit findings do not replace the need for a full recertification audit.
* B. Incorrect:
* Recertification is not about industry benchmarking-it is about ISMS effectiveness.

Relevant Standard Reference:

* ISO/IEC 17021-1:2015 Clause 9.6.4 (Recertification Process)

Valid ISO-IEC-27001-Lead-Auditor-CN Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Auditor-CN Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Auditor-CN exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Auditor-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Auditor-CN dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Auditor-CN_examcollection.html (**418** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)