최신버전ISO-IEC-27001-Lead-Auditor-CN퍼펙트덤프 최신데모문제완벽한덤프공부자료

BONUS!!! PassTIP ISO-IEC-27001-Lead-Auditor-CN 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1AyBl5ZAXMzVanmWysPulW1DGGXdO2tsd

PassTIP에는 IT인증시험의 최신PECB ISO-IEC-27001-Lead-Auditor-CN학습가이드가 있습니다. PassTIP 는 여러분들이PECB ISO-IEC-27001-Lead-Auditor-CN시험에서 패스하도록 도와드립니다. PECB ISO-IEC-27001-Lead-Auditor-CN시험준비시간이 충분하지 않은 분은 덤프로 철저한 시험대비해보세요. 문제도 많지 않고 깔끔하게 문제와 답만으로 되어있어 가장 빠른 시간내에PECB ISO-IEC-27001-Lead-Auditor-CN시험합격할수 있습니다.

PECB ISO-IEC-27001-Lead-Auditor 中文 Exam Syllabus Topics:

Section	Objectives
Closing the Audit	- Audit reporting and follow-up • 1. Audit report preparation • 2. Corrective action review
Conducting an Audit	- Audit execution • 1. Nonconformity identification • 2. Interviewing techniques • 3. Evidence collection and verification
Information Security Management System (ISMS) based on ISO/IEC 27001	- ISO/IEC 27001 requirements (Clauses 4–10) • 1. Support and resources • 2. Operation and controls • 3. Planning and risk management • 4. Performance evaluation • 5. Leadership and commitment • 6. Improvement and corrective actions • 7. Context of the organization

Fundamentals of Information Security Auditing	- Audit principles based on ISO 19011 • 1. Confidentiality and independence • 2. Integrity, fair presentation, due professional care
Planning and Initiating an Audit	- Audit program and planning activities • 1. Audit team selection • 2. Defining audit objectives, scope, and criteria

>> ISO-IEC-27001-Lead-Auditor-CN퍼펙트 덤프 최신 데모문제 <<

ISO-IEC-27001-Lead-Auditor-CN최신덤프문제 - ISO-IEC-27001-Lead-Auditor-CN최신 업데이트 시험덤프

PassTIP PECB인증ISO-IEC-27001-Lead-Auditor-CN시험덤프 구매전 구매사이트에서 무료샘플을 다운받아 PDF버전 덤프내용을 우선 체험해보실수 있습니다. 무료샘플을 보시면PassTIP PECB인증ISO-IEC-27001-Lead-Auditor-CN시험대비자료에 믿음이 갈것입니다.고객님의 이익을 보장해드리기 위하여PassTIP는 시험불합격시 덤프비용전액환불을 무조건 약속합니다. PassTIP의 도움으로 더욱 많은 분들이 멋진 IT전문가로 거듭나기를 바라는바입니다.

최신 ISO 27001 ISO-IEC-27001-Lead-Auditor-CN 무료샘플문제 (Q194-Q199):

질문 # 194
您正在一家提供醫療保健服務的住宅療養院進行 ISMS 審核。審核計畫的下一步是驗證資訊安全事件管理流程。IT 安全經理介紹了資訊安全事件管理程序（文件參考 ID：ISMS_L2_16，版本 4），並解釋此流程基於 ISO/IEC 27035-1:2016。
您查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 小時內報告給聯絡人 (PoC)」。在訪問員工時，您發現大家對「弱點、事件、事件」意義的理解有差異。
IT安全經理解釋說，6個月前舉辦了一次線上「資訊安全應對」培訓研討會。所有受訪者均參與並通過了報告練習和課程評估。
您正在準備審計結果。選擇兩個正確的選項。

- A. 存在不合格項 (NC)。資訊安全事件培訓失敗。這不符合第 7.2 條和控制措施 A.6.3。
- B. 有改進的機會 (OFI)。報告資訊安全弱點、事件和事件。這與第 9.1 條和控制措施 A.5.24 有關。
- C. 還有改進的機會 (OFI)。提高資訊安全事件訓練效果。這與第 7.2 條和控制措施 A.6.3 相關。
- D. 沒有不合格項。資訊安全處置訓練卓有成效。這符合第 7.2 條和控制措施 A.6.3。
- E. 存在不合格項 (NC)。事件管理報告流程的術語不明確，員工對「弱點、事件和事件」意義的誤解證明了這一點。這不符合第 9.1 條和控制措施 A.5.24。
- F. 沒有不合格項。報告資訊安全弱點、事件和事故。
  這符合第 9.1 條和控制措施 A.5.24。

정답：C,E

설명：
According to ISO/IEC 27001:2022 clause 7.2, the organization must ensure that the persons doing work under its control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. The organization must also provide information security awareness education and training to its personnel and relevant interested parties. According to control A.6.3, the organization must ensure that all employees and contractors are made aware of the information security incident management procedures and their expected roles and responsibilities. Therefore, an opportunity for improvement (OFI) can be identified if the information security incident training effectiveness can be improved, as evidenced by the differences in the understanding of the meaning of "weakness, event, and incident" among the staff.
According to ISO/IEC 27001:2022 clause 9.1, the organization must monitor, measure, analyze and evaluate the information security performance and the effectiveness of the ISMS. The organization must also retain appropriate documented information as evidence of the monitoring and measurement results. According to control A.5.24, the organization must establish and maintain an information security incident management process that includes the following activities:

* reporting information security events and weaknesses;
* assessing and deciding on information security events;
* responding to information security incidents;
* learning from information security incidents;
* collecting evidence and disclosing information.
Therefore, a nonconformity (NC) can be identified if the terminology of the incident management reporting process is unclear, as evidenced by the staff misunderstanding of the meaning of "weakness, event, and incident". This could lead to inconsistent or inaccurate reporting, assessment, response, learning, and disclosure of information security incidents, which could affect the information security performance and the effectiveness of the ISMS.
Reference:
* ISO/IEC 27001:2022, clauses 7.2, 9.1, and Annex A controls A.5.24 and A.6.3
* [PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 15-16, 18-19, 22-23
* ISO/IEC 27035-1:2016, clauses 4, 5, 6, 7, and 8
* ISO 27001 - Annex A.16: Information Security Incident Management
* ISO 27001:2022 Annex A Control 5.24 - What's New?

질문 # 195
您是認證機構指派的 ISMS 審核小組組長，負責對資料中心客戶進行後續審核。
根據 ISO 19011:2018，後續審核的目的是要驗證下列哪一項？

- A. 管理系統的有效性
- B. ISMS 目標的實施
- C. 風險處理計劃的實施
- D. 糾正措施的完成情況和有效性

정답：D

설명：
The purpose of a follow-up audit is to verify the completion and effectiveness of corrective actions taken by the auditee in response to the nonconformities identified in a previous audit1. A follow-up audit is a type of audit that is conducted after an initial audit, and it focuses on the specific areas where nonconformities were found and corrective actions were agreed upon2. A follow-up audit can be conducted as a separate audit or as part of a scheduled audit, depending on the nature and severity of the nonconformities and the audit programme objectives3.
The other options are not the purpose of a follow-up audit, but rather the purpose of other types of audits. For example:
*Option A is the purpose of a performance audit, which is a type of audit that evaluates the effectiveness of the management system in achieving its intended results4.
*Option B is the purpose of a compliance audit, which is a type of audit that verifies the conformity of the management system with the specified requirements, such as the ISMS objectives5.
*Option C is the purpose of a process audit, which is a type of audit that examines the inputs, activities, outputs, and interactions of a specific process within the management system, such as the risk treatment process.
References: 1: ISO 19011:2018, 6.7; 2: ISO 19011:2018, 3.7; 3: ISO 19011:2018, 5.5.2; 4: ISO 19011:2018, 3.6; 5: ISO 19011:2018, 3.5; : ISO 19011:2018, 3.4; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]

질문 # 196
完成第一階段並準備第二階段初步認證審核後，受審核方通知審核小組負責人，他們希望擴大審核範圍，以包括該組織最近收購的另外兩個場所。
考慮到這些訊息，您希望審計小組負責人採取什麼行動？

- A. 通知被審核方審核組長接受請求
- B. 安排使用視訊會議平台完成兩個站點的遠端第一階段審核
- C. 獲取有關其他站點的信息，以通知管理審核計劃的個人
- D. 增加第 2 階段審核的長度以包含額外的站點

정답：C

설명：
According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, the audit team leader should obtain information about the additional sites to inform the individual(s) managing the audit programme, as this may affect the audit objectives, scope,

criteria, duration, resources, and risks. The audit team leader should also review the audit plan and make any necessary adjustments in consultation with the auditee and the audit client1. References: 1: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 27, section
4.3.2.2.

질문 # 197
您工作的資料中心目前正在尋求 ISO/IEC27001:2022 認證。在為您的初次認證訪問做準備時，您集團內另一個資料中心的同事已進行了多次內部審核。他們在今年稍早獲得了 ISO/IEC 27001:2022 證書。
您剛剛獲得內部 ISMS 審核員資格，您的經理要求您在外部認證機構到達之前審查審核流程和審核結果，作為最終檢查。
以下哪六項會讓您擔心是否符合 ISO/IEC 27001:2022 要求？

- A. 審計流程規定審計結果將提供給「相關」經理，而不是最高管理階層
- B. 審核程序不考慮先前審核的結果
- C. 審計報告不以硬拷貝形式（即紙本形式）保存。它們僅作為「.POF 文件」儲存在組織的 Intranet 上
- D. 審核計畫顯示年內不定期進行管理審核
- E. 審核計畫未引用審核方法或審核職責
- F. 迄今為止的審計報告已使用關鍵績效指標資訊來僅關注 ISMS 流程的效率
- G. 雖然已定義每次內部審核的範圍，但尚未為迄今為止進行的審核定義審核標準
- H. 審核計畫未考慮資訊安全流程的相對重要性
- I. 審核計畫要求審核員必須獨立於他們審核的領域，以滿足 ISO/IEC 27001:2022 的要求
- J. 根據審核計劃，在認證訪問之前不會審核高階主管對 ISMS 的承諾

정답：B,D,F,G,H,J

설명:
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 9.3 requires top management to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness1. Clause 9.2 requires the organization to conduct internal audits at planned intervals to provide information on whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022, and is effectively implemented and maintained1. Therefore, when reviewing the audit process and audit findings as a final check before the external certification body arrives, an internal ISMS auditor should verify that these clauses are met in accordance with the audit criteria.
Six of the following statements would cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* The audit programme shows management reviews taking place at irregular intervals during the year:
This statement would cause concern because it implies that the organization is not conducting management reviews at planned intervals, as required by clause 9.3. This may affect the ability of top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS.
* The audit programme does not take into account the relative importance of information security processes: This statement would cause concern because it implies that the organization is not applying a risk-based approach to determine the audit frequency, methods, scope and criteria, as recommended by ISO 19011:2018, which provides guidelines for auditing management systems2. This may affect the ability of the organization to identify and address the most significant risks and opportunities for its ISMS.
* Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date: This statement would cause concern because it implies that the organization is not establishing audit criteria for each internal audit, as required by clause 9.2. Audit criteria are the set of policies, procedures or requirements used as a reference against which audit evidence is compared2.
Without audit criteria, it is not possible to determine whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022.
* Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes: This statement would cause concern because it implies that the organization is not evaluating the effectiveness of ISMS processes, as required by clause 9.1. Effectiveness is the extent to which planned activities are realized and planned results achieved2. Efficiency is the relationship between the result achieved and the resources used2. Both aspects are important for measuring and evaluating ISMS performance and improvement.
* The audit programme does not take into account the results of previous audits: This statement would cause concern because it implies that the organization is not using the results of previous audits as an input for planning and conducting subsequent audits, as recommended by ISO 19011:20182. This may affect the ability of the organization to identify and address any recurring or unresolved issues or nonconformities related to its ISMS.
* Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme: This statement would cause concern because it implies that the organization is not verifying that top management demonstrates leadership and commitment with respect to its ISMS, as required by clause 5.1. This may affect the ability of top management to ensure that the

ISMS policy and objectives are established and compatible with the strategic direction of the organization; that roles, responsibilities and authorities for relevant roles are assigned and communicated; that resources needed for the ISMS are available; that communication about information security matters is established; that continual improvement of the ISMS is promoted; that other relevant management reviews are aligned with those of information security; and that support is provided to other relevant roles1.
The other statements would not cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific format or media for documenting or storing audit reports, as long as they are controlled according to clause 7.5.
* The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for auditor independence, as long as the audit is conducted objectively and impartially, in accordance with ISO 19011:20182.
* The audit programme does not reference audit methods or audit responsibilities: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for referencing audit methods or audit responsibilities in the audit programme, as long as they are defined and documented according to ISO 19011:20182.
* The audit process states the results of audits will be made available to 'relevant' managers, not top management: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for communicating the results of audits to top management, as long as they are reported to the relevant parties and used as an input for management review, according to clause 9.3.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

질문 # 198
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。高階管理人員對審查結果表示不滿，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：
審計團隊在處理財務報告系統相關問題時，是否遵循了最佳審計實務？

- A. 不，審計團隊應該因為該行為的非法性質而退出審計。
- B. 是的，因為這超出了審計範圍。
- C. 不，審核團隊應該聯絡認證機構並報告情況。

정답：C

설명：

Comprehensive and Detailed In-Depth Explanation:
* B. Correct Answer:
* The financial reporting system issue is a critical security concern, and the audit team should have reported the situation to the certification body for further action.
* ISO 19011:2018 mandates auditors to escalate issues that impact compliance.
* A. Incorrect:
* Financial systems fall within ISMS scope if they contain sensitive data-it is not beyond the scope.
* C. Incorrect:
* Withdrawal is unnecessary unless legal violations prevent an effective audit.
Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2 (Internal Audit) & ISO 19011:2018 Clause 6.7 (Audit Follow-Up and Reporting of Serious Issues)

질문 # 199
.....

- scalar.usc.edu, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, scalar.usc.edu, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, estar.jp, fortunetelleroracle.com, fortunetelleroracle.com, www.impactio.com, www.slideshare.net, camp-fire.jp, Disposable vapes