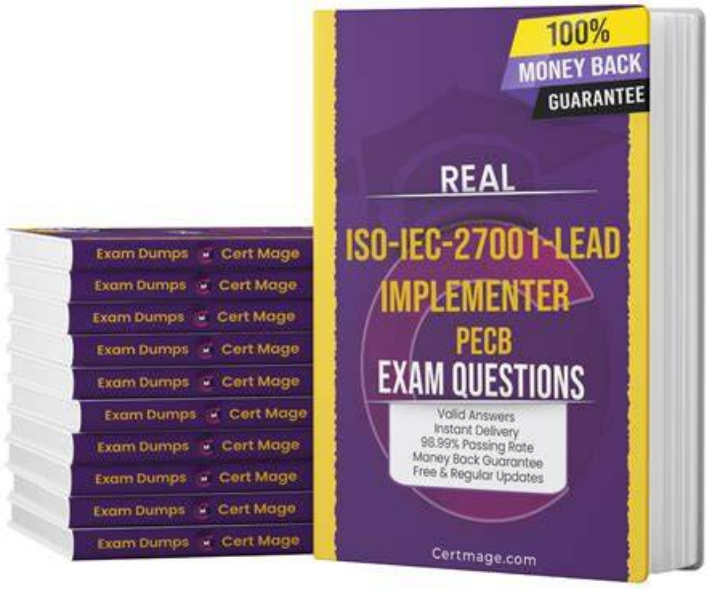
Dumps PECB ISO-IEC-27001-Lead-Auditor-CN PDF & New ISO-IEC-27001-Lead-Auditor-CN Test Prep



What's more, part of that Dumps4PDF ISO-IEC-27001-Lead-Auditor-CN dumps now are free: https://drive.google.com/open?id=1YArv5MWtdJemJFnH3r_6nD_6CgLix8fe

Of course, the future is full of unknowns and challenges for everyone. Even so, we all hope that we can have a bright future. Pass the ISO-IEC-27001-Lead-Auditor-CN exam, for most people, is an ability to live the life they want, and the realization of these goals needs to be established on a good basis of having a good job. A good job requires a certain amount of competence, and the most intuitive way to measure competence is whether you get a series of the test ISO-IEC-27001-Lead-Auditor-CN Certification and obtain enough qualifications.

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

Section	Weight	Objectives
Information Security Controls (ISO/IEC 27002:2022)	25%	- Control categories and implementation guidance • 1. Technological controls • 2. People controls • 3. Physical controls • 4. Organizational controls
Fundamental Concepts of Information Security	15%	- Information security principles and definitions • 1. Risk management fundamentals • 2. Confidentiality, integrity, availability - Overview of ISO/IEC 27000 family of standards • 1. Structure and scope of ISO/IEC 27000 series • 2. Relationship between ISO/IEC 27001 and other standards

Requirements of ISO/IEC 27001:2022	30%	- Support, operation, performance evaluation and improvement • 1. Corrective action and continual improvement • 2. Internal audit and management review • 3. Resource management and competence - Leadership and planning • 1. Information security objectives and risk treatment planning • 2. Management commitment and policy establishment - General requirements and ISMS scope definition • 1. Understanding the organization and its context • 2. Determining ISMS boundaries and applicability
Auditing Principles and Practices	30%	- Audit execution • 1. Conducting interviews and document reviews • 2. Identifying nonconformities and opportunities for improvement • 3. Collecting and verifying audit evidence - Audit preparation and planning • 1. Defining audit scope, criteria and methodology • 2. Development of audit plan and checklist - Audit concepts and principles • 1. Independence, objectivity and evidence-based approach • 2. Audit types and objectives - Audit reporting and follow-up • 1. Corrective action verification and closure • 2. Structure and content of audit report

Get Ready for ISO-IEC-27001-Lead-Auditor-CN with PECB's Updated Dumps and Stay Current with Free Updates for 1 Year

We can make sure that if you purchase our ISO-IEC-27001-Lead-Auditor-CN exam questions, you will have the right to enjoy our perfect after sale service and the high quality products. So do not hesitate and buy our ISO-IEC-27001-Lead-Auditor-CN study guide, we believe you will find surprise from our exam products. And not only you can enjoy the service before you pay for our ISO-IEC-27001-Lead-Auditor-CN learning guide, you can also have the right to have free updates for one year after your purchase.

PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) Sample Questions (Q380-Q385):

NEW QUESTION # 380
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，收集客戶數據，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戶服務水準。

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85%的聊天查詢。
公司成功整合聊天機器人後，將其發布供客戶使用。然而，該聊天機器人卻出現了幾個問題。由於測試不足，且在訓練階段(本應學習查詢模式)缺乏樣本數據，聊天機器人無法有效解答用戶查詢。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戶的諮詢，導致傳統客服人員不堪重負，無法幫助客戶處理他們的要求。
意識到潛在風險，Fintive決定實施一系列新的控制措施。這些措施包括啟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、定期執行存取審查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查。
問題
基於上述情況，為了確保資訊隱私安全，Fintive決定實施安全控制措施。這種做法是否可以接受？

- A. 不，因為在聊天機器人之上實施過多的控制可能會導致組織效率下降。
- B. 是的，但前提是安全控制措施不會幹擾 Fintive 的日常運作。
- C. 是的，為了確保資訊隱私，組織必須實施安全控制。

Answer: C

Explanation:
From Exact Extract:
1. ISO/IEC 27001:2022 - Obligation to implement security controls
ISO/IEC 27001:2022 requires organizations to implement information security controls to address identified risks, particularly where personally identifiable information (PII) is processed.
Under Clause 6.1.3 - Information security risk treatment, the standard requires that an organization:
"Determine all controls that are necessary to implement the information security risk treatment option(s) chosen." In this scenario, the chatbot introduced new and unmitigated risks, including:
* Incorrect handling of user input
* Potential unauthorized disclosure of information (sending random files)
* Processing of PII without sufficient safeguards
Therefore, implementing additional security controls is mandatory, not optional.
2. ISO/IEC 27002:2022 - Privacy and monitoring controls
The controls implemented by Fintive directly align with Annex A of ISO/IEC 27002:2022, including:
* A.5.34 - Privacy and protection of PIIRequires organizations to protect personal data in line with legal, regulatory, and contractual requirements.
* A.8.15 - LoggingRequires audit logs to be enabled to record events for investigation.
* A.8.16 - Monitoring activitiesRequires monitoring systems to detect anomalous behavior.
* A.5.18 - Access rightsRequires periodic access reviews to prevent unauthorized access.
These controls are explicitly designed to detect errors, misuse, unauthorized access, and suspicious behavior
- exactly the risks described in the scenario.
3. Why the other options are incorrect
* Option A - IncorrectISO/IEC 27001 does not permit organizations to avoid implementing controls simply because they may affect operations. Operational impact is considered during risk assessment, but security and privacy obligations take precedence, especially for PII.
* Option B - IncorrectISO/IEC 27001 does not limit the number of controls. Controls must be appropriate to the risk, not minimized for efficiency. A reduction in efficiency does not justify non- compliance or privacy violations.
4. Auditor conclusion
Implementing security controls to protect information privacy is:
* Required by ISO/IEC 27001:2022
* Consistent with ISO/IEC 27002:2022 Annex A controls
* Appropriate given the identified risks
* A correct application of risk treatment and continual improvement

NEW QUESTION # 381
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、智慧財產權、銀行和金融服務領域的客戶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 內部審核兩年了。
現在，他們已向知名且值得信賴的認證機構ISMA申請ISO/IEC 27001認證。
在第一階段審核期間，審核小組審查了實施過程中所建立的所有 ISMS 文件。
他們還審查和評估了管理審查和內部審計的記錄。

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，因此審核組約談了內部審核員。訪談透過提供對內部稽核計畫和程序的詳細了解，驗證了內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。在資訊安全政策審查期間，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，審核小組檢查了 15 份員工培訓記錄（共 50 份），得出的結論是 Lawsy 符合 ISO/IEC 27001 有關培訓和意識的要求。為了支持這個結論，他們影印了檢查過的員工訓練記錄。
根據上述場景，回答以下問題：
審計小組複印了所檢查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？請參閱場景 7。

- A. 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
- B. 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
- 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: A

Explanation:
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 # 382
您是經驗豐富的 ISMS 審核團隊領導，指導審核員進行培訓。您決定透過詢問她一系列問題來測試她對後續審核的了解。這是您的問題和她的答案。
她正確回答了您的哪四個問題？

- A. 問：後續審核是否應該尋求發現新的不合格項？答：是的
- B. 問：後續審核的結果是否該向審核客戶報告？答：沒有
- C. 問：後續審核是否應該考慮商定的改進機會以及糾正措施？
  年
- D. 問：後續審核的目的是驗證糾正、糾正措施和改進機會的完成嗎？答：是的
- E. 問：如果需要，後續審核的結果是否可以成為另一次後續審核？答：是的
- F. 問：後續審核是否應確保不合格問題得到有效解決？答：是的
- G. 問：所有審核都需要後續審核嗎？答：沒有
- H. 問：後續審核的結果是否應該向負責最初識別 NC 審核的審核組組長報告？答：是的

Answer: D,E,F,G

Explanation:
Based on the understanding of follow-up audits, especially in the context of Information Security Management Systems (ISMS) and the guidelines provided by ISO 19011:2018, here are the four questions from your list that the auditor in training has answered correctly:
B: Q: Should follow-up audits seek to ensure nonconformities have been effectively addressed? A: YES This is correct. The primary purpose of follow-up audits is to verify that nonconformities identified in previous audits have been effectively addressed and the corrective actions taken are suitable and effective.
D: Q: Is the purpose of a follow-up audit to verify the completion of corrections, corrective actions, and opportunities for improvement? A: YES Yes, the follow-up audit aims to verify the completion and effectiveness of corrections and corrective actions. It may also consider the implementation of opportunities for improvement identified during the initial audit.
E: Q: Are follow-up audits required for all audits? A: NO This is correct. Follow-up audits are not automatically required for all audits. They are typically conducted when nonconformities or other significant issues were identified in an earlier audit and there's a need to verify the implementation and effectiveness of the corrective actions.
H: Q: Could an outcome from a follow-up audit be another follow-up audit if required? A: YES Yes, this is a possible outcome. If

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

NEW QUESTION # 383
作為 ISMS 實施的一部分，行銷機構開發了自己的風險評估方法。這是可以接受的嗎？

- A. 否，實施 ISMS 時，應使用 ISO/IEC 27001 提供的風險評估方法
- B. 是的，可以使用任何符合 ISO/IEC 27001 要求的風險評估方法
- C. 是，只有當風險評估方法與公認的風險評估方法一致時

Answer: B

Explanation:
ISO/IEC 27001 does not mandate the use of a specific risk assessment methodology. Organizations are free to choose their own approach as long as it is systematic, consistent, and capable of producing valid and comparable results. This allows organizations, such as the marketing agency in the question, to adapt the methodology to suit their specific needs and business context, provided it complies with the requirements set out in the standard.
References: PECB ISO/IEC 27001 Lead Auditor Course Materials; ISO/IEC 27001:2013 Standard, Clause
6.1.2.

NEW QUESTION # 384
您是一位經驗豐富的 ISMS 審核團隊領導，為審核員提供培訓指導。她問您為什麼制定與不合格品分級相關的具體標準很重要。
下列哪一項答案是正確的？

- A. 因為評分標準將確保所有審核員以完全相同的方式對不合格項進行評分
- B. 因為 ISO/IEC 27001:2022 要求它
- C. 因為分級標準為評估整個組織的不合格項提供了共同基礎
- D. 因為評分標準的建立和實施顯示了對糾正措施流程的高度承諾

Answer: C

Explanation:
The correct response is A, because grading criteria provide a common basis for the evaluation of nonconformities across the organization. Grading criteria are the rules or standards that define the severity or impact of nonconformities, and help to determine the appropriate corrective actions and follow-up activities. Grading criteria are important for several reasons, such as:
They ensure consistency and objectivity in the assessment and reporting of nonconformities, and avoid subjective or arbitrary judgments.
They facilitate the communication and understanding of nonconformities among the auditors, the auditees, and the audit clients, and enable the comparison and benchmarking of nonconformities across different processes, functions, or locations.
They support the prioritization and allocation of resources for the resolution of nonconformities, and the monitoring and measurement of the effectiveness of the corrective actions.

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

NEW QUESTION # 385
.....

In order to gain more competitive advantages when you are going for a job interview, more and more people have been longing to get a ISO-IEC-27001-Lead-Auditor-CN certification. They think the certification is the embodiment of their ability; they are already convinced that getting a ISO-IEC-27001-Lead-Auditor-CN certification can help them look for a better job. There is no doubt that it is very difficult for most people to pass the exam and have the certification easily. If you are also weighted with the trouble about a ISO-IEC-27001-Lead-Auditor-CN Certification, we are willing to soothe your trouble and comfort you.