

ISO-IEC-27001-Lead-Auditor-CN Frequent Updates | Test ISO-IEC-27001-Lead-Auditor-CN Lab Questions



DOWNLOAD the newest Prep4sureExam ISO-IEC-27001-Lead-Auditor-CN PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1LjLwDYktm3najeLw2fyBZwbIUkNkrQbn>

Thanks to modern technology, learning online gives people access to a wider range of knowledge, and people have got used to convenience of electronic equipment. As you can see, we are selling our ISO-IEC-27001-Lead-Auditor-CN learning guide in the international market, thus there are three different versions of our ISO-IEC-27001-Lead-Auditor-CN exam materials: PDF, Soft and APP versions. It is worth mentioning that, the simulation test of our ISO-IEC-27001-Lead-Auditor-CN Study Guide is available in our software version. With the simulation test, all of our customers will get accustomed to the ISO-IEC-27001-Lead-Auditor-CN exam easily, and pass the exam with confidence.

Our ISO-IEC-27001-Lead-Auditor-CN real materials support your preferences of different practice materials, so three versions are available. PDF version - legible to read and remember, support customers' printing request. Software version of ISO-IEC-27001-Lead-Auditor-CN real materials - supporting simulation test system, and support Windows system users only. App online version of ISO-IEC-27001-Lead-Auditor-CN Guide question - suitable to all kinds of equipment or digital devices, supportive to offline exercises on the condition that you practice it without mobile data. You can take a look of these ISO-IEC-27001-Lead-Auditor-CN exam dumps and take your time to decide.

>> ISO-IEC-27001-Lead-Auditor-CN Frequent Updates <<

Free PDF Quiz 2026 Unparalleled PECB ISO-IEC-27001-Lead-Auditor-CN Frequent Updates

To become more powerful and struggle for a new self, getting a professional ISO-IEC-27001-Lead-Auditor-CN certification is the first step beyond all questions. We suggest you choose our ISO-IEC-27001-Lead-Auditor-CN test prep ----an exam braindump leader in the field. Since we release the first set of the ISO-IEC-27001-Lead-Auditor-CN quiz guide, we have won good response from our customers and until now---a decade later, our products have become more mature and win more recognition. And our ISO-IEC-27001-Lead-Auditor-CN Exam Torrent will also be sold at a discount from time to time and many preferential activities are waiting for you.

PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) Sample Questions (Q37-Q42):

NEW QUESTION # 37

AppFolk 是一家軟體開發公司，正在尋求 ISO/IEC 27001 認證。都包括在內。這是可以接受的嗎？

- A. 是的，審核和 ISMS 範圍不一定需要相同
- B. 不，對被審核方所在工業部門不重要的部門可以排除在審核範圍之外
- C. 不，審核範圍應反映 ISMS 涵蓋的組織的所有部門

Answer: C

Explanation:

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

NEW QUESTION # 38

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。

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 the cloud server remotely. No further action is needed.	24 hours

您想進一步調查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. 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）
- B. 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）
- C. 收集更多證據，說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）
- 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）
- F. 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）

Answer: B,E

Explanation:

*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 organization 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 # 39

設想:

Northstorm 是一家線上零售商店，提供獨特的復古和現代配件。它最初進入了一個小型市場，但隨著整個電子商務格局的發展而逐漸發展壯大。Northstorm 專門在線上工作，確保高效的付款處理、庫存管理、行銷工具和出貨訂單。它採用優先排序來接收、補貨和運送其最受歡迎的產品。

Northstorm 傳統上透過託管其網站並完全控制其基礎架構（包括硬體、軟體和資料管理）來管理其 IT 營運。然而，由於缺乏響應的基礎設施，這種方法阻礙了其發展。為了增強其電子商務和支付系統，Northstorm 選擇擴展其內部資料中心，並在三個月內分兩個階段完成擴建。最初，該公司升級了其核心伺服器、銷售點、訂購、計費、資料庫和備份系統。第二階段涉及改善郵件、付款和網路功能。此外，在此階段，Northstorm 採用了針對個人識別資訊 (PII) 控制者和 PII 處理者的國際標準，以確保其資料處理實務安全並符合全球法規。

儘管進行了擴張，但 Northstorm 升級後的資料中心仍未能滿足其不斷變化的業務需求。這種不足導致了一些新的挑戰，包括訂單優先事項問題。客戶報告未收到優先訂單，且公司難以迅速回應。這主要是因為主伺服器無法處理來自 YouDecide 的訂單，YouDecide 是一款旨在優先處理訂單和模擬客戶互動的應用程式。該應用程式依賴先進的演算法，與升級期間安裝的新作業系統 (OS) 不相容。

面對緊急的兼容性問題，Northstorm 在沒有經過適當驗證的情況下迅速修補了應用程式，導致安裝了受損版本。這次安全漏洞導致主伺服器受到影響，該公司的網站離線一週。認識到需要更可靠的解決方案，該公司決定將其網站託管外包給電子商務提供者。該公司簽署了有關產品所有權的保密協議，並在過渡之前對使用者存取權限進行了徹底審查，以增強安全性。

根據情境 1，Northstorm 在第二階段的擴張中採用了哪一種國際標準？

- A. ISO/IEC 27009
- **B. ISO/IEC 27701**
- C. ISO/IEC 27003

Answer: B

Explanation:

Comprehensive and Detailed In-Depth

Northstorm adopted an international standard for Personally Identifiable Information (PII) controllers and PII processors to ensure its data handling practices were secure and compliant with global regulations. This aligns directly with ISO/IEC 27701, which extends ISO/IEC 27001 and ISO/IEC 27002 to cover Privacy Information Management Systems (PIMS), specifically addressing the protection of PII.

A. ISO/IEC 27701 - Correct Answer. This standard is designed for organizations acting as PII controllers and processors and provides guidelines on privacy management, regulatory compliance, and data protection.

B. ISO/IEC 27009 - Incorrect because this standard provides guidance on sector-specific requirements for ISMS, not privacy or PII protection.

C. ISO/IEC 27003 - Incorrect because it provides general implementation guidance for ISMS, not specific controls for PII processing.

NEW QUESTION # 40

您正在療養院進行 ISMS 審核，療養院的住戶總是戴著電子腕帶來監測他們的位置、心跳和血壓。腕帶會自動將這些資料上傳到雲端伺服器，供工作人員進行醫療保健監控和分析。

您現在希望驗證最高管理層是否已制定資訊安全策略和目標。您正在對行動裝置策略進行抽樣，並確定該策略的安全目標是「確保遠端辦公和行動裝置使用的安全」。

禁止個人行動裝置連接至療養院網路、處理和儲存居民資料。

本公司在 ISMS 範圍內的行動裝置應在資產登記冊中登記。

本公司的行動裝置應實施或啟用實體保護，即密碼保護的螢幕鎖定/解鎖、臉部或指紋解鎖裝置。

本公司的行動裝置應定期備份。

若要驗證行動裝置策略和目標是否已實施且有效，請為稽核追蹤選擇三個選項。

- A. 從值班醫護人員處抽取部分行動設備，並與資產登記冊驗證行動裝置資訊
- B. 探訪設備供應商，確保他們了解 ISMS 政策
- C. 查看內部審核報告以確保 IT 部門已接受審核
- D. 檢查資產註冊以確保所有個人行動裝置已註冊
- E. 查看訪客登記簿，確保任何訪客都不能在療養院內攜帶個人手機
- F. 與高階主管面談，核實他們參與制定資訊安全政策和資訊安全目標的情況
- G. 檢查資產註冊以確保所有公司的行動裝置已註冊
- H. 與接待人員面談，確保在進入療養院之前檢查所有訪客和員工的行李

Answer: A,C,G

Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 5.2 requires top management to establish an information security policy that provides the framework for setting information security objectives. Clause 6.2 requires top management to ensure that the information security objectives are established at relevant functions and levels. Therefore, when verifying that the information security policy and objectives have been established by top management, an ISMS auditor should review relevant documents and records that demonstrate top management's involvement and commitment.

To verify that the mobile device policy and objectives are implemented and effective, an ISMS auditor should review relevant documents and records that demonstrate how the policy and objectives are communicated, monitored, measured, analyzed, and evaluated. The auditor should also sample and verify the implementation of the controls that are stated in the policy.

Three options for the audit trail that are relevant to verifying the mobile device policy and objectives are:

Review the internal audit report to make sure the IT department has been audited: This option is relevant because it can provide evidence of how the IT department, which is responsible for managing the mobile devices and their security, has been evaluated for its conformity and effectiveness in implementing the mobile device policy and objectives. The internal audit report can also reveal any nonconformities, corrective actions, or opportunities for improvement related to the mobile device policy and objectives.

Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register: This option is relevant because it can provide evidence of how the mobile devices that are used by the medical staff, who are involved in processing and storing residents' data, are registered in the asset register and have physical protection enabled. This can verify the implementation and effectiveness of two of the controls that are stated in the mobile device policy.

Review the asset register to make sure all company's mobile devices are registered: This option is relevant because it can provide evidence of how the company's mobile devices that are within the ISMS scope are identified and accounted for. This can verify the implementation and effectiveness of one of the controls that are stated in the mobile device policy.

The other options for the audit trail are not relevant to verifying the mobile device policy and objectives, as they are not related to the policy or objectives or their implementation or effectiveness. For example:

Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding physical security or access control, but not specifically to mobile devices.

Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security awareness or compliance, but not specifically to mobile devices.

Interview the supplier of the devices to make sure they are aware of the ISMS policy: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security within supplier relationships, but not specifically to mobile devices.

Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to verifying that the information security policy and objectives have been established by top management, but not specifically to mobile devices.

NEW QUESTION # 41

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三方審核。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 個月內離開的 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 小時內刪除存取權限。

當被審核方被問及為何延遲刪除訪問權限時，他們回答說，“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. 同意針對 5.18 提出輕微不符合項。
- B. 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。
- C. 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。
- D. 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。
- **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. 不同意提出輕微不符合項，有足夠的證據證明昇級為重大不符合項是合理的。

Answer: E

NEW QUESTION # 42

.....

In reaction to the phenomenon, therefore, the ISO-IEC-27001-Lead-Auditor-CN test material is reasonable arrangement each time the user study time, as far as possible let users avoid using our latest ISO-IEC-27001-Lead-Auditor-CN exam torrent for a long period of time, it can better let the user attention relatively concentrated time efficient learning. The ISO-IEC-27001-Lead-Auditor-CN practice materials in every time users need to master the knowledge, as long as the user can complete the learning task in this period, the ISO-IEC-27001-Lead-Auditor-CN test material will automatically quit learning system, to alert users to take a break, get ready for the next period of study.

Test ISO-IEC-27001-Lead-Auditor-CN Lab Questions: <https://www.prep4sureexam.com/ISO-IEC-27001-Lead-Auditor-CN-dumps-torrent.html>

These two versions of our ISO-IEC-27001-Lead-Auditor-CN practice guide helps you to test your knowledge and over the exam anxiety, PECB ISO-IEC-27001-Lead-Auditor-CN Frequent Updates In addition to that CCNA voice official exam certification guide PDF is supplied by Cisco, PECB ISO-IEC-27001-Lead-Auditor-CN Frequent Updates All questions are mention in these PDF files, PECB ISO-IEC-27001-Lead-Auditor-CN Frequent Updates If 100% success, free updates, free demos, and a money-back guarantee are not enough to make your mind.

Placing a blood pressure cuff on the arm, Home ISO-IEC-27001-Lead-Auditor-CN is where my main office sits, where I get all of my work done, and where you can find me most days, These two versions of our ISO-IEC-27001-Lead-Auditor-CN Practice Guide helps you to test your knowledge and over the exam anxiety.

Professional ISO-IEC-27001-Lead-Auditor-CN Frequent Updates Covers the Entire Syllabus of ISO-IEC-27001-Lead-Auditor-CN

In addition to that CCNA voice official exam certification guide PDF is supplied Certification ISO-IEC-27001-Lead-Auditor-CN Dump by Cisco, All questions are mention in these PDF files, If 100% success, free updates, free demos, and a money-back guarantee are not enough to make your mind.

Nobody wants to be stranded in the same position in his or her company.

- Free ISO-IEC-27001-Lead-Auditor-CN Exam Questions Latest ISO-IEC-27001-Lead-Auditor-CN Test Guide Test ISO-IEC-27001-Lead-Auditor-CN Price Immediately open (www.examcollectionpass.com) and search for **【 ISO-IEC-27001-Lead-Auditor-CN 】** to obtain a free download ISO-IEC-27001-Lead-Auditor-CN Latest Study Questions
- Braindumps ISO-IEC-27001-Lead-Auditor-CN Downloads Latest Braindumps ISO-IEC-27001-Lead-Auditor-CN Ebook Reliable ISO-IEC-27001-Lead-Auditor-CN Exam Testking Easily obtain free download of ISO-IEC-27001-Lead-Auditor-CN by searching on www.pdfvce.com  Braindumps ISO-IEC-27001-Lead-Auditor-CN Downloads
- ISO-IEC-27001-Lead-Auditor-CN New Test Bootcamp Unlimited ISO-IEC-27001-Lead-Auditor-CN Exam Practice Valid Braindumps ISO-IEC-27001-Lead-Auditor-CN Pdf Download 《 ISO-IEC-27001-Lead-Auditor-CN 》 for free by simply searching on www.prepawaypdf.com ISO-IEC-27001-Lead-Auditor-CN Latest Practice Questions
- ISO-IEC-27001-Lead-Auditor-CN Latest Practice Questions ISO-IEC-27001-Lead-Auditor-CN Reliable Test Vce ISO-IEC-27001-Lead-Auditor-CN Reliable Test Vce Search for ISO-IEC-27001-Lead-Auditor-CN and download it for free immediately on www.pdfvce.com Test ISO-IEC-27001-Lead-Auditor-CN Price
- Valid Braindumps ISO-IEC-27001-Lead-Auditor-CN Pdf ISO-IEC-27001-Lead-Auditor-CN Reliable Test Duration

