

# **ISO-IEC-27001-Lead-Auditor-CN Study Materials: PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) - ISO-IEC-27001-Lead-Auditor-CN Actual Questions & ISO-IEC-27001-Lead-Auditor-CN Quiz Guide**



P.S. Free & New ISO-IEC-27001-Lead-Auditor-CN dumps are available on Google Drive shared by ITExamSimulator:  
<https://drive.google.com/open?id=1Nt43zLUmmvKaj58Rp9zVqYDsAnGXuQAV>

There is no doubt that we all dream of working for top companies around the globe. Some people make it through but some keep on thinking about how to break that glass. If you are among those who belong to the latter category, you should start the preparations for the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) (ISO-IEC-27001-Lead-Auditor-CN) certification exam to improve your knowledge, expertise and crack even the toughest interview easily.

Are you an exam jittering? Are you like a cat on hot bricks before your driving test? Do you have put a test anxiety disorder? If your answer is yes, we think that it is high time for you to use our ISO-IEC-27001-Lead-Auditor-CN Exam Question. Our study materials have confidence to help you pass exam successfully and get related certification that you long for, and we can guarantee that if you don't pass the exam, we will give you full refund.

**>> Current ISO-IEC-27001-Lead-Auditor-CN Exam Content <<**

## **ISO-IEC-27001-Lead-Auditor-CN Test Questions Fee & Exam ISO-IEC-27001-Lead-Auditor-CN Pattern**

Dear, when you find PECB ISO-IEC-27001-Lead-Auditor-CN practice training, please assess it with careful analysis and do not miss it any more. The ISO-IEC-27001-Lead-Auditor-CN free demo is available and accessible for download. You can have a try and do your decision. In addition, it is very easy to make an order with our streamline process. Then you can get the ISO-IEC-27001-Lead-Auditor-CN Test Dumps in about 5-10 mins after payment and instant download it, and start study. 100% is the guarantee of us, so please test assured to purchase ISO-IEC-27001-Lead-Auditor-CN practice torrent.

## PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) Sample Questions (Q300-Q305):

### NEW QUESTION # 300

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、控制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:

哪個選項可以證明不利的認證建議是合理的?請參閱場景 8。

- A. 與缺乏資訊標籤程序相關的輕微不合格項
- B. 提交的行動計劃的不切實際的日期(兩週)
- C. 與在可移動媒體中儲存敏感資訊相關的主要不符合項

**Answer: C**

Explanation:

The major nonconformity related to storing sensitive information in removable media justifies the unfavorable recommendation for certification. This issue directly contradicts the information classification scheme's stipulations, indicating a significant oversight in enforcing the ISMS policies.

### NEW QUESTION # 301

管理審核計畫的個人負責下列哪六項行動?

- A. 定義單獨審核的目標、範圍和標準
- B. 選擇審核團隊
- C. 確定審核計畫所需的資源
- D. 審核期間與受審核方的溝通
- E. 建立審核計畫
- F. 保留審核結果的記錄資訊
- G. 確定審核計畫的範圍
- H. 定義單獨審核的計畫

**Answer: A,B,E,F,G,H**

Explanation:

According to ISO 19011:2018, which provides guidelines for auditing management systems, an audit programme is a set of one or more audits planned for a specific time frame and directed towards a specific purpose<sup>1</sup>. The individual(s) managing the audit programme are responsible for establishing, implementing and maintaining the audit programme in accordance with the organization's policies and objectives<sup>1</sup>. This includes defining the extent of the audit programme based on strategic direction, risks and opportunities; establishing the audit programme by defining its objectives, scope and criteria; determining the resources necessary for the audit programme; selecting competent auditors and assigning them to appropriate audits; defining the objectives, scope and criteria for each individual audit; defining the plan of each individual audit; retaining documented information of the audit results; reviewing and improving the performance of the audit programme<sup>1</sup>. Therefore, these six actions are part of the responsibilities of the

individual(s) managing the audit programme. The other option, communicating with the auditee during the audit, is not a responsibility of the individual(s) managing the audit programme, but rather a responsibility of the audit team leader<sup>1</sup>. Reference: ISO 19011:2018 - Guidelines for auditing management systems

### NEW QUESTION # 302

下列敘述中哪兩項是正確的？

- A. 該組織不得將審查立法環境以確保遵守法律法規的任務外包。
- B. 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。
- C. 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。
- D. 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。
- E. 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。
- F. 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。

**Answer: C,F**

Explanation:

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 # 303

作為審計員，您已經注意到 ABC Inc. 已製定了管理可移動儲存媒體的程序。該程式基於 ABC Inc. 採用的分類方案。另一方面，被歸類為「公共」的資訊沒有保密要求：因此，僅適用確保其完整性和可用性的程序。這是什麼類型的審計結果？

- A. 一致性
- B. 異常
- C. 不合格

**Answer: A**

Explanation:

This scenario represents a conformity because ABC Inc. has implemented procedures for managing removable storage media that align with the classification scheme of the information stored. When information is classified as "confidential," more stringent procedures apply, whereas for "public" information, the procedures focus only on integrity and availability, following the organization's defined information classification policy.

### NEW QUESTION # 304

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。

PECB

iteksam simulator.com

Appoint an audit team leader

Issue the report

To complete the sequence 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 the options to the appropriate blank section.

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

**Answer:**

**Explanation:**

Appoint an audit team leader

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

To complete the sequence 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 the options to the appropriate blank section.

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

**Explanation:**

Appoint an audit team leader

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

To complete the sequence 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 the options to the appropriate blank section.

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

PECB

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 manner<sup>12</sup>.

\* 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 observations<sup>123</sup>.

\* 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 elements<sup>123</sup>:

- \* 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 accordingly<sup>123</sup>.

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 # 305

.....

If you download and install on your personal computer online, you can copy to any other electronic products and use offline. The software test engine of PECB ISO-IEC-27001-Lead-Auditor-CN is very practical. You can study any time anywhere you want. Comparing to PDF version, the software test engine of PECB ISO-IEC-27001-Lead-Auditor-CN also can simulate the real exam scene so that you can overcome your bad mood for the real exam and attend exam casually.

**ISO-IEC-27001-Lead-Auditor-CN Test Questions Fee:** <https://www.itexamsimulator.com/ISO-IEC-27001-Lead-Auditor-CN-brain-dumps.html>

About your blurry memorization of the knowledge, our ISO-IEC-27001-Lead-Auditor-CN learning materials can help them turn to very clear ones, So lots of IT candidates feel confused, but considering a better job and good social status, they still seek for the valid and useful PECB ISO-IEC-27001-Lead-Auditor-CN Test Questions Fee ISO-IEC-27001-Lead-Auditor-CN Test Questions Fee - PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) practice dumps, PECB Current ISO-IEC-27001-Lead-Auditor-CN Exam Content If you are looking for valid & useful test braindumps, our products are suitable for you.

Using the Site Definition Wizard, [privacy\\_icons.jpg](#) Click to view larger image, About your blurry memorization of the knowledge, our ISO-IEC-27001-Lead-Auditor-CN Learning Materials can help them turn to very clear ones.

## Latest PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) real exams, ISO-IEC-27001-Lead-Auditor-CN vce dumps

So lots of IT candidates feel confused, but considering a ISO-IEC-27001-Lead-Auditor-CN better job and good social status, they still seek for the valid and useful PECB PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版) practice dumps.

If you are looking for valid & useful test Exam ISO-IEC-27001-Lead-Auditor-CN Pattern braindumps, our products are suitable for you, You must first register PECB ISO-IEC-27001-Lead-Auditor-CN exam, Our updated ISO-IEC-27001-Lead-Auditor-CN Dumps questions are the perfect way to prepare for the exam quickly and effectively.

- Efficient and Convenient Preparation with [www.exam4labs.com](http://www.exam4labs.com)'s Updated PECB ISO-IEC-27001-Lead-Auditor-CN Practice Test  Easily obtain ( ISO-IEC-27001-Lead-Auditor-CN ) for free download through [▶▶](#) [www.exam4labs.com](http://www.exam4labs.com)   Reliable ISO-IEC-27001-Lead-Auditor-CN Exam Testking

