

# New ISO-IEC-27001-Lead-Auditor Braindumps Questions | ISO-IEC-27001-Lead-Auditor Test Guide



DOWNLOAD the newest Braindumpsqa ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free:  
<https://drive.google.com/open?id=1yzCUFPa7gdM0FNWVQpxIbDs60rtS9-O1>

Braindumpsqa has the ability to help IT people for success. Braindumpsqa PECB ISO-IEC-27001-Lead-Auditor exam dumps are the training materials that help you succeed. As long as you want to Pass ISO-IEC-27001-Lead-Auditor Test, you must choose Braindumpsqa. We guarantee your success in the first attempt. If you fail, we will give you a FULL REFUND of your purchasing fee.

PECB ISO-IEC-27001-Lead-Auditor exam is an internationally recognized certification that validates a professional's expertise in auditing and managing information security management systems based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is suitable for professionals who want to pursue a career in information security management, audit, or compliance. ISO-IEC-27001-Lead-Auditor Exam covers various topics related to information security management, including risk management, control objectives, audit techniques, and compliance with legal and regulatory requirements.

>> New ISO-IEC-27001-Lead-Auditor Braindumps Questions <<

## Free PDF Quiz PECB First-grade ISO-IEC-27001-Lead-Auditor - New PECB Certified ISO/IEC 27001 Lead Auditor exam Braindumps Questions

You will get high passing score in the PECB ISO-IEC-27001-Lead-Auditor Real Exam with our valid test questions and answers. Braindumpsqa can provide you with the most reliable ISO-IEC-27001-Lead-Auditor exam dumps and study guide to ensure you get certification smoothly. We guarantee the high accuracy of questions and answers to help candidates pass exam with 100% pass rate.

## PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q156-Q161):

### NEW QUESTION # 156

All are prohibited in acceptable use of information assets, except:

- A. Company-wide e-mails with supervisor/TL permission.
- B. E-mail copies to non-essential readers
- C. Electronic chain letters
- D. Messages with very large attachments or to a large number of recipients.

**Answer: A**

Explanation:

Explanation

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 # 157

Which two of the following are examples of audit methods that 'do' involve human interaction?

- A. Analysing data by remotely accessing the auditee's server
- B. Observing work performed by remote surveillance
- C. Analysing data by remotely accessing the auditee's server
- **D. Performing an independent review of procedures in preparation for an audit**
- **E. Reviewing the auditee's response to an audit finding**

**Answer: D,E**

Explanation:

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 not<sup>2</sup>. 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 exchange<sup>2</sup>. 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. Reference: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

#### NEW QUESTION # 158

Which is the glue that ties the triad together

- **A. Technology**
- B. Collaboration
- C. Process
- D. People

**Answer: A**

Explanation:

The triad refers to the three elements of information security: confidentiality, integrity and availability<sup>3</sup>. Technology is the glue that ties the triad together, as it provides the means to implement various controls and measures to protect information from unauthorized access, modification or loss<sup>3</sup>. Reference: ISO/IEC 27001:2022 Lead Auditor Training Course - BSI

#### NEW QUESTION # 159

Which three of the following phrases are objectives' in relation to an audit?

- A. International Standard

- B. Complete audit on time
- C. Management policy
- D. Regulatory requirements
- E. Identify opportunities for improvement
- F. Confirm the scope of the management system

**Answer: D,E,F**

Explanation:

Explanation

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 system<sup>1</sup>. 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 # 160

Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.

Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.

Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.

During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.

They also reviewed and evaluated the records from management reviews and internal audits.

Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.

The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.

Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.

Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.

During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.

Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.

Based on the scenario above, answer the following question:

Lawsy lacks a procedure regarding the use of laptops outside the workplace and it relies on employees' common knowledge to protect the confidentiality of information stored in the laptops. This presents:

- A. A nonconformity
- B. A conformity
- C. An anomaly

**Answer: A**

Explanation:

Lawsy's lack of specific procedures for the use of laptops outside the workplace, despite allowing such use, represents a nonconformity. ISO/IEC 27001 requires that security controls and management processes be clearly defined, documented, and

implemented. Relying solely on employees' common knowledge does not fulfill the standard's requirements for managing information security risks associated with mobile and teleworking.

### NEW QUESTION # 161

We know deeply that a reliable ISO-IEC-27001-Lead-Auditor exam material is our company's foothold in this competitive market. High accuracy and high quality are the most important things we always looking for. Compared with the other products in the market, our ISO-IEC-27001-Lead-Auditor latest questions grasp of the core knowledge and key point of the real exam, the targeted and efficient PECB Certified ISO/IEC 27001 Lead Auditor exam study training dumps guarantee our candidates to pass the test easily. Passing exam won't be a problem anymore as long as you are familiar with our ISO-IEC-27001-Lead-Auditor Exam Material (only about 20 to 30 hours practice). High accuracy and high quality are the reasons why you should choose us.

- [illegible]