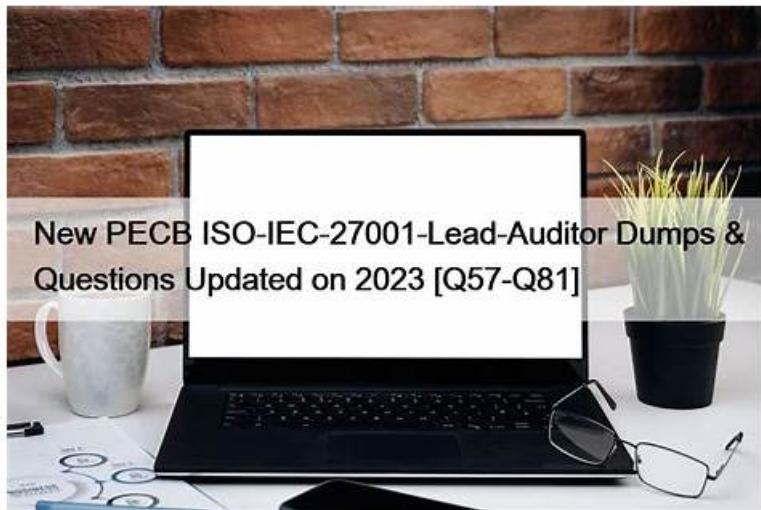


Latest PECB ISO-IEC-27001-Lead-Auditor Test Objectives - ISO-IEC-27001-Lead-Auditor Exam Syllabus



P.S. Free 2025 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by VCEPrep:
<https://drive.google.com/open?id=1W5OUGovEdDGkYfl4JneE4DLFw-jc5gl6>

If you are working all the time, and you hardly find any time to prepare for the ISO-IEC-27001-Lead-Auditor exam, then VCEPrep present the smart way to ISO-IEC-27001-Lead-Auditor exam prep for the exam. You can always prepare for the ISO-IEC-27001-Lead-Auditor test whenever you find free time with the help of our ISO-IEC-27001-Lead-Auditor Pdf Dumps. We have curated all the ISO-IEC-27001-Lead-Auditor questions and answers that you can view the exam PECB ISO-IEC-27001-Lead-Auditor PDF brain dumps and prepare for the exam. We guarantee that you will be able to pass the ISO-IEC-27001-Lead-Auditor in the first attempt.

PECB ISO-IEC-27001-Lead-Auditor exam is designed for professionals who wish to become certified lead auditors in the field of information security management systems (ISMS). ISO-IEC-27001-Lead-Auditor exam is offered by PECB, a well-known certification body that provides training, examination, and certification services for various international standards such as ISO, GDPR, and ITIL. The ISO-IEC-27001-Lead-Auditor Exam aims to assess the knowledge and skills of candidates in leading an ISMS audit team and conducting an audit according to the requirements of ISO/IEC 27001:2013 standard.

>> Latest PECB ISO-IEC-27001-Lead-Auditor Test Objectives <<

ISO-IEC-27001-Lead-Auditor Dumps Torrent: PECB Certified ISO/IEC 27001 Lead Auditor exam & ISO-IEC-27001-Lead-Auditor Exam Bootcamp

We are carrying out renovation about ISO-IEC-27001-Lead-Auditor test engine all the time to meet the different requirements of the diversified production market. Thus we have prepared three kinds of versions on ISO-IEC-27001-Lead-Auditor preparation materials. If you are used to study with paper-based materials you can choose the PDF version of our ISO-IEC-27001-Lead-Auditor Study Guide. If you would like to get the mock test before the real ISO-IEC-27001-Lead-Auditor exam you can choose the software version, and if you want to study in anywhere at any time then our online APP version is your best choice since you can download it in any electronic devices.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q171-Q176):

NEW QUESTION # 171

You are an experienced ISMS audit team leader providing instruction to a class of auditors in training. The subject of today's lesson is the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022.

You provide the class with a series of activities. You then ask the class to sort these activities into the order in which they appear in the standard.

What is the correct sequence they should report back to you?

1 st	
2 nd	
3 rd	
4 th	
5 th	
6 th	

PECB

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.

Create and maintain information security risk criteria	Identify the risks that need to be considered when planning for the information security management system	Assess the potential consequences that would arise if the risk were to materialise	Select appropriate risk treatment options
Carry out information security risk assessments at planned intervals			
Consider the results of risk assessment and the status of the risk treatment plan at management review			

Answer:

Explanation:

1 st	Identify the risks that need to be considered when planning for the information security management system
2 nd	Assess the potential consequences that would arise if the risk were to materialise
3 rd	Select appropriate risk treatment options
4 th	Carry out information security risk assessments at planned intervals
5 th	Consider the results of risk assessment and the status of the risk treatment plan at management review

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.

Create and maintain information security risk criteria	Identify the risks that need to be considered when planning for the information security management system	Assess the potential consequences that would arise if the risk were to materialise	Select appropriate risk treatment options
Carry out information security risk assessments at planned intervals			
Consider the results of risk assessment and the status of the risk treatment plan at management review			

Explanation:

A screenshot of a chat Description automatically generated

1 st	Create and maintain information security risk criteria
2 nd	Identify the risks that need to be considered when planning for the information security management system
3 rd	Assess the potential consequences that would arise if the risk were to materialise
4 th	Select appropriate risk treatment options
5 th	Carry out information security risk assessments at planned intervals
6 th	Consider the results of risk assessment and the status of the risk treatment plan at management review

The correct sequence of activities for the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022 is as follows:

1st: Create and maintain information security risk criteria
 2nd: Identify the risks that need to be considered when planning for the information security management system
 3rd: Assess the potential consequences that would arise if the risk were to materialise
 4th: Select appropriate risk treatment options
 5th: Carry out information security risk assessments at planned intervals
 6th: Consider the results of risk assessment and the status of the risk treatment plan at management review
 This sequence is based on the information security risk management process described in ISO/IEC 27001:2022 clause 6.1, which includes the following activities:

establishing and maintaining information security risk criteria;

ensuring that repeated information security risk assessments produce consistent, valid and comparable results; identifying the information security risks; analyzing the information security risks; evaluating the information security risks; treating the information security risks; accepting the information security risks and the residual information security risks; communicating and consulting with stakeholders throughout the process; monitoring and reviewing the information security risks and the risk treatment plan.

References:

NEW QUESTION # 172

You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.

The audit they have been invited to participate in is a third-party surveillance audit of a data centre. The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.

Select three options that relate to ISO/IEC 27001:2022's requirements regarding external providers.

- A. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
- B. I will ensure the organization has determined the need to communicate with external providers regarding the ISMS
- C. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
- D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
- E. I will ensure that the organization has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
- F. I will ensure external providers have a documented process in place to notify the organization of any risks arising from the use of its products or services
- G. I will ensure that the organization ranks its external providers and allocates the majority of its work to those providers who are rated the highest
- H. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group

Answer: A,F,H

Explanation:

Explanation

* A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organization to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organization. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider¹²

* B. I will ensure external providers have a documented process in place to notify the organization of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO

27001:2022 requires the organization to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organization of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organization. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete¹²

* E. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organization to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organization should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organization should also maintain records of the monitoring, review and evaluation results¹²

* F. I will ensure the organization has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organization to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organization should define the purpose, content, frequency, methods, and responsibilities for such communication,

* and ensure that it is consistent with the information security policy and objectives. The organization should also retain documented information of the communication as evidence of its implementation¹² The following activities are not appropriate for the assessment of external providers according to ISO

27001:2022:

* C. I will ensure that the organization has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organization to have a reserve external provider for each critical process. The organization may choose to have a contingency plan or

a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider¹²

* D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable¹²

* G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation¹²

* H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation¹²

References:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1

2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

NEW QUESTION # 173

Which of the following is a possible event that can have a disruptive effect on the reliability of information?

- A. Threat
- B. Dependency
- C. Risk
- D. Vulnerability

Answer: A

Explanation:

A possible event that can have a disruptive effect on the reliability of information is a threat. A threat is anything that has the potential to harm an asset or its protection, such as a natural disaster, a human error, a malicious attack, etc. A threat can exploit a vulnerability or weakness in an asset or its protection and cause an adverse impact on the confidentiality, integrity or availability of information. ISO/IEC 27001:2022 defines threat as "potential cause of an unwanted incident, which can result in harm to a system or organization" (see clause 3.48). Reference: [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 Threat?

NEW QUESTION # 174

An employee caught with offense of abusing the internet, such as P2P file sharing or video/audio streaming, will not receive a warning for committing such act but will directly receive an IR.

- A. True
- B. False

Answer: A

Explanation:

An employee caught with offense of abusing the internet, such as P2P file sharing or video/audio streaming, will not receive a warning for committing such act but will directly receive an IR, because this is a violation of the organization's information security policy and acceptable use policy. An IR (incident report) is a formal document that records the details of an information security incident and the actions taken to resolve it. An IR may also trigger disciplinary actions against the employee, depending on the severity and impact of the incident. Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], [ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements], Example of an information security policy, Example of an acceptable use policy

NEW QUESTION # 175

Which measure is a preventive measure?

- A. Installing a logging system that enables changes in a system to be recognized
- **B. Putting sensitive information in a safe**
- C. Shutting down all internet traffic after a hacker has gained access to the company systems

Answer: B

NEW QUESTION # 176

.....

PECB certifications have strong authority in this field and are recognized by all companies in most of companies in the whole world. ISO-IEC-27001-Lead-Auditor new test camp questions are the best choice for candidates who are determined to clear exam urgently. If you purchase our ISO-IEC-27001-Lead-Auditor New Test Camp questions to pass this exam, you will make a major step forward for relative certification. Also you can use our products pass the other exams.

ISO-IEC-27001-Lead-Auditor Exam Syllabus: <https://www.vceprep.com/ISO-IEC-27001-Lead-Auditor-latest-vce-prep.html>

- Free ISO-IEC-27001-Lead-Auditor Vce Dumps Test ISO-IEC-27001-Lead-Auditor Valid ISO-IEC-27001-Lead-Auditor Sample Questions Answers Search for ISO-IEC-27001-Lead-Auditor and download exam materials for free through [www.examcollectionpass.com] Test ISO-IEC-27001-Lead-Auditor Valid
- Test ISO-IEC-27001-Lead-Auditor Valid ISO-IEC-27001-Lead-Auditor Exam Material ISO-IEC-27001-Lead-Auditor Valid Test Vce Copy URL  www.pdfvce.com  open and search for ISO-IEC-27001-Lead-Auditor to download for free ISO-IEC-27001-Lead-Auditor Dumps Guide
- ISO-IEC-27001-Lead-Auditor Sample Questions Answers High ISO-IEC-27001-Lead-Auditor Passing Score Test ISO-IEC-27001-Lead-Auditor Valid Search for "ISO-IEC-27001-Lead-Auditor" and download exam materials for free through www.exam4pdf.com Free ISO-IEC-27001-Lead-Auditor Vce Dumps
- PECB - Useful ISO-IEC-27001-Lead-Auditor - Latest PECB Certified ISO/IEC 27001 Lead Auditor exam Test Objectives Open www.pdfvce.com and search for ISO-IEC-27001-Lead-Auditor to download exam materials for free ISO-IEC-27001-Lead-Auditor Valid Dumps Questions
- Free ISO-IEC-27001-Lead-Auditor Vce Dumps ISO-IEC-27001-Lead-Auditor Exam Material Real ISO-IEC-27001-Lead-Auditor Exam Search for ISO-IEC-27001-Lead-Auditor and download exam materials for free through www.pass4leader.com Test ISO-IEC-27001-Lead-Auditor Valid
- ISO-IEC-27001-Lead-Auditor Online Training Materials Test ISO-IEC-27001-Lead-Auditor Valid ISO-IEC-27001-Lead-Auditor Latest Cram Materials Open  www.pdfvce.com and search for ISO-IEC-27001-Lead-Auditor to download exam materials for free ISO-IEC-27001-Lead-Auditor Current Exam Content
- ISO-IEC-27001-Lead-Auditor Download Pdf ISO-IEC-27001-Lead-Auditor Dumps Vce ISO-IEC-27001-Lead-Auditor Hottest Certification Easily obtain free download of  ISO-IEC-27001-Lead-Auditor by searching on  www.vceengine.com ISO-IEC-27001-Lead-Auditor Reliable Test Testking
- ISO-IEC-27001-Lead-Auditor Download Pdf Valid Dumps ISO-IEC-27001-Lead-Auditor Pdf Valid Dumps ISO-IEC-27001-Lead-Auditor Pdf Search for  ISO-IEC-27001-Lead-Auditor and obtain a free download on  www.pdfvce.com ISO-IEC-27001-Lead-Auditor Sample Questions Answers
- Pass Guaranteed 2025 Marvelous PECB Latest ISO-IEC-27001-Lead-Auditor Test Objectives Search on  www.getvalidtest.com  for ISO-IEC-27001-Lead-Auditor to obtain exam materials for free download Free ISO-IEC-27001-Lead-Auditor Vce Dumps
- Quiz 2025 PECB Marvelous ISO-IEC-27001-Lead-Auditor: Latest PECB Certified ISO/IEC 27001 Lead Auditor exam Test Objectives Simply search for  ISO-IEC-27001-Lead-Auditor for free download on  www.pdfvce.com ISO-IEC-27001-Lead-Auditor Sample Questions Answers
- Pass Guaranteed 2025 Marvelous PECB Latest ISO-IEC-27001-Lead-Auditor Test Objectives Search for ISO-IEC-27001-Lead-Auditor on  www.passcollection.com immediately to obtain a free download Valid ISO-IEC-27001-Lead-Auditor Exam Syllabus
- adamree449.blogspot.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, soocareer.com, leantheprocess.com, study.stcs.edu.np, motionentrance.edu.np, Disposable vapes

<https://drive.google.com/open?id=1W5OUGovEdDGkYfl4JneE4DLFw-jc5gI6>