ISO-IEC-27001-Lead-Auditor Exam Questions And Answers, ISO-IEC-27001-Lead-Auditor Valid Braindumps Sheet

2026 Latest Actual4test ISO-IEC-27001-Lead-Auditor PDF Dumps and ISO-IEC-27001-Lead-Auditor Exam Engine Free Share: https://drive.google.com/open?id=1LzLv3O_BVJnH24kggGKZ2WYKEXP966OS

Actual4test is a website to improve the pass rate of PECB certification ISO-IEC-27001-Lead-Auditor exam. Senior IT experts in the Actual4test constantly developed a variety of successful programs of passing PECB certification ISO-IEC-27001-Lead-Auditor exam, so the results of their research can 100% guarantee you PECB certification ISO-IEC-27001-Lead-Auditor exam for one time. Actual4test's training tools are very effective and many people who have passed a number of IT certification exams used the practice questions and answers provided by Actual4test. Some of them who have passed the PECB Certification ISO-IEC-27001-Lead-Auditor Exam also use Actual4test's products. Selecting Actual4test means choosing a success

PECB ISO-IEC-27001-Lead-Auditor (PECB Certified ISO/IEC 27001 Lead Auditor) certification exam is designed to test an individual's knowledge, skills, and competence to effectively plan and perform an audit of an information security management system (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is recognized globally and is highly valued by organizations that prioritize information security.

PECB ISO-IEC-27001-Lead-Auditor (PECB Certified ISO/IEC 27001 Lead Auditor) Certification Exam is a professional certification program designed for individuals who want to demonstrate their expertise in auditing information security management systems (ISMS) based on the ISO/IEC 27001 standard. PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam is offered by the Professional Evaluation and Certification Board (PECB), a global provider of training, examination, and certification services for professionals in the field of information security, quality management, and other related areas.

>> ISO-IEC-27001-Lead-Auditor Exam Questions And Answers <<

Free PDF PECB - High Hit-Rate ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam Exam Questions And Answers

It is quite clear that let the facts speak for themselves is more convincing than any word, therefore, we have prepared free demo in

this website for our customers to have a taste of the ISO-IEC-27001-Lead-Auditor test torrent compiled by our company. You will understand the reason why we are so confident to say that the ISO-IEC-27001-Lead-Auditor Exam Torrent compiled by our company is the top-notch ISO-IEC-27001-Lead-Auditor exam torrent for you to prepare for the exam. You can choose to download our free demo at any time as you like, you are always welcome to have a try, and we trust that our ISO-IEC-27001-Lead-Auditor exam materials will never let you down.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q143-Q148):

NEW QUESTION # 143
You are an experienced audit team leader guiding an auditor in training.
Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the PEOPLE controls listed in the Statement of Applicability (SoA) and mplemented at the site.
Select four controls from the following that would you expect the auditor in training to review.

- A. Information security awareness, education and training
- B. How protection against malware is implemented
- C. The organisation's business continuity arrangements
- D. The conducting of verification checks on personnel
- E. The operation of the site CCTV and door control systems
- F. Confidentiality and nondisclosure agreements
- G. Remote working arrangements
- H. The organisation's arrangements for information deletion

Answer: A,D,F,G

Explanation:
The PEOPLE controls are related to the human aspects of information security, such as roles and responsibilities, awareness and training, screening and contracts, and remote working. The auditor in training should review the following controls:
Confidentiality and nondisclosure agreements (A): These are contractual obligations that bind the employees and contractors of the organisation to protect the confidentiality of the information they handle, especially the data of external clients. The auditor should check if these agreements are signed, updated, and enforced by the organisation. This control is related to clause A.7.2.1 of ISO/IEC
27001:2022.
Information security awareness, education and training: These are activities that aim to enhance the knowledge, skills, and behaviour of the employees and contractors regarding information security. The auditor should check if these activities are planned, implemented, evaluated, and improved by the organisation. This control is related to clause A.7.2.2 of ISO/IEC 27001:2022.
Remote working arrangements (D): These are policies and procedures that govern the information security aspects of working from locations other than the organisation's premises, such as home or public places. The auditor should check if these arrangements are defined, approved, and monitored by the organisation. This control is related to clause A.6.2.1 of ISO/IEC 27001:2022.
The conducting of verification checks on personnel (E): These are background checks that verify the identity, qualifications, and suitability of the employees and contractors who have access to sensitive information or systems. The auditor should check if these checks are conducted, documented, and reviewed by the organisation. This control is related to clause A.7.1.1 of ISO/IEC 27001:2022.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements
PECB Candidate Handbook ISO/IEC 27001 Lead Auditor, 1 ISO 27001:2022 Lead Auditor - IECB, 2 ISO 27001:2022 certified ISMS lead auditor - Jisc, 3 ISO/IEC 27001:2022 Lead Auditor Transition Training Course, 4 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy, 5

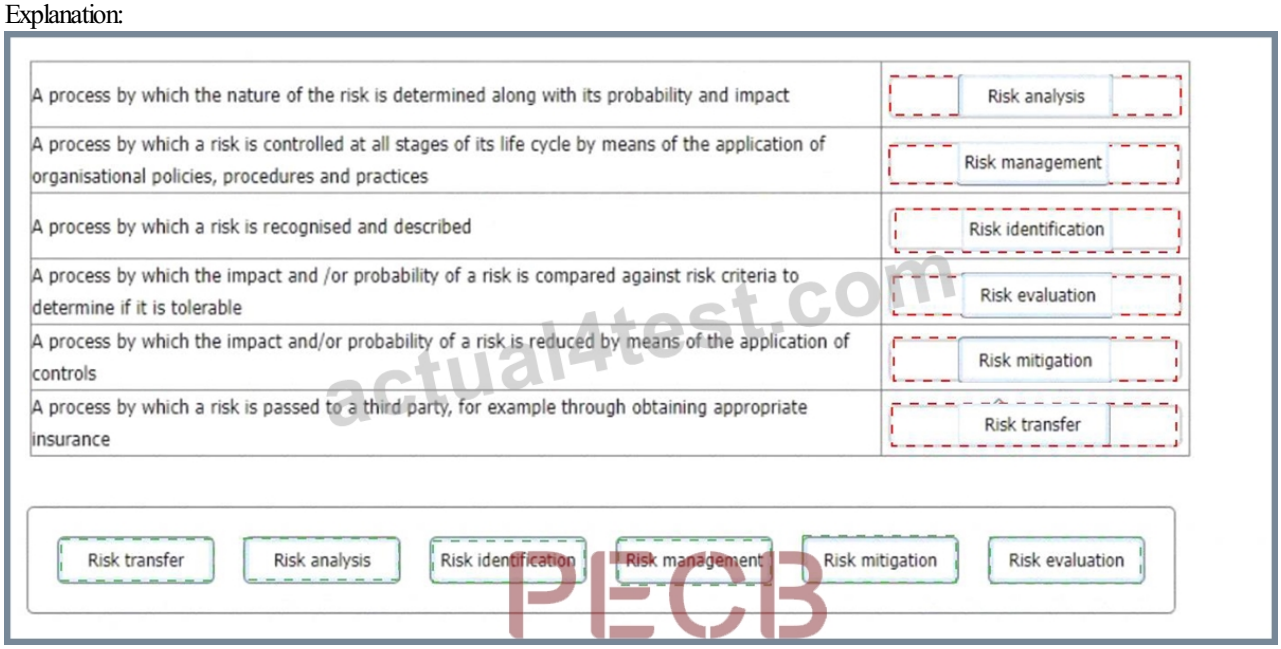
NEW QUESTION # 144
You are an experienced ISMS audit team leader providing instruction to an auditor in training. They are unclear in their understanding of risk processes and ask you to provide them with an example of each of the processes detailed below.
Match each of the descriptions provided to one of the following risk management processes.
To complete the table 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 each option to the appropriate blank section.

A process by which the nature of the risk is determined along with its probability and impact	
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	
A process by which a risk is recognised and described	
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	

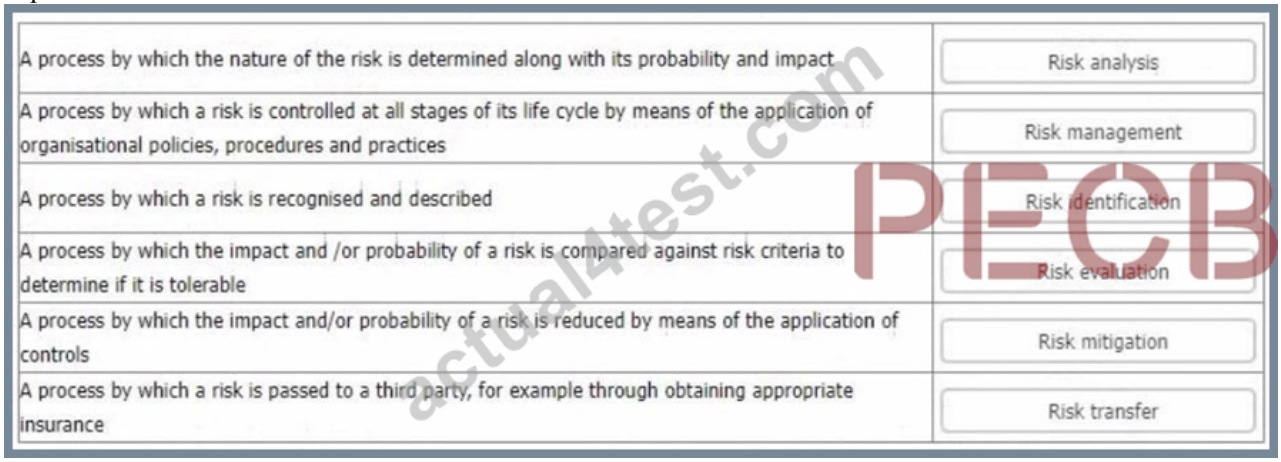
Risk transfer | Risk analysis | Risk identification | Risk management | Risk mitigation | Risk evaluation

Answer:

Explanation:



Explanation:



Risk analysis is the process by which the nature of the risk is determined along with its probability and impact. Risk analysis involves estimating the likelihood and consequences of potential events or situations that could affect the organization's information security objectives or requirements12. Risk analysis could use qualitative or quantitative methods, or a combination of both12.
Risk management is the process by which a risk is controlled at all stages of its life cycle by means of the application of

organisational policies, procedures and practices. Risk management involves establishing the context, identifying, analyzing, evaluating, treating, monitoring, and reviewing the risks that could affect the organization's information security performance or compliance12. Risk management aims to ensure that risks are identified and treated in a timely and effective manner, and that opportunities for improvement are exploited12.
Risk identification is the process by which a risk is recognised and described. Risk identification involves identifying and documenting the sources, causes, events, scenarios, and potential impacts of risks that could affect the organization's information security objectives or requirements12. Risk identification could use various techniques, such as brainstorming, interviews, checklists, surveys, or historical data12.
Risk evaluation is the process by which the impact and/or probability of a risk is compared against risk criteria to determine if it is tolerable. Risk evaluation involves comparing the results of risk analysis with predefined criteria that reflect the organization's risk appetite, tolerance, or acceptance12. Risk evaluation could use various methods, such as ranking, scoring, or matrix12. Risk evaluation helps to prioritize and decide on the appropriate risk treatment options12.
Risk mitigation is the process by which the impact and/or probability of a risk is reduced by means of the application of controls. Risk mitigation involves selecting and implementing measures that are designed to prevent, reduce, transfer, or accept risks that could affect the organization's information security objectives or requirements12. Risk mitigation could include various types of controls, such as technical, organizational, legal, or physical12. Risk mitigation should be based on a cost-benefit analysis and a residual risk assessment12.
Risk transfer is the process by which a risk is passed to a third party, for example through obtaining appropriate insurance. Risk transfer involves sharing or shifting some or all of the responsibility or liability for a risk to another party that has more capacity or capability to manage it12. Risk transfer could include various methods, such as contracts, agreements, partnerships, outsourcing, or insurance12. Risk transfer should not be used as a substitute for effective risk management within the organization12.
References :=
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management

NEW QUESTION # 145
You are an experienced audit team leader guiding an auditor in training, Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.
Select four controls from the following that would you expect the auditor in training to review.

- A. Remote working arrangements
- B. How the organisation evaluates its exposure to technical vulnerabilities
- C. Confidentiality and nondisclosure agreements
- D. Access to and from the loading bay
- E. How access to source code and development tools are managed
- F. Information security awareness, education and training
- G. The development and maintenance of an information asset inventory
- H. The organisation's business continuity arrangements
- I. The conducting of verification checks on personnel
- J. How protection against malware is implemented
- K. How information security has been addressed within supplier agreements
- L. How power and data cables enter the building
- M. The operation of the site CCTV and door control systems
- N. The organisation's arrangements for information deletion
- O. The organisation's arrangements for maintaining equipment
- P. Rules for transferring information within the organisation and to other organisations

Answer: B,E,J,M

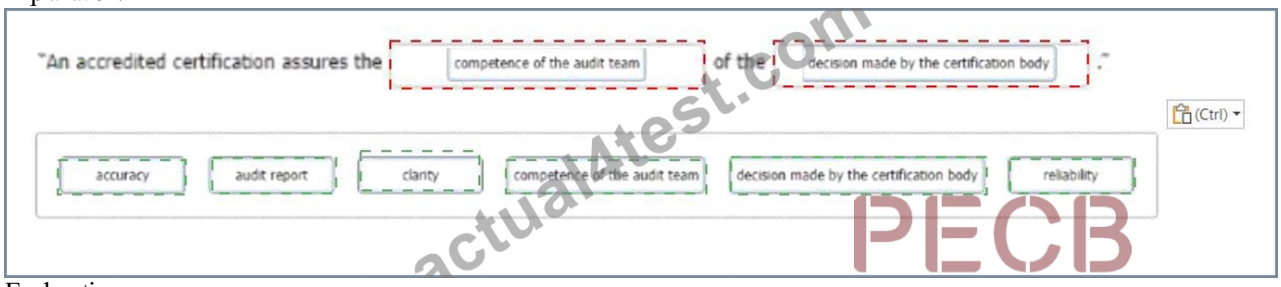
Explanation:
According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), an organization should select and implement appropriate controls to achieve its information security objectives1. The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS1. The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls2. Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:
* How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious

software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems2. This control is related to control A.12.2.1 of ISO/IEC 27002:20132.
* How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures2. This control is related to control A.12.6.1 of ISO/IEC 27002:20132.
* How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or systems that are developed or maintained by the organization or its external providers2. This control is related to control A:14.2.5 of ISO/IEC 27002:20132.
* The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed2. This control is related to control A.11.1.4 of ISO/IEC 27002:20132.
The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance of an information asset inventory (related to control A.
8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

NEW QUESTION # 146
Select the words that best complete the sentence:
To complete the sentence with the word(s) click on the blank section you want to complete so that it is highlighted in red, and then click on the application text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Answer:

Explanation:



Explanation
competence of the audit team and decision made by the certification body According to ISO/IEC 17021-1, which specifies the requirements for bodies providing audit and certification of management systems, an accredited certification means that the certification body has been evaluated by an accreditation body against recognized standards to demonstrate its competence, impartiality and performance capability1. Therefore, an accredited certification assures the competence of the audit team that conducts the audit in accordance with ISO 19011 and ISO/IEC 27001:2022, and the decision made by the certification body that grants or maintains the certification based on the audit evidence and findings2. References: ISO/IEC
17021-1:2015 - Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION # 147
Scenario 8: Tessa. Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.
Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organization's security controls and its risk tolerance in accurately characterizing the risk level within an organization On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.
After performing the required auditing activities, Tessa initiated an audit team meeting They analyzed one of Michael s findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organization's daily operations, which he believed was caused by one of the organization's IT technicians As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit.
During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.
Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.
Based on the scenario above, answer the following question:
Question:
What must Tessa do regarding the presentation of nonconformities during the closing meeting?

- A. Consistently align discussions with the relevant standard clauses
- B. Only present major nonconformities
- C. Provide detailed analysis of each nonconformity, including potential impacts on the organization

Answer: C

Explanation:
Comprehensive and Detailed In-Depth Explanation:
* A. Correct Answer:
* ISO 19011:2018 mandates that auditors present all nonconformities with sufficient detail and context to ensure proper understanding and corrective action planning.
* Failure to explain nonconformities fully could lead to ineffective remediation.
* B. Incorrect:
* Minor nonconformities must also be presented to ensure full transparency.
* C. Incorrect:
* Aligning with standard clauses is necessary, but detailed analysis is more critical.
Relevant Standard Reference:
* ISO 19011:2018 Clause 6.6.2 (Presentation of Audit Findings in Closing Meetings)

NEW QUESTION # 148
.....

□ and obtain a free download □Pass Leader ISO-IEC-27001-Lead-Auditor Dumps

- Pdf ISO-IEC-27001-Lead-Auditor Format □ Valid ISO-IEC-27001-Lead-Auditor Test Online □ Pdf ISO-IEC-27001-Lead-Auditor Format □ Go to website ➤ www.pdfvce.com □ open and search for " ISO-IEC-27001-Lead-Auditor " to download for free □Clearer ISO-IEC-27001-Lead-Auditor Explanation
- Valid ISO-IEC-27001-Lead-Auditor Test Online □ Test ISO-IEC-27001-Lead-Auditor Dumps Demo □ ISO-IEC-27001-Lead-Auditor Valid Exam Tutorial □ Open ➥ www.practicevce.com □ enter ⇛ ISO-IEC-27001-Lead-Auditor ⇚ and obtain a free download □Advanced ISO-IEC-27001-Lead-Auditor Testing Engine
- 100% Pass-Rate ISO-IEC-27001-Lead-Auditor Exam Questions And Answers Provide Prefect Assistance in ISO-IEC-27001-Lead-Auditor Preparation □ Open website ➽ www.pdfvce.com □ and search for ▸ ISO-IEC-27001-Lead-Auditor ◂ for free download □Pass Leader ISO-IEC-27001-Lead-Auditor Dumps
- Practice ISO-IEC-27001-Lead-Auditor Test Engine □ Latest ISO-IEC-27001-Lead-Auditor Exam Camp □ ISO-IEC-27001-Lead-Auditor Dumps Torrent □ Easily obtain [ISO-IEC-27001-Lead-Auditor] for free download through ➥ www.prepawaypdf.com □ □Valid ISO-IEC-27001-Lead-Auditor Test Online
- Updated PECB ISO-IEC-27001-Lead-Auditor Exam Questions – Key to Your Career Growth □ Easily obtain （ ISO-IEC-27001-Lead-Auditor ） for free download through ▸ www.pdfvce.com ◂ □Test ISO-IEC-27001-Lead-Auditor Dumps Demo
- PECB ISO-IEC-27001-Lead-Auditor Exam Questions And Answers - www.examcollectionpass.com - Leading Provider in Certification Exams Materials □ Open ➠ www.examcollectionpass.com □ and search for [ISO-IEC-27001-Lead-Auditor] to download exam materials for free □Test ISO-IEC-27001-Lead-Auditor Dumps Demo
- Study Anywhere Anytime With PECB ISO-IEC-27001-Lead-Auditor PDF Questions □ ➡ www.pdfvce.com □□□ is best website to obtain ▸ ISO-IEC-27001-Lead-Auditor ◂ for free download □Test ISO-IEC-27001-Lead-Auditor Dumps Demo
- PECB ISO-IEC-27001-Lead-Auditor Exam Questions And Answers - www.easy4engine.com - Leading Provider in Certification Exams Materials □ Easily obtain ⇛ ISO-IEC-27001-Lead-Auditor ⇚ for free download through ➽ www.easy4engine.com □ □Advanced ISO-IEC-27001-Lead-Auditor Testing Engine
- Pass Guaranteed High-quality PECB - ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam Exam Questions And Answers □ Enter ☀ www.pdfvce.com □☀□ and search for ✔ ISO-IEC-27001-Lead-Auditor □✔□ to download for free □Test ISO-IEC-27001-Lead-Auditor Dumps Demo
- Pass Leader ISO-IEC-27001-Lead-Auditor Dumps □ Study ISO-IEC-27001-Lead-Auditor Plan □ Reliable ISO-IEC-27001-Lead-Auditor Dumps Ppt □ Copy URL 【 www.troytecdumps.com 】 open and search for { ISO-IEC-27001-Lead-Auditor } to download for free □Pdf ISO-IEC-27001-Lead-Auditor Format
- martinabemf951387.corpfinwiki.com, socialrator.com, pennyqavh765534.iyublog.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, sociallweb.com, mathegclt488749.life3dblog.com, bookmarkmargin.com, keirangjxw466553.daneblogger.com, hassanozpu331904.blazingblog.com, murraymcsw989431.theblogfairy.com, Disposable vapes

P.S. Free 2026 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by Actual4test: https://drive.google.com/open?id=1LzLv3O_BVJnH24kggGKZ2WYKEXP966OS