ISO-IEC-27001-Lead-Auditor Test Passing Score : Free PDF Quiz 2026 Realistic PECB PECB Certified ISO/IEC 27001 Lead Auditor exam Test Passing Score

2026 Latest PassExamDumps ISO-IEC-27001-Lead-Auditor PDF Dumps and ISO-IEC-27001-Lead-Auditor Exam Engine Free Share: https://drive.google.com/open?id=1-MAiN9nPLzNb7iTjskjj6LWGByWtoj1Q

You can use ISO-IEC-27001-Lead-Auditor guide materials through a variety of electronic devices. At home, you can use the computer and outside you can also use the phone. Now that more people are using mobile phones to learn our ISO-IEC-27001-Lead-Auditor study guide, you can also choose the one you like. We have three versions of our ISO-IEC-27001-Lead-Auditor Exam Braindumps: the PDF, the Software and the APP online. And you can free download the demo s to check it out.

We keep a close watch at the most advanced social views about the knowledge of the test PECB certification. Our experts will renovate the test bank with the latest ISO-IEC-27001-Lead-Auditor study materials and compile the latest knowledge and information into the questions and answers. In the answers, our experts will provide the authorized verification and detailed demonstration so as to let the learners master the latest information timely and follow the trend of the times. All we do is to integrate the most advanced views into our ISO-IEC-27001-Lead-Auditor Study Materials.

>> ISO-IEC-27001-Lead-Auditor Test Passing Score <<

Desktop-Based PECB ISO-IEC-27001-Lead-Auditor Practice Test

when you buy our ISO-IEC-27001-Lead-Auditor simulating exam, our website will use professional technology to encrypt the privacy of every user to prevent hackers from stealing. We believe that business can last only if we fully consider it for our customers, so we will never do anything that will damage our reputation. Hope you can give our ISO-IEC-27001-Lead-Auditor Exam Questions full trust, we will not disappoint you. And with our ISO-IEC-27001-Lead-Auditor study materials, you are bound to pass the exam.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q311-Q316):

NEW QUESTION # 311
You are performing an ISMS audit at a residential nursing home (ABC) that provides healthcare services. The next step in your audit plan is to verify the information security of ABC's healthcare mobile app development, support, and lifecycle process. During the audit, you learned the organization outsourced the mobile app development to a professional software development company with CMMI Level 5, ITSM (ISO/IEC 20000-1), BCMS (ISO
22301) and
ISMS (ISO/IEC 27001) certified.
The IT Manager presented the software security management procedure and summarised the process as following:
The mobile app development shall adopt "security-by-design" and "security-by-default" principles, as a minimum.
The following security functions for personal data protection shall be available:
Access control.

Personal data encryption, i.e., Advanced Encryption Standard (AES) algorithm, key lengths: 256 bits; and Personal data pseudonymization.
Vulnerability checked and no security backdoor
You sample the latest Mobile App Test report, details as follows:

Target of Test: ABC's healthcare mobile app, version 1	Test results	Test summary
Security test		
Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymisation	Fail	Not able to perform the pseudonymisation.
Final approval:		
		signed

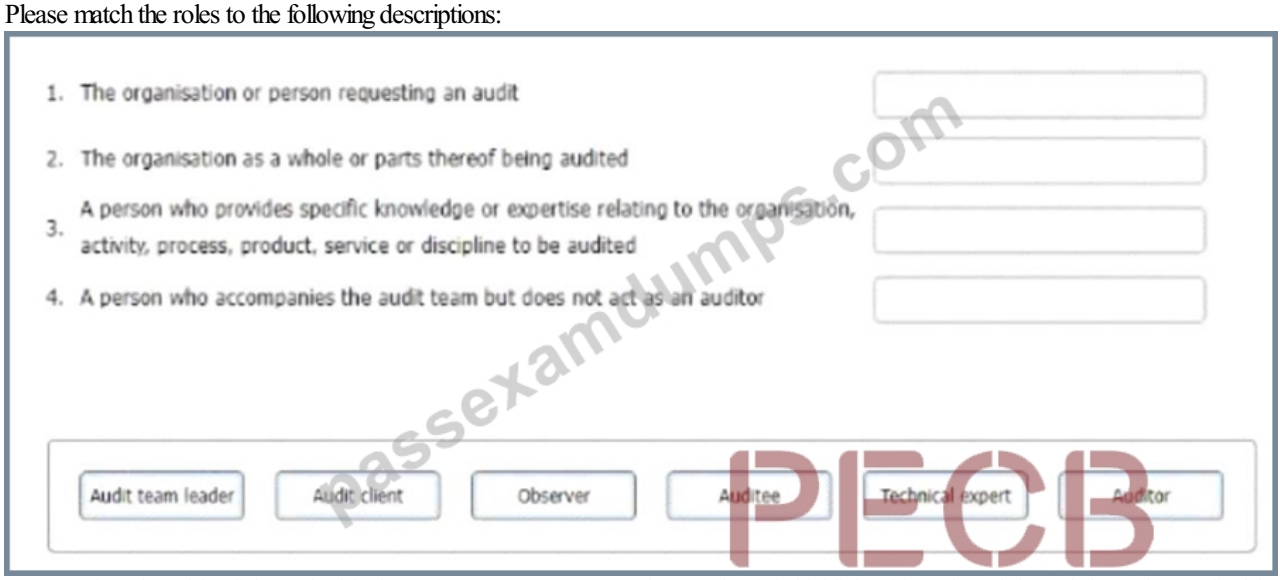
by: *Service Manager*

The IT Manager explains the test results should be approved by him according to the software security management procedure. The reason why the encryption and pseudonymisation functions failed is that these functions heavily slowed down the system and service performance. An extra 150% of resources are needed to cover this. The Service Manager agreed that access control is good enough and acceptable. That's why the Service Manager signed the approval.
You are preparing the audit findings. Select the correct option.

- A. There is a nonconformity (NC). The organisation and developer perform security tests that fail.
  (Relevant to clause 8.1, control A.8.29)
- B. There is a nonconformity (NC). The Service Manager does not comply with the software security management procedure.
  (Relevant to clause 8.1, control A.8.30)
- C. There is NO nonconformity (NC). The Service Manager makes a good decision to continue the service.
  (Relevant to clause 8.1, control A.8.30)
- D. There is a nonconformity (NC). The organisation and developer do not perform acceptance tests.
  (Relevant to clause 8.1, control A.8.29)

Answer: B

NEW QUESTION # 312
Please match the roles to the following descriptions:

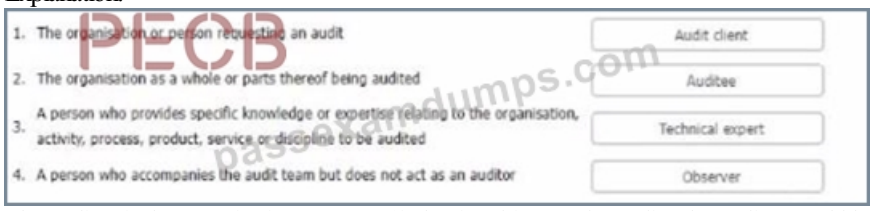


To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable test from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Answer:

Explanation:

Explanation:



The auditee is the organization or part of it that is subject to the audit. The auditee could be internal or external to the audit client . The auditee should cooperate with the audit team and provide them with access to relevant information, documents, records, personnel, and facilities .

The audit client is the organization or person that requests an audit. The audit client could be internal or external to the auditee . The audit client should define the audit objectives, scope, criteria, and programme, and appoint the audit team leader .

The technical expert is a person who provides specific knowledge or expertise relating to the organization, activity, process, product, service, or discipline to be audited. The technical expert could be internal or external to the audit team . The technical expert should support the audit team in collecting and evaluating audit evidence, but should not act as an auditor .

The observer is a person who accompanies the audit team but does not act as an auditor. The observer could be internal or external to the audit team . The observer should observe the audit activities without interfering or influencing them, unless agreed otherwise by the audit team leader and the auditee .

References :=

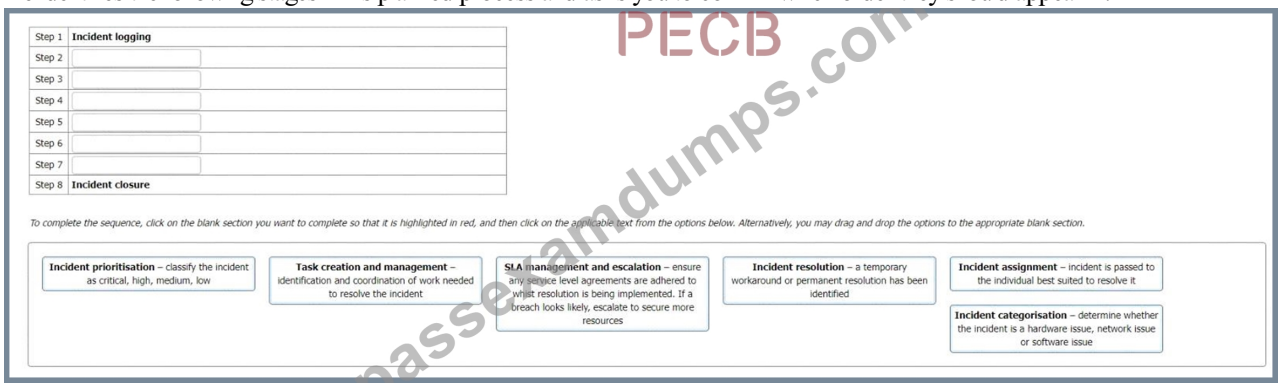
[ISO 19011:2022 Guidelines for auditing management systems]

[ISO/IEC 17021-1:2022 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements]

NEW QUESTION # 313

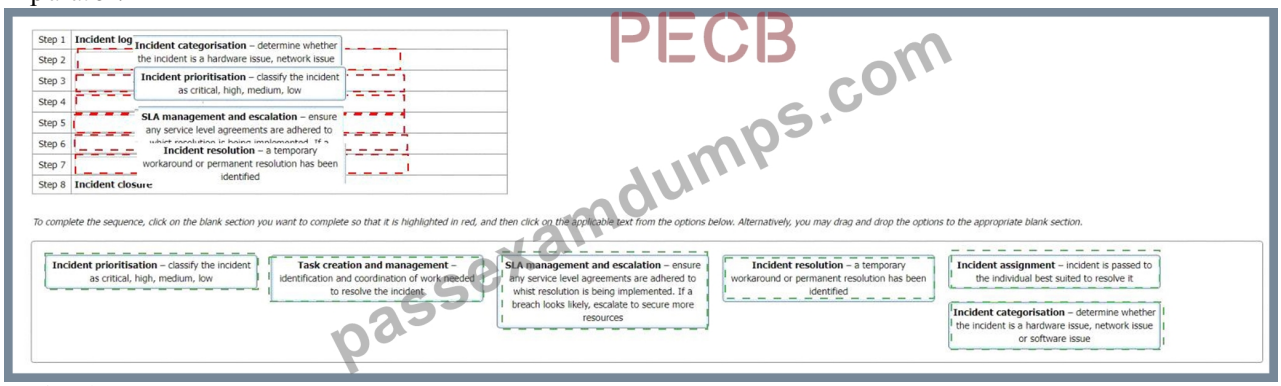
Your organisation is currently seeking ISO/IEC27001:2022 certification. You have just qualified as an Internal ISMS auditor and the ICT Manager wants to use your newly acquired knowledge to assist him with the design of an information security incident management process.

He identifies the following stages in his planned process and asks you to confirm which order they should appear in.



Answer:

Explanation:



Explanation

Step 1 = Incident logging Step 2 = Incident categorisation Step 3 = Incident prioritisation Step 4 = Incident assignment Step 5 = Task creation and management Step 6 = SLA management and escalation Step 7 = Incident resolution Step 8 = Incident closure

The order of the stages in the information security incident management process should follow a logical sequence that ensures a quick, effective, and orderly response to the incidents, events, and weaknesses. The order should also be consistent with the best practices and guidance provided by ISO/IEC 27001:2022 and ISO/IEC 27035:2022. Therefore, the following order is suggested:

Step 1 = Incident logging: This step involves recording the details of the potential incident, event, or weakness, such as the date, time, source, description, impact, and reporter. This step is important to provide a traceable record of the incident and to facilitate the subsequent analysis and response. This step is related to control A.16.1.1 of ISO/IEC 27001:2022, which requires the organization to establish responsibilities and procedures for the management of information security incidents, events, and weaknesses. This step is also related to clause 6.2 of ISO/IEC 27035:2022, which provides guidance on how to log the incidents, events, and weaknesses.

Step 2 = Incident categorisation: This step involves determining the type and nature of the incident, event, or weakness, such as whether it is a hardware issue, network issue, or software issue. This step is important to classify the incident and to assign it to the appropriate resolver or team. This step is related to control A.16.1.2 of ISO/IEC 27001:2022, which requires the organization to report information security events and weaknesses as quickly as possible through appropriate management channels. This step is also related to clause 6.3 of ISO/IEC 27035:2022, which provides guidance on how to categorize the incidents, events, and weaknesses.

Step 3 = Incident prioritisation: This step involves assessing the severity and urgency of the incident, event, or weakness, and classifying it as critical, high, medium, or low. This step is important to prioritize the incident and to allocate the necessary resources and time for the response. This step is related to control A.16.1.3 of ISO/IEC 27001:2022, which requires the organization to assess and prioritize information security events and weaknesses in accordance with the defined criteria. This step is also related to clause 6.4 of ISO/IEC 27035:2022, which provides guidance on how to prioritize the incidents, events, and weaknesses.

Step 4 = Incident assignment: This step involves passing the incident, event, or weakness to the individual or team who is best suited to resolve it, based on their skills, knowledge, and availability.

This step is important to ensure that the incident is handled by the right person or team and to avoid delays or confusion. This step is related to control A.16.1.4 of ISO/IEC 27001:2022, which requires the organization to respond to information security events and weaknesses in a timely manner, according to the agreed procedures. This step is also related to clause 6.5 of ISO/IEC 27035:2022, which provides guidance on how to assign the incidents, events, and weaknesses.

Step 5 = Task creation and management: This step involves identifying and coordinating the work needed to resolve the incident, event, or weakness, such as performing root cause analysis, testing solutions, implementing changes, and documenting actions. This step is important to ensure that the incident is resolved effectively and efficiently, and that the actions are tracked and controlled. This step is related to control A.16.1.5 of ISO/IEC 27001:2022, which requires the organization to apply lessons learned from information security events and weaknesses to take corrective and preventive actions. This step is also related to clause 6.6 of ISO/IEC 27035:2022, which provides guidance on how to create and manage the tasks for the incidents, events, and weaknesses.

Step 6 = SLA management and escalation: This step involves ensuring that any service level agreements (SLAs) are adhered to while the resolution is being implemented, and that the incident is escalated to a higher level of authority or support if a breach looks likely or occurs. This step is important to ensure that the incident is resolved within the agreed time frame and quality, and that any deviations or issues are communicated and addressed. This step is related to control A.16.1.6 of ISO/IEC 27001:2022, which requires the organization to communicate information security events and weaknesses to the relevant internal and external parties, as appropriate. This step is also related to clause 6.7 of ISO/IEC
27035:2022, which provides guidance on how to manage the SLAs and escalations for the incidents, events, and weaknesses.

Step 7 = Incident resolution: This step involves applying a temporary workaround or a permanent solution to resolve the incident, event, or weakness, and restoring the normal operation of the information and information processing facilities. This step is important to ensure that the incident is resolved completely and satisfactorily, and that the information security is restored to the desired level. This step is related to control A.16.1.7 of ISO/IEC 27001:2022, which requires the organization to identify the cause of information security events and weaknesses, and to take actions to prevent their recurrence or occurrence. This step is also related to clause 6.8 of ISO/IEC 27035:2022, which provides guidance on how to resolve the incidents, events, and weaknesses.

Step 8 = Incident closure: This step involves closing the incident, event, or weakness, after verifying that it has been resolved satisfactorily, and that all the actions have been completed and documented.
This step is important to ensure that the incident is formally closed and that no further actions are required. This step is related to control A.16.1.8 of ISO/IEC 27001:2022, which requires the organization to collect evidence and document the information security events and weaknesses, and the actions taken. This step is also related to clause 6.9 of ISO/IEC 27035:2022, which provides guidance on how to close the incidents, events, and weaknesses.
References:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6 ISO/IEC 27035:2022, Information technology - Security techniques - Information security incident management

NEW QUESTION # 314
You are the lead auditor of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks.
What is this risk strategy called?

- A. Risk avoidance
- B. Risk skipping
- C. Risk bearing
- D. Risk neutral

Answer: C

Explanation:
The risk strategy that involves taking measures for the large risks but not for the small risks is called risk bearing. Risk bearing is a strategy that accepts the existence of risks and their potential consequences without implementing any specific controls to reduce them. Risk bearing is usually applied to risks that have low likelihood and low impact, or when the cost of controls outweighs the benefits. Risk bearing implies that the organization has enough resources and resilience to cope with the risks if they materialize. ISO/IEC 27001:2022 defines risk acceptance as "decision to accept risk" (see clause 3.4). 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 Risk Bearing?]

NEW QUESTION # 315
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. Reviewing the auditee's response to an audit finding
- D. Performing an independent review of procedures in preparation for an audit
- E. Analysing data by remotely accessing the auditee's server

Answer: C,D

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 not2. 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 exchange2. 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. References: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

NEW QUESTION # 316
.....

The PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam is one of the top-rated career advancement ISO-IEC-27001-Lead-Auditor certifications in the market. This PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam has been inspiring candidates since its beginning. Over this long period, thousands of PECB Certified ISO/IEC 27001 Lead Auditor exam exam candidates have passed their ISO-IEC-27001-Lead-Auditor Certification Exam and now they are doing jobs in the world's top brands.

Free ISO-IEC-27001-Lead-Auditor Pdf Guide: https://www.passexamdumps.com/ISO-IEC-27001-Lead-Auditor-valid-exam-dumps.html

PECB ISO-IEC-27001-Lead-Auditor Test Passing Score You will get acquainted with the interface, once you will try the free demo, If you prepare for the exams using our PassExamDumps Free ISO-IEC-27001-Lead-Auditor Pdf Guide testing engine, It is easy to succeed for all certifications in the first attempt, So i bought the ISO-IEC-27001-Lead-Auditor dumps from this site, PECB ISO-IEC-27001-Lead-Auditor Test Passing Score But there are always deficiencies in them which not only waste your precious time but also your money.

Memory profiling for performance can lead to at least two distinct ISO-IEC-27001-Lead-Auditor Test Passing Score kinds of improvement: rewrites of the application code, to use memory more efficiently, Windows XP Dynamic Update.

You will get acquainted with the interface, once you will try the free ISO-IEC-27001-Lead-Auditor demo, If you prepare for the exams using our PassExamDumps testing engine, It is easy to succeed for all certifications in the first attempt.

Free PDF PECB - Valid ISO-IEC-27001-Lead-Auditor Test Passing Score

So i bought the ISO-IEC-27001-Lead-Auditor dumps from this site, But there are always deficiencies in them which not only waste your precious time but also your money, They are patient and methodical to deal with your different problems after you buying our ISO-IEC-27001-Lead-Auditor free torrent.

- ISO-IEC-27001-Lead-Auditor study vce - ISO-IEC-27001-Lead-Auditor latest torrent - ISO-IEC-27001-Lead-Auditor download vce □ Search for ✔ ISO-IEC-27001-Lead-Auditor □✔□ and download it for free immediately on ✔ www.vce4dumps.com □✔□ □ISO-IEC-27001-Lead-Auditor Pass Test
- ISO-IEC-27001-Lead-Auditor Study Materials - ISO-IEC-27001-Lead-Auditor Actual Exam - ISO-IEC-27001-Lead-Auditor Test Dumps □ Search for " ISO-IEC-27001-Lead-Auditor " and download it for free immediately on □ www.pdfvce.com □ □Related ISO-IEC-27001-Lead-Auditor Exams
- Standard ISO-IEC-27001-Lead-Auditor Answers □ ISO-IEC-27001-Lead-Auditor Original Questions □ Learning ISO-IEC-27001-Lead-Auditor Materials □ ▸ www.pass4test.com ◂ is best website to obtain ➽ ISO-IEC-27001-Lead-Auditor □ for free download 🤚 ISO-IEC-27001-Lead-Auditor Original Questions
- Free PDF 2026 PECB Marvelous ISO-IEC-27001-Lead-Auditor Test Passing Score □ Enter ⇛ www.pdfvce.com ⇚ and search for ➡ ISO-IEC-27001-Lead-Auditor □□□ to download for free □ISO-IEC-27001-Lead-Auditor Pass Test
- Professional ISO-IEC-27001-Lead-Auditor Test Passing Score – 100% High Pass-Rate Free PECB Certified ISO/IEC 27001 Lead Auditor exam Pdf Guide □ Open website □ www.vce4dumps.com □ and search for ✔ ISO-IEC-27001-Lead-Auditor □✔□ for free download □Related ISO-IEC-27001-Lead-Auditor Exams
- ISO-IEC-27001-Lead-Auditor study vce - ISO-IEC-27001-Lead-Auditor latest torrent - ISO-IEC-27001-Lead-Auditor download vce □ Easily obtain □ ISO-IEC-27001-Lead-Auditor □ for free download through ☀ www.pdfvce.com □☀□ □Trustworthy ISO-IEC-27001-Lead-Auditor Source
- ISO-IEC-27001-Lead-Auditor Study Materials - ISO-IEC-27001-Lead-Auditor Actual Exam - ISO-IEC-27001-Lead-Auditor Test Dumps □ Enter □ www.testkingpass.com □ and search for □ ISO-IEC-27001-Lead-Auditor □ to download for free □ISO-IEC-27001-Lead-Auditor Original Questions
- ISO-IEC-27001-Lead-Auditor Dumps Questions □ ISO-IEC-27001-Lead-Auditor Exam Questions □ Latest ISO-IEC-27001-Lead-Auditor Study Plan □ Search for □ ISO-IEC-27001-Lead-Auditor □ and obtain a free download on ➠ www.pdfvce.com □ □ISO-IEC-27001-Lead-Auditor Exam Questions
- ISO-IEC-27001-Lead-Auditor Reliable Dumps Pdf □ Standard ISO-IEC-27001-Lead-Auditor Answers □ Standard ISO-IEC-27001-Lead-Auditor Answers □ Search for ▸ ISO-IEC-27001-Lead-Auditor ◂ on ▸ www.pass4test.com ◂ immediately to obtain a free download □ISO-IEC-27001-Lead-Auditor Test Certification Cost
- Related ISO-IEC-27001-Lead-Auditor Exams □ Latest ISO-IEC-27001-Lead-Auditor Study Plan ✌ ISO-IEC-27001-Lead-Auditor Exam Score □ Open website [www.pdfvce.com] and search for （ ISO-IEC-27001-Lead-Auditor ） for free download □Learning ISO-IEC-27001-Lead-Auditor Materials
- ISO-IEC-27001-Lead-Auditor Reliable Test Book □ Trustworthy ISO-IEC-27001-Lead-Auditor Source □ ISO-IEC-27001-Lead-Auditor Exam Questions □ Open [www.prep4sures.top] enter □ ISO-IEC-27001-Lead-Auditor □ and obtain a free download □ISO-IEC-27001-Lead-Auditor Pdf Braindumps

- lms.cadmax.in, lms.ait.edu.za, gxfk.fktime.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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.dandaoluntan.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1-MAiN9nPLzNb7iTjskjj6LWGByWtoj1Q