

HOT ISO-IEC-27001-Lead-Auditor Reliable Exam Question - High-quality PECB PECB Certified ISO/IEC 27001 Lead Auditor exam - ISO-IEC-27001-Lead-Auditor Valid Exam Syllabus



DOWNLOAD the newest PassLeaderVCE ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free:
https://drive.google.com/open?id=1b9-SKXkVBpDdkUTvd_wvXkOBcP1bjD5T

With our ISO-IEC-27001-Lead-Auditor practice test software, you can simply assess yourself by going through the ISO-IEC-27001-Lead-Auditor practice tests. We highly recommend going through the ISO-IEC-27001-Lead-Auditor answers multiple times so you can assess your preparation for the ISO-IEC-27001-Lead-Auditor exam. Make sure that you are preparing yourself for the ISO-IEC-27001-Lead-Auditor test with our practice test software as it will help you get a clear idea of the real ISO-IEC-27001-Lead-Auditor exam scenario. By passing the exams multiple times on practice test software, you will be able to pass the real ISO-IEC-27001-Lead-Auditor test in the first attempt.

Many people prefer to buy our ISO-IEC-27001-Lead-Auditor valid study guide materials because they deeply believe that if only they buy them can definitely pass the ISO-IEC-27001-Lead-Auditor test. The reason why they like our ISO-IEC-27001-Lead-Auditor guide questions is that our study materials' quality is very high and the service is wonderful. For years we always devote ourselves to perfecting our ISO-IEC-27001-Lead-Auditor Study Materials and shaping our products into the model products which other companies strive hard to emulate. We boost the leading research team and the top-ranking sale service.

>> ISO-IEC-27001-Lead-Auditor Reliable Exam Question <<

ISO-IEC-27001-Lead-Auditor Valid Exam Syllabus, ISO-IEC-27001-Lead-Auditor Latest Mock Test

To help you get the PECB exam certification, we provide you with the best valid ISO-IEC-27001-Lead-Auditor pdf prep material. The customizable and intelligence ISO-IEC-27001-Lead-Auditor test engine will bring you to a high efficiency study way. The ISO-IEC-27001-Lead-Auditor test engine contains self-assessment features like marks, progress charts, etc. Besides, the Easy-to-use ISO-IEC-27001-Lead-Auditor layout will facilitate your preparation for ISO-IEC-27001-Lead-Auditor real test. You can pass your ISO-IEC-27001-Lead-Auditor certification without too much pressure.

PECB ISO-IEC-27001-Lead-Auditor Certification is a highly regarded certification in the field of information security management. It is designed to test the knowledge and skills of individuals seeking to become certified ISO/IEC 27001 lead auditors. Individuals who hold this certification are considered experts in the field and are highly valued by organizations around the world.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q199-Q204):

NEW QUESTION # 199

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.

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

Answer: I,L,M,O

Explanation:

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 # 200

Scenario 2

Knight is an electronics company based in Northern California, the US that develops video game consoles.

With over 300 employees globally, Knight is celebrating its fifth anniversary by launching the G-Console, a next-generation gaming system aimed at international markets. G-Console is considered to be the ultimate media machine of 2021, and it will give players the best gaming experience. The console pack will include a pair of VR headsets, two games, and other gifts.

Over the years, the company has developed a strong reputation for integrity, honesty, and respect toward their customers. Besides being a very customer-oriented company, Knight also gained wide recognition within the gaming industry because of its quality.

As one of the leading video game console developers in the world, Knight often finds itself a target for malicious activities. Therefore, it has implemented an information security management system (ISMS) based on ISO/IEC 27001, and its scope was communicated to employees of the company over a weekly meeting.

Recently, however, Knight experienced a security breach when hackers leaked proprietary information. In response, the incident response team (IRT) immediately began a thorough investigation of the system and the specifics of the incident. Initially, the IRT suspected that employees may have used weak passwords, allowing hackers to easily access their accounts. Upon further investigation, it was revealed that the hackers captured traffic from the file transfer protocol (FTP), which transmits data using clear-text passwords for authentication.

In light of this security incident, and following the IRT's recommendations, Knight decided to replace the FTP with Secure Shell (SSH) protocol. This change ensures that any captured traffic is encrypted, significantly improving security.

After implementing these changes, Knight conducted a risk assessment to verify that the implementation of controls had minimized the risk of similar incidents. Based on the results of the risk assessment, they chose a risk treatment option to treat the risk.

Question

Based on Scenario 2, the risk treatment option was based on the risk assessment results. Is this acceptable?

- A. No, the risk treatment option should be based solely on financial considerations regardless of the risk assessment results.
- **B. Yes, an appropriate risk treatment option is taking into account the risk assessment results.**
- C. No, the risk treatment options should be randomly selected to ensure unbiased decision-making.

Answer: B

Explanation:

ISO/IEC 27001:2022 explicitly requires that risk treatment decisions be based on the results of the information security risk assessment. Clause 6.1.3 states that, after completing a risk assessment, the organization shall determine appropriate risk treatment options and select controls to implement those options.

This ensures that controls are proportionate, justified, and aligned with actual information security risks rather than arbitrary or purely cost-driven decisions.

In the scenario, Knight conducted a risk assessment after implementing SSH to replace FTP and then chose a risk treatment option based on the assessment results. This approach is fully compliant with ISO/IEC 27001.

The organization first identified the risk, implemented a control to address the vulnerability, and then reassessed the residual risk to confirm whether it was reduced to an acceptable level. This demonstrates a structured and systematic risk management process. Option B is incorrect because ISO/IEC 27001 does not allow financial considerations to override risk assessment outcomes. While cost is a factor, it must be balanced against the risk and potential impact. Option C is incorrect because random selection of risk treatment options contradicts the fundamental principles of risk-based decision-making and would undermine the effectiveness of the ISMS.

Therefore, selecting a risk treatment option based on risk assessment results is not only acceptable but required under ISO/IEC 27001:2022.

NEW QUESTION # 201

Integrity of data means

- A. Data should be viewable at all times
- **B. Accuracy and completeness of the data**

- C. Data should be accessed by only the right people

Answer: B

Explanation:

Integrity of data means accuracy and completeness of the data. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Data should be viewable at all times is not related to integrity, but to availability. Data should be accessed by only the right people is not related to integrity, but to confidentiality. References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4.

NEW QUESTION # 202

Select the option which best describes how Information Security Management System audits should be conducted:

- A. Audit methods should be used to assess audit evidence in order to generate audit recommendations. Then, the audit recommendations should be created and presented to the auditee at the closing meeting.
- B. Audit objectives should be used to assess audit evidence in order to generate audit conclusions. Then, the audit findings should be created and presented to the audit client at the closing meeting.
- C. Audit objectives should be used to assess objective evidence in order to generate audit conclusions. Then, the audit recommendations should be created and presented to top management at management review.
- D. Audit criteria should be used to assess objective evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team leader at the closing meeting.
- E. Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.
- F. Audit criteria should be used to assess circumstantial evidence in order to generate audit outcomes. Then, the audit report should be created and presented to the audit team at the audit team meeting.

Answer: E

Explanation:

The option that best describes how Information Security Management System (ISMS) audits should be conducted, aligning with best practices and standards like ISO/IEC 27001:2022, is:

D: Audit methods should be used to assess objective evidence in order to generate audit findings. Then, the audit conclusion should be created and presented to the auditee at the closing meeting.

NEW QUESTION # 203

You are performing an ISMS initial certification audit at a residential nursing home that provides healthcare services. The next step in your audit plan is to conduct the closing meeting. During the final audit team meeting, as an audit team leader, you agree to report 2 minor nonconformities and 1 opportunity for improvement as below:

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings		Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.		Clause 7.4 and Control A.5.24	N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
Team Leader			signed by Audit	

Select one option of the recommendation to the audit programme manager you are going to advise to the auditee at the closing meeting.

- A. Recommend certification after your approval of the proposed corrective action plan Recommend that the findings can be closed out at a surveillance audit in 1 year
- B. Recommend certification immediately
- C. Recommend that a full scope re-audit is required within 6 months
- D. Recommend that an unannounced audit is carried out at a future date
- E. Recommend that a partial audit is required within 3 months

Answer: A

Explanation:

According to ISO/IEC 17021-1:2015, which specifies the requirements for bodies providing audit and certification of management systems, clause 9.4.9 requires the certification body to make a certification decision based on the information obtained during the audit and any other relevant information¹. The certification body should also consider the effectiveness of the corrective actions taken by the auditee to address any nonconformities identified during the audit¹. Therefore, when making a recommendation to the audit programme manager, an ISMS auditor should consider the nature and severity of the nonconformities and the proposed corrective actions.

Based on the scenario above, the auditor should recommend certification after their approval of the proposed corrective action plan and recommend that the findings can be closed out at a surveillance audit in 1 year. The auditor should provide the following justification for their recommendation:

Justification: This recommendation is appropriate because it reflects the fact that the auditee has only two minor nonconformities and one opportunity for improvement, which do not indicate a significant or systemic failure of their ISMS. A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall effectiveness or conformity². An opportunity for improvement is defined as a suggestion for improvement beyond what is required by ISO/IEC 27001:2022. Therefore, these findings do not prevent or preclude certification, as long as they are addressed by appropriate corrective actions within a reasonable time frame. The auditor should approve the proposed corrective action plan before recommending certification, to ensure that it is realistic, achievable, and effective. The auditor should also recommend that the findings can be closed out at a surveillance audit in 1 year, to verify that the corrective actions have been implemented and are working as intended.

The other options are not valid recommendations for the audit programme manager, as they are either too lenient or too strict for the given scenario. For example:

Recommend certification immediately: This option is not valid because it implies that the auditor ignores or accepts the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182, which provides guidelines for auditing

management systems. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to consider the effectiveness of the corrective actions taken by the auditee before making a certification decision.

Recommend that a full scope re-audit is required within 6 months: This option is not valid because it implies that the auditor overreacts or exaggerates the nonconformities, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a re-audit is necessary based on the nature and extent of nonconformities and other relevant factors. A full scope re-audit is usually reserved for major nonconformities or multiple minor nonconformities that indicate a serious or widespread failure of an ISMS.

Recommend that an unannounced audit is carried out at a future date: This option is not valid because it implies that the auditor distrusts or doubts the auditee's commitment or capability to implement corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to conduct unannounced audits only under certain conditions, such as when there are indications of serious problems with an ISMS or when required by sector-specific schemes.

Recommend that a partial audit is required within 3 months: This option is not valid because it implies that the auditor imposes or prescribes a specific time frame or scope for verifying corrective actions, which is contrary to the audit principles and objectives of ISO 19011:20182. It also contradicts the requirement of ISO/IEC 17021-1:20151, which requires the certification body to determine whether a partial audit is necessary based on the nature and extent of nonconformities and other relevant factors. A partial audit may be appropriate for minor nonconformities, but the time frame and scope should be agreed upon with the auditee and based on the proposed corrective action plan.

NEW QUESTION # 204

.....

Our ISO-IEC-27001-Lead-Auditor study quiz are your optimum choices which contain essential know-hows for your information. If you really want to get the certificate successfully, only ISO-IEC-27001-Lead-Auditor guide materials with intrinsic contents can offer help they are preminent materials can satisfy your both needs of studying or passing with efficiency. For our ISO-IEC-27001-Lead-Auditor Exam Brandumps contain the most useful information on the subject and are always the latest according to the efforts of our professionals.

ISO-IEC-27001-Lead-Auditor Valid Exam Syllabus: <https://www.passleadervce.com/ISO-27001/reliable-ISO-IEC-27001-Lead-Auditor-exam-learning-guide.html>

- Reliable ISO-IEC-27001-Lead-Auditor Exam Labs Reliable ISO-IEC-27001-Lead-Auditor Real Test Exam ISO-IEC-27001-Lead-Auditor Learning Download ISO-IEC-27001-Lead-Auditor for free by simply entering www.pdf.dumps.com website Reliable ISO-IEC-27001-Lead-Auditor Exam Labs
- Exam ISO-IEC-27001-Lead-Auditor Learning ISO-IEC-27001-Lead-Auditor Latest Exam Labs Reliable ISO-IEC-27001-Lead-Auditor Exam Labs Easily obtain (ISO-IEC-27001-Lead-Auditor) for free download through { www.pdfvce.com } Reliable ISO-IEC-27001-Lead-Auditor Real Test
- TOP ISO-IEC-27001-Lead-Auditor Reliable Exam Question - PECB PECB Certified ISO/IEC 27001 Lead Auditor exam - Valid ISO-IEC-27001-Lead-Auditor Valid Exam Syllabus Enter **【 www.troytecdumps.com 】** and search for ISO-IEC-27001-Lead-Auditor to download for free ISO-IEC-27001-Lead-Auditor Valid Test Tutorial
- ISO-IEC-27001-Lead-Auditor Valid Study Guide - ISO-IEC-27001-Lead-Auditor Exam Training Material - ISO-IEC-27001-Lead-Auditor Free Download Demo Easily obtain free download of ISO-IEC-27001-Lead-Auditor by searching on [www.pdfvce.com] ISO-IEC-27001-Lead-Auditor Valid Exam Practice
- Quiz 2026 PECB Reliable ISO-IEC-27001-Lead-Auditor Reliable Exam Question Open website www.testkingpass.com and search for [ISO-IEC-27001-Lead-Auditor] for free download Latest ISO-IEC-27001-Lead-Auditor Dumps Files
- ISO-IEC-27001-Lead-Auditor Study Guide - ISO-IEC-27001-Lead-Auditor Guide Torrent - ISO-IEC-27001-Lead-Auditor Practice Test Search for (ISO-IEC-27001-Lead-Auditor) and easily obtain a free download on **【 www.pdfvce.com 】** Valid Test ISO-IEC-27001-Lead-Auditor Tutorial
- ISO-IEC-27001-Lead-Auditor Training Pdf Most ISO-IEC-27001-Lead-Auditor Reliable Questions ISO-IEC-27001-Lead-Auditor Latest Exam Labs Search for ISO-IEC-27001-Lead-Auditor on { www.prepawayete.com } immediately to obtain a free download Reliable ISO-IEC-27001-Lead-Auditor Test Duration
- Hot ISO-IEC-27001-Lead-Auditor Reliable Exam Question | Amazing Pass Rate For ISO-IEC-27001-Lead-Auditor Exam | Trusted ISO-IEC-27001-Lead-Auditor: PECB Certified ISO/IEC 27001 Lead Auditor exam Simply search for ISO-IEC-27001-Lead-Auditor for free download on “ www.pdfvce.com ” ISO-IEC-27001-Lead-Auditor Pass Leader Dumps
- Valid ISO-IEC-27001-Lead-Auditor Exam Materials Customizable ISO-IEC-27001-Lead-Auditor Exam Mode Latest ISO-IEC-27001-Lead-Auditor Dumps Files Enter { www.examdumps.com } and search for (ISO-IEC-27001-Lead-Auditor) to download for free ISO-IEC-27001-Lead-Auditor Latest Exam Labs
- Free PDF 2026 PECB ISO-IEC-27001-Lead-Auditor: PECB Certified ISO/IEC 27001 Lead Auditor exam Fantastic

