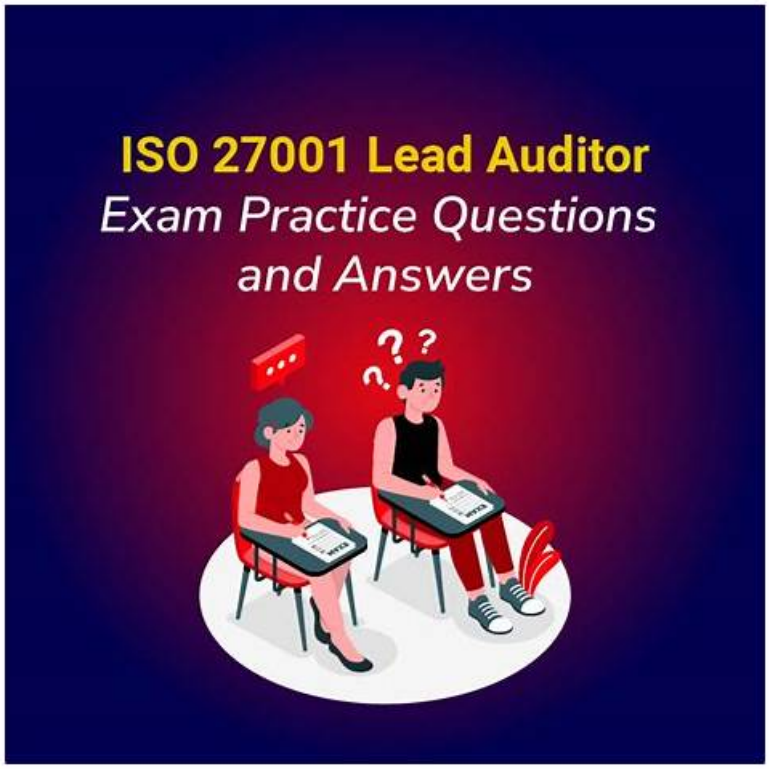
ISO-IEC-27001-Lead-Auditor Test Objectives Pdf - ISO-IEC-27001-Lead-Auditor Detailed Answers



P.S. Free 2026 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by RealExamFree: https://drive.google.com/open?id=1Ab_9ersmCOTDar0i6afNpOO9QnDtlOsr

Our ISO-IEC-27001-Lead-Auditor study materials boost the self-learning and self-evaluation functions so as to let the clients understand their learning results and learning process , then find the weak links to improve them. Through the self-learning function the learners can choose the learning methods by themselves and choose the contents which they think are important. Through the self-evaluation function the learners can evaluate their mastery degree of our ISO-IEC-27001-Lead-Auditor Study Materials and their learning process. The two functions can help the learners adjust their learning arrangements and schedules to efficiently prepare the exam.

To be eligible for the PECB ISO-IEC-27001-Lead-Auditor Certification Exam, individuals must have a minimum of five years of professional experience in information security, including two years of experience in ISMS implementation or auditing. They must also have completed a PECB ISO/IEC 27001 Lead Auditor training course or equivalent. ISO-IEC-27001-Lead-Auditor exam consists of multiple-choice questions and is available in several languages. Successful candidates demonstrate a comprehensive understanding of the ISO/IEC 27001 standard and are equipped to lead and manage a successful audit team. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is highly valued by organizations seeking to maintain the security and confidentiality of their information assets and provides a competitive advantage for professionals seeking career advancement in the field of information security.

PECB ISO-IEC-27001-Lead-Auditor Certification Exam is designed for professionals who wish to become certified as ISO/IEC 27001 Lead Auditors. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is globally recognized and demonstrates an individual's expertise in auditing information security management systems (ISMS) based on the ISO/IEC 27001 standard. ISO-IEC-27001-Lead-Auditor exam covers various topics such as auditing principles, techniques, and best practices, as well as risk management and information security controls.

PECB ISO-IEC-27001-Lead-Auditor Exam is intended for individuals who have already completed a lead auditor training program, or who have significant experience in the field of information security management. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is recognized worldwide and is highly valued by employers in the information security industry.

>> ISO-IEC-27001-Lead-Auditor Test Objectives Pdf <<

ISO-IEC-27001-Lead-Auditor Detailed Answers | ISO-IEC-27001-Lead-Auditor Valid Dumps Ebook

Everybody wants success, but not everyone has a strong mind to persevere in study. If you feel unsatisfied with your present status, our ISO-IEC-27001-Lead-Auditor actual exam can help you out. Our products always boast a pass rate as high as 99%. Using our ISO-IEC-27001-Lead-Auditor study materials can also save your time in the exam preparation. If you choose our ISO-IEC-27001-Lead-Auditor Test Engine, you are going to get the ISO-IEC-27001-Lead-Auditor certification easily. Just make your choice and purchase our study materials and start your study right now!

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q330-Q335):

NEW QUESTION # 330
In regard to generating an audit finding, select the words that best complete the following sentence.
To complete the sentence with the best word(s), 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 option to the appropriate blank section.

Answer:

Explanation:
Explanation
Audit evidence should be evaluated against the audit criteria in order to determine audit findings.
Audit evidence is the information obtained by the auditors during the audit process that is used as a basis for forming an audit opinion or conclusion12. Audit evidence could include records, documents, statements, observations, interviews, or test results12.
Audit criteria are the set of policies, procedures, standards, regulations, or requirements that are used as a reference against which audit evidence is compared12. Audit criteria could be derived from internal or external sources, such as ISO standards, industry best practices, or legal obligations12.
Audit findings are the results of a process that evaluates audit evidence and compares it against audit criteria13. Audit findings can show that audit criteria are being met (conformity) or that they are not being met (nonconformity). They can also identify best practices or improvement opportunities13.
References :=
ISO 19011:2022 Guidelines for auditing management systems
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements
Components of Audit Findings - The Institute of Internal Auditors

NEW QUESTION # 331
Which one of the following statements best describes the purpose of conducting a document review?

- A. To detect any nonconformity of the management system, if documented, with audit criteria and to identify information to support the audit plan
- B. To decide about the conformity of the documented management system with audit standards and to gather findings to support the audit process
- C. To reveal whether the documented management system is nonconforming with audit criteria and to gather evidence to support the audit report
- D. To determine the conformity of the management system, as far as documented, with audit criteria and to gather information to support the on-site audit activities

Answer: D

Explanation:
Explanation
A document review is a process of examining the documented information related to the management system before the on-site audit activities. The purpose of a document review is to: 12 Determine the conformity of the management system, as far as documented, with audit criteria, i.e., to check whether the documents are consistent, complete, and compliant with the requirements of ISO/IEC 27001 and any other applicable standards or regulations.
Gather information to support the on-site audit activities, i.e., to identify the scope, objectives, processes, controls, risks, and opportunities of the management system, and to plan the audit methods, techniques, and resources accordingly.

The other statements are not accurate, because:
A document review does not reveal or decide about the conformity or nonconformity of the management system as a whole, but only of the documented information. The conformity or nonconformity of the management system is determined by the on-site audit activities, which include interviews, observations, and tests12 A document review does not gather evidence or findings to support the audit report or process, but information to support the on-site audit activities. The evidence or findings are collected during the on-site audit activities, which are then documented and reported12 A document review does not detect any nonconformity of the management system, if documented, but determines the conformity of the documented information. The nonconformity of the management system is detected by the on-site audit activities, which evaluate the performance and effectiveness of the management system12 A document review does not identify information to support the audit plan, but gathers information to support the on-site audit activities. The audit plan is prepared before the document review, based on the audit scope, objectives, criteria, and program. The document review is part of the audit plan implementation12 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 # 332
Which two of the following statements are true?

- A. The benefit of certifying an ISMS is to obtain contracts from governmental institutions
- B. The purpose of an ISMS is to apply a risk management process for preserving information security
- C. The benefits of implementing an ISMS primarily result from a reduction in information security risks
- D. The purpose of an ISMS is to demonstrate compliance with regulatory requirements

Answer: B,C

Explanation:
The benefits of implementing an ISMS are not limited to a reduction in information security risks, but also include improved business performance, customer satisfaction, legal compliance, and stakeholder confidence.
The benefit of certifying an ISMS is not only to obtain contracts from governmental institutions, but also to demonstrate the organisation's commitment to information security to other potential customers, partners, and regulators. The purpose of an ISMS is to apply a risk management process for preserving information security, which means identifying, analysing, evaluating, treating, monitoring, and reviewing the information security risks that the organisation faces. The purpose of an ISMS is not to demonstrate compliance with regulatory requirements, but rather to ensure that the organisation meets its own information security objectives and obligations.
References:
* ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB
* ISO/IEC 27001:2013 Information technology - Security techniques - Information security
* management systems - Requirements [Section 0.1] and [Section 1]

NEW QUESTION # 333
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. Confidentiality and nondisclosure agreements
- B. The organisation's business continuity arrangements
- C. Information security awareness, education and training
- D. Access to and from the loading bay
- E. The organisation's arrangements for maintaining equipment
- F. The conducting of verification checks on personnel
- G. How information security has been addressed within supplier agreements
- H. The organisation's arrangements for information deletion
- I. How protection against malware is implemented
- J. Remote working arrangements
- K. The operation of the site CCTV and door control systems
- L. The development and maintenance of an information asset inventory
- M. Rules for transferring information within the organisation and to other organisations

- N. How the organisation evaluates its exposure to technical vulnerabilities
- O. How access to source code and development tools are managed
- P. How power and data cables enter the building

Answer: I,K,N,O

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. Reference: 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 # 334
What type of measure involves the stopping of possible consequences of security incidents?

- A. Preventive
- B. Detective
- C. Corrective
- D. Repressive

Answer: D

Explanation:
Explanation
A repressive measure is a type of measure that involves the stopping of possible consequences of security incidents. A security incident is an event that compromises the confidentiality, integrity, or availability of information assets3. A repressive measure is a measure that aims to prevent or reduce the harm caused by a security incident after it has occurred. Examples of repressive measures include blocking malicious IP addresses, revoking user access rights, isolating infected systems, or restoring data from backups4. Repressive measures are different from preventive measures, which are measures that aim to avoid or reduce the likelihood of a security incident before it occurs. Examples of preventive measures include installing antivirus software, enforcing password policies, encrypting sensitive data, or conducting security awareness training4.
Therefore, the correct answer is C. References: ISO/IEC 27000:2022, clause 3.25; Lepide.

NEW QUESTION # 335
......

Our experts are well-aware of the problems of exam candidates particularly of those who can't manage to spare time to study the ISO-IEC-27001-Lead-Auditor exam questions due to their heavy work pressure. Hence, our ISO-IEC-27001-Lead-Auditor study materials have been developed into a simple content and language for our worthy customers all over the world. What is more, you will find there are only the keypoints in our ISO-IEC-27001-Lead-Auditor learning guide.

ISO-IEC-27001-Lead-Auditor Detailed Answers: https://www.realexamfree.com/ISO-IEC-27001-Lead-Auditor-real-exam-dumps.html

P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by RealExamFree:

https://drive.google.com/open?id=1Ab_9ersmCOTDar0i6afNpOO9QnDtlOsr