Valid PECB ISO-IEC-27001-Lead-Auditor Test Dumps, 100% ISO-IEC-27001-Lead-Auditor Correct Answers

Real ISO-IEC-27001-Lead-Auditor Dumps - PECB
Correct Answers updated on 2023 [Q48-Q69]

What's more, part of that BraindumpsIT ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=1XURfJRbeDuPQ_J288ZvIhKeT_a_KQTMP

If you are clueless about the oncoming exam, our ISO-IEC-27001-Lead-Auditor practice materials are trustworthy materials for your information. More than tens of thousands of exam candidate coincide to choose our ISO-IEC-27001-Lead-Auditor practice materials. Our ISO-IEC-27001-Lead-Auditor practice materials are perfect for they come a long way on their quality. If you commit any errors, which can correct your errors with accuracy rate more than 98 percent. To get more useful information about our ISO-IEC-27001-Lead-Auditor practice materials, please read the following information.

PECB ISO-IEC-27001-Lead-Auditor certification exam is designed to validate the skills and knowledge of professionals in the field of information security management. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is ideal for individuals who want to demonstrate their expertise in auditing and assessing the effectiveness of an organization's information security management system (ISMS) based on the ISO/IEC 27001 standard.

The PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam is intended for professionals who want to become certified lead auditors for ISO/IEC 27001, including individuals who are responsible for managing an organization's ISMS, auditing ISMS, or providing consultancy services related to ISMS. ISO-IEC-27001-Lead-Auditor Exam covers a wide range of topics, including the principles, concepts, and requirements of ISO/IEC 27001, the audit process, and the roles and responsibilities of an auditor.

>> Valid PECB ISO-IEC-27001-Lead-Auditor Test Dumps <<

100% ISO-IEC-27001-Lead-Auditor Correct Answers | Reliable ISO-IEC-27001-Lead-Auditor Test Objectives

There are three versions of PECB Certified ISO/IEC 27001 Lead Auditor exam test torrent—PDF, software on pc, and app online， the most distinctive of which is that you can install ISO-IEC-27001-Lead-Auditor test answers on your computer to simulate the real exam environment, without limiting the number of computers installed. The buying process of ISO-IEC-27001-Lead-Auditor Test Answers is very simple, which is a big boon for simple people. After the payment of ISO-IEC-27001-Lead-Auditor guide torrent is successful, you will receive an email from our system within 5-10 minutes; click on the link to login and then you can learn immediately with ISO-IEC-27001-Lead-Auditor guide torrent.

PECB ISO-IEC-27001-Lead-Auditor Certification is recognized globally as a benchmark for professionals who want to demonstrate their competence in the field of information security management system auditing. PECB Certified ISO/IEC 27001 Lead Auditor exam certification provides tangible evidence of an individual's expertise and ability to effectively audit and assess the information security management system of an organization, ensuring that it complies with the requirements of the ISO 27001 standard. PECB Certified ISO/IEC 27001 Lead Auditor exam certification is also a valuable asset for professionals looking to advance their careers in the field of information security management, as it demonstrates their commitment to ongoing professional development and their dedication to maintaining the highest standards of excellence in their work.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q90-Q95):

NEW QUESTION # 90
A member of staff denies sending a particular message.
Which reliability aspect of information is in danger here?

- A. correctness
- B. integrity
- C. confidentiality
- D. availability

Answer: B

Explanation:
Explanation
The reliability aspect of information that is in danger when a member of staff denies sending a particular message is integrity. Integrity implies that information is authentic and can be verified as such. If a member of staff denies sending a message, it means that either the message was forged or the sender is lying, both of which violate the integrity of the information. Availability, correctness and confidentiality are not directly affected by this scenario. ISO/IEC 27001:2022 defines integrity as "property of accuracy and completeness" (see clause 3.24). References: [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 Integrity?

NEW QUESTION # 91
A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.
Where in the incident cycle is moving to a stand-by arrangements found?

- A. between threat and incident
- B. between damage and recovery
- C. between recovery and threat
- D. between incident and damage

Answer: D

NEW QUESTION # 92
Which one of the following statements best describes the purpose of conducting a document review?

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

Answer: A

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

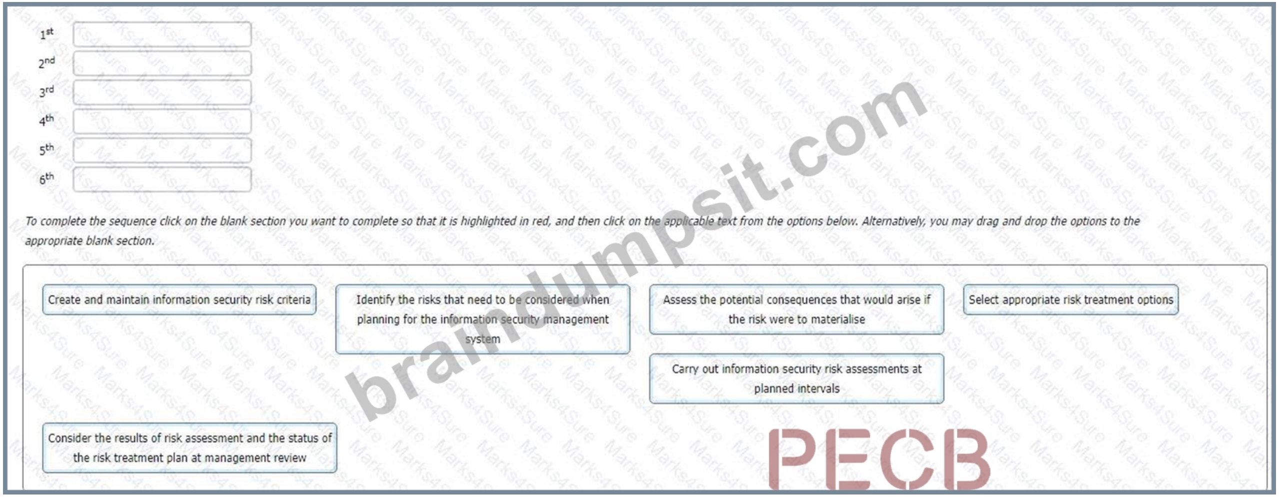
* A document review does not gather evidence or findings to support the audit report or process, but information to support the on-site audit activities. The evidence or findings are collected during the on-site audit activities, which are then documented and reported12

* 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 # 93

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?



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

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

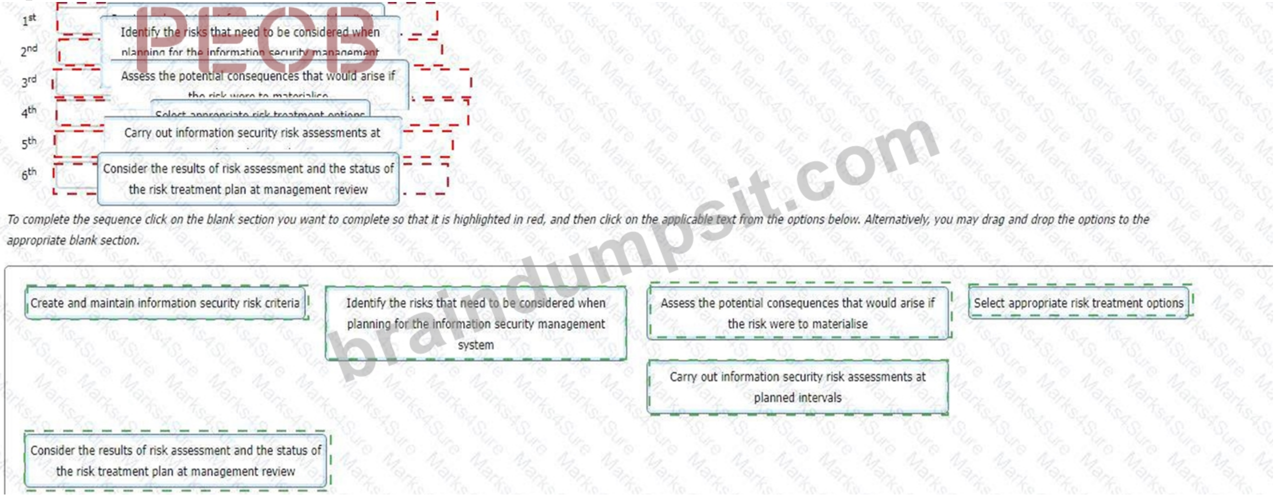
Select appropriate risk treatment options

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:



1st
2nd Identify the risks that need to be considered when planning for the information security management
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
6th 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

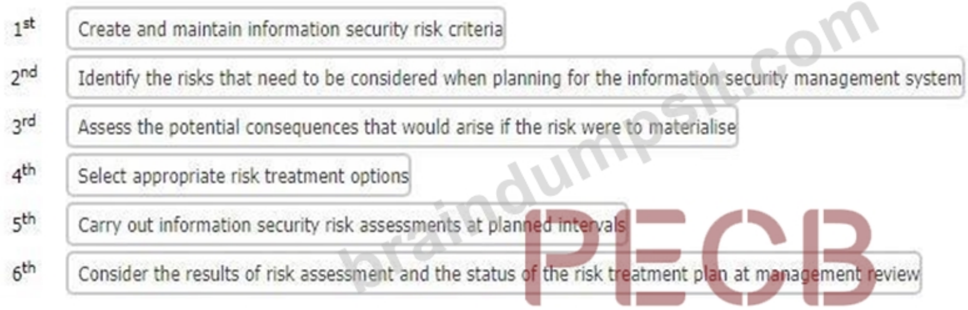
Assess the potential consequences that would arise if the risk were to materialise

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:



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

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:

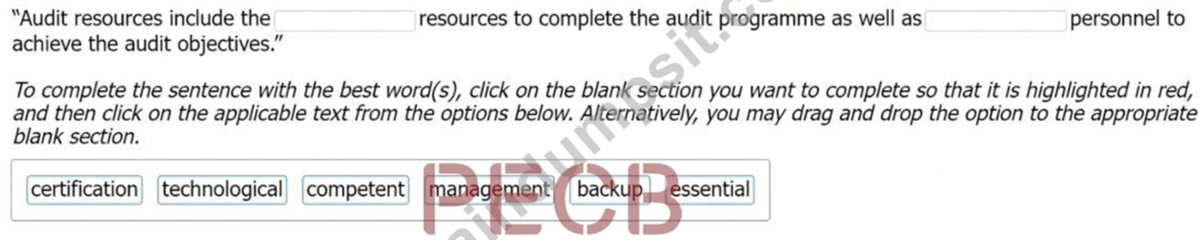
* establishing and maintaining information security risk criteria;
* ensuring that repeated information security risk assessments produce consistent, valid and comparable results;
* identifying the information security risks;
* analyzing the information security risks;
* evaluating the information security 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:

* ISO/IEC 27001:2022, clause 6.1
* [PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 14-15
* ISO 27001 Risk Management in Plain English

NEW QUESTION # 94

Select the words that best complete the sentence below to describe audit resources:



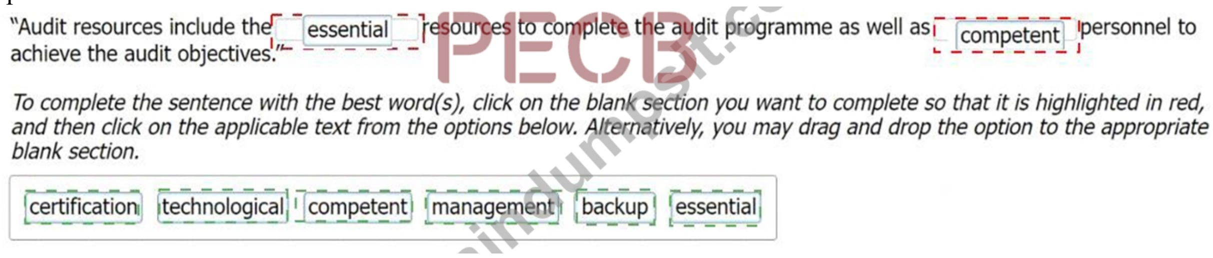
"Audit resources include the ______ resources to complete the audit programme as well as ______ personnel to achieve the audit objectives."

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.

certification | technological | competent | management | backup | essential

Answer:

Explanation:



"Audit resources include the essential resources to complete the audit programme as well as competent personnel to achieve the audit objectives."

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.

certification | technological | competent | management | backup | essential

Explanation:

According to ISO 19011:2018, clause 5.3, the person responsible for managing the audit programme should determine the resources necessary for the audit programme, such as the audit team members, the budget, the time, the tools, etc. The audit resources should be sufficient and appropriate to ensure the quality and effectiveness of the audit programme and the audit results. The audit resources include the following elements12:

* Essential resources: These are the resources that are required to conduct the audit programme and the individual audits, such as

the audit documents, the audit methods, the audit tools, the audit schedule, the audit budget, etc. The essential resources should be identified and allocated based on the audit objectives, scope, and criteria, and the availability and cooperation of the auditee. The essential resources should also be reviewed and updated as necessary to reflect any changes or deviations in the audit programme or the individual audits.

* Competent personnel: These are the audit team members who have the appropriate knowledge, skills, and experience to conduct the audit effectively and efficiently, and to provide credible and reliable audit results and recommendations. The competent personnel should include the audit team leader, the auditors, and any technical experts or observers who support the audit team. The competent personnel
* should be selected and appointed based on the audit objectives, scope, and criteria, and the specific competence requirements for the audit programme and the individual audits. The competent personnel should also be independent and impartial, and avoid any conflicts of interest or self-interest that may affect the audit results or the audit decisions.

References:
* ISO 19011:2018 - Guidelines for auditing management systems, clause 5.3
* PECB Candidate Handbook ISO 27001 Lead Auditor, page 19

NEW QUESTION # 95

......

course.rowholesaler.com, Disposable vapes

DOWNLOAD the newest BraindumpsIT ISO-IEC-27001-Lead-Auditor PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1XURfJRbeDuPQ_J288ZvIhKeT_a_KQTMP