ISO-IEC-27001-Lead-Auditor Übungsmaterialien, ISO-IEC-27001-Lead-Auditor Unterlage

Laden Sie die neuesten ITZert ISO-IEC-27001-Lead-Auditor PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1hUPO1pvHoAF1N6f0pz4MEUJK1ta_Gm4g

Die echten und originalen Prüfungsfragen und Antworten zu ISO-IEC-27001-Lead-Auditor（PECB Certified ISO/IEC 27001 Lead Auditor exam）bei ITZert wurden verfasst von unseren PECB-Experten mit den Informationen von ISO-IEC-27001-Lead-Auditor（PECB Certified ISO/IEC 27001 Lead Auditor exam）aus dem Testcenter wie PROMETRIC oder VUE.

Die PECB ISO-IEC-27001-Lead-Auditor-Prüfung ist eine wesentliche Zertifizierung für Fachleute, die Experten in der Prüfung von Informationssicherheitsmanagementsystemen werden möchten. Diese Zertifizierung ist von Organisationen hoch geschätzt und zeigt, dass der Inhaber die erforderlichen Fähigkeiten und Kenntnisse hat, um effektive Audits durchzuführen, die den Anforderungen von ISO/IEC 27001 entsprechen. Wenn Sie Ihre Karriere im Bereich des Informationssicherheitsmanagements verbessern möchten, ist die PECB ISO-IEC-27001-Lead-Auditor-Zertifizierung definitiv eine Überlegung wert.

Die Prüfung besteht aus einer schriftlichen Prüfung und einer praktischen Prüfung. Die schriftliche Prüfung behandelt die theoretischen Aspekte des Informations-Sicherheits-Managements und der Prüfung, während die praktische Prüfung die Fähigkeit einer Person bewertet, die gelernten Konzepte in einer realen Situation anzuwenden. Die Prüfung ist anspruchsvoll und es wird erwartet, dass die Teilnehmer ein solides Verständnis der Prinzipien des Informations-Sicherheits-Managements, des Risikomanagements und des Prüfungsprozesses haben.

Die PECB ISO-IEC-27001-Lead-Auditor-Prüfung ist eine international anerkannte Zertifizierung, die die Kompetenz einer Person in der Prüfung eines Information Security Management Systems (ISMS) gegen den ISO/IEC 27001-Standard bestätigt. Die Prüfung wird vom Professional Evaluation and Certification Board (PECB) angeboten, einem führenden Anbieter von Schulungen, Prüfungen und Zertifizierungsdiensten für eine Vielzahl internationaler Standards.

>> ISO-IEC-27001-Lead-Auditor Übungsmaterialien <<

ISO-IEC-27001-Lead-Auditor Unterlage & ISO-IEC-27001-Lead-Auditor Prüfungsaufgaben

Wenn Sie Ihre Position in der konkurrenzfähigen Gesellschaft durch die PECB ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung festigen und Ihre fachliche Fähigkeiten verbessern wollen, müssen Sie gute Fachkenntnisse besitzen und sich viel Mühe für die Prüfung geben. Aber es ist nicht so einfach, die PECB ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung zu bestehen. Vielleicht durch die PECB ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung können Sie Ihnen der IT-Branche vorstellen. Aber man braucht nicht unbedingt viel Zeit und Energie, die Fachkenntnisse kennenzulernen. Sie können die Schulungsunterlagen zur PECB ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung von ITZert wählen. Sie werden zielgerichtet nach den IT-Zertifizierungsprüfungen entwickelt. Mit ihr können Sie mühelos die schwierige PECB ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung bestehen.

PECB Certified ISO/IEC 27001 Lead Auditor exam ISO-IEC-27001-Lead-Auditor Prüfungsfragen mit Lösungen (Q100-Q105):

100. Frage
Scenario 2: Knight is an electronics company from Northern California, US that develops video game consoles. Knight has more than 300 employees worldwide. On the fifth anniversary of their establishment, they have decided to deliver the G-Console, a new generation video game console aimed for worldwide markets. G-Console is considered to be the ultimate media machine of 2021 which will give the best gaming experience to players.
The console pack will include a pair of VR headset, two
games, and other gifts.
Over the years, the company has developed a good reputation by showing integrity, honesty, and respect toward their customers. This good reputation is one of the reasons why most passionate gamers aim to have Knight's G-console as soon as it is released in the market.
Besides being a very customer-oriented company, Knight
also gained wide recognition within the gaming industry because of the developing quality. Their prices are a bit higher than the reasonable standards allow.
Nonetheless, that is not considered an issue for most loyal customers of Knight, as their quality is top-notch.
Being one of the top video game console developers in the world, Knight is also often the center of attention for malicious activities. The company has had an operational ISMS for over a year. The ISMS scope includes all departments of Knight, except Finance and HR departments.
Recently, a number of Knight's files containing proprietary information were leaked by hackers. Knight's incident response team (IRT) immediately started to analyze every part of the system and the details of the incident.
The IRT's first suspicion was that Knight's employees used weak passwords and consequently were easily cracked by hackers who gained unauthorized access to their accounts. However, after carefully investigating the incident, the IRT determined that hackers accessed accounts by capturing the file transfer protocol (FTP) traffic.
FTP is a network protocol for transferring files between accounts. It uses clear text passwords for authentication.
Following the impact of this information security incident and with IRT's suggestion, Knight decided to replace the FTP with Secure Shell (SSH) protocol, so anyone capturing the traffic can only see encrypted data.
Following these changes, Knight conducted a risk assessment to verify that the implementation of controls had minimized the risk of similar incidents. The results of the process were approved by the ISMS project manager who claimed that the level of risk after the implementation of new controls was in accordance with the company's risk acceptance levels.
Based on this scenario, answer the following question:
According to scenario 2, the ISMS scope was not applied to the Finance and HR Department of Knight. Is this acceptable?

- A. No, the ISMS scope must include all organizational units and processes
- B. Yes, the ISMS must be applied only to processes and assets that may directly impact information security
- C. Yes, the ISMS scope can include the whole organization or only particular departments within the organization

Antwort: C

101. Frage
You are an experienced ISMS audit team leader conducting a third-party surveillance audit of an internet services provider. You are reviewing the organization's risk assessment processes for conformity with ISO/IEC 27001:2022.
Which three of the following audit findings would prompt you to raise a nonconformity report?

- A. The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
- B. The organisation's risk assessment criteria have not been reviewed and approved by top management
- C. The organisation's information security risk assessment process suggests each risk is allocated a risk owner
- D. There is a different system in place for assessing operational information security risks and for assessing strategic information security risks
- E. The organisation has not used RAG (Red, Amber, Green) to classify its' information security risks. Instead, it has used a smiling emoji, a neutral face emoji and a sad face emoji
- F. Both systems contain additional information security risks which are not associated with preserving the confidentiality, integrity and accessibility of information
- G. The organisation has assessed the probability of all of its information security risks as either 0%, 25%, 50%, 75% or 100%
- H. The organisation is treating information security risks in the order in which they are identified

Antwort: A,B,H

Begründung:
The three audit findings that would prompt you to raise a nonconformity report are:
*The organisation is treating information security risks in the order in which they are identified
*The organisation's risk assessment criteria have not been reviewed and approved by top management
*The organisation's information security risk assessment process is based solely on an assessment of the impact of each risk
According to ISO/IEC 27001:2022, clause 6.1.2, the organisation must establish and maintain an information security risk management process that is consistent with the organisation's context and aligned with its overall risk management approach1. This process must include the following steps:
*Establishing the risk assessment criteria, which must be approved by top management and reflect the organisation's risk appetite and objectives2
*Identifying the information security risks, which must consider the assets, threats, vulnerabilities, impacts, and likelihoods3
*Analysing the information security risks, which must determine the levels of risk and compare them with the risk criteria4
*Evaluating the information security risks, which must prioritise the risks and decide whether they need treatment or not5 Therefore, the audit findings B, E, and F indicate that the organisation is not following the required steps of the information security risk management process, and thus are nonconformities with the standard.
The other audit findings are not necessarily nonconformities, as they may be acceptable depending on the organisation's context and justification. For example:
*Audit finding A may be acceptable if the organisation has identified and treated the additional information security risks that are relevant to its scope and objectives, and has documented the rationale for doing so6
*Audit finding C may be acceptable if the organisation has assigned clear roles and responsibilities for the information security risk management process, and has ensured that the risk owners have the authority and competence to manage the risks7
*Audit finding D may be acceptable if the organisation has defined and communicated the meaning and implications of the emoji-based risk classification, and has ensured that it is consistent with the risk criteria and the risk treatment process8
*Audit finding G may be acceptable if the organisation has justified the use of discrete values for the probability of the information security risks, and has ensured that they are realistic and consistent with the risk criteria and the risk analysis method9
*Audit finding H may be acceptable if the organisation has established and maintained different systems for assessing operational and strategic information security risks, and has ensured that they are integrated and aligned with the overall risk management approach and the ISMS objectives10 References: 1: ISO/IEC 27001:2022, 6.1.2; 2: ISO/IEC 27001:2022, 6.1.2 a); 3: ISO/IEC 27001:2022, 6.1.2 b); 4: ISO/IEC 27001:2022, 6.1.2 c); 5: ISO/IEC 27001:2022, 6.1.2 d); 6: ISO/IEC 27001:2022, A.0.2; 7: ISO/IEC 27001:2022, 5.3; 8: ISO/IEC 27001:2022, 6.1.2 a) 2); 9: ISO/IEC 27001:2022, 6.1.2 c) 2); 10: ISO/IEC 27001:2022, 6.1.2 a) 1); : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

102. Frage
You are an experienced ISMS audit team leader conducting a third-party surveillance visit.
You notice that although the auditee is claiming conformity with ISO/IEC 27001:2022 they are still referring to Improvement as clause 10.2 (as it was in the 2013 edition) when this is now clause 10.1 in the 2022 edition. You have confirmed they are meeting all of the 2022 requirements set out in the standard.
Select one option of the action you should take.

- A. Bring the matter up at the closing meeting
- B. Raise a nonconformity against clause 7.5.3 - Control of documented information
- C. Note the issue in the audit report
- D. Raise it as an opportunity for improvement

Antwort: D

Begründung:
The correct action to take in this situation is to raise it as an opportunity for improvement. This is because the auditee is not violating any requirement of the standard, but rather using outdated terminology that does not reflect the current version of the standard. An opportunity for improvement is a suggestion for enhancing the performance or effectiveness of the ISMS1. It is not a nonconformity, which is a failure to fulfil a requirement2. Therefore, option B is incorrect. Option A is also incorrect, because noting the issue in the audit report without raising it as an opportunity for improvement would not provide any value or feedback to the auditee. Option D is also incorrect, because bringing the matter up at the closing meeting without documenting it as an opportunity for improvement would not ensure that the auditee takes any action to address it.
References: 1: ISMS Auditing Guideline - ISO27000, page 11; 2: ISO/IEC 27000:2022, 3.28; : ISMS Auditing Guideline - ISO27000; : ISO/IEC 27000:2022

103. Frage
You are an experienced ISMS audit team leader. An auditor in training has approached you to ask you to clarify the different types of audits she may be required to undertake.
Match the following audit types to the descriptions.
To complete the table click on the blank section you want to complete so that It is highlighted In fed, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Antwort:

Begründung:
Explanation:

104. Frage
You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.
The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.
Select three options that relate to ISO/IEC 27001:2022's requirements regarding external providers.

- A. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
- B. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
- C. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
- D. I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
- E. I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
- F. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
- G. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
- H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest

Antwort: C,D,G

Begründung:
A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12
B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO
27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12
E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider's deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12
F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it

is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO
27001:2022:
C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12
D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12
G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12
H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 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

105. Frage
.....

von { ISO-IEC-27001-Lead-Auditor } □ISO-IEC-27001-Lead-Auditor Fragenpool

- ISO-IEC-27001-Lead-Auditor Studienmaterialien: PECB Certified ISO/IEC 27001 Lead Auditor exam - ISO-IEC-27001-Lead-Auditor Zertifizierungstraining □ Suchen Sie auf der Webseite [www.pruefungfrage.de] nach [ISO-IEC-27001-Lead-Auditor] und laden Sie es kostenlos herunter □ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung
- ISO-IEC-27001-Lead-Auditor Der beste Partner bei Ihrer Vorbereitung der PECB Certified ISO/IEC 27001 Lead Auditor exam □ Öffnen Sie die Webseite ✔ www.itzert.com □✔□ und suchen Sie nach kostenloser Download von ✔ ISO-IEC-27001-Lead-Auditor □✔□ □ISO-IEC-27001-Lead-Auditor Dumps Deutsch
- ISO-IEC-27001-Lead-Auditor Der beste Partner bei Ihrer Vorbereitung der PECB Certified ISO/IEC 27001 Lead Auditor exam □ Suchen Sie einfach auf □ de.fast2test.com □ nach kostenloser Download von ✔ ISO-IEC-27001-Lead-Auditor □✔□ □ISO-IEC-27001-Lead-Auditor Zertifizierungsprüfung
- ISO-IEC-27001-Lead-Auditor Antworten □ ISO-IEC-27001-Lead-Auditor Deutsch □ ISO-IEC-27001-Lead-Auditor Zertifikatsdemo □ Suchen Sie jetzt auf 「 www.itzert.com 」 nach ➡ ISO-IEC-27001-Lead-Auditor □□□ und laden Sie es kostenlos herunter □ISO-IEC-27001-Lead-Auditor PDF Testsoftware
- ISO-IEC-27001-Lead-Auditor Studienmaterialien: PECB Certified ISO/IEC 27001 Lead Auditor exam - ISO-IEC-27001-Lead-Auditor Zertifizierungstraining □ Suchen Sie jetzt auf [www.pruefungfrage.de] nach ➤ ISO-IEC-27001-Lead-Auditor □ und laden Sie es kostenlos herunter □ISO-IEC-27001-Lead-Auditor Musterprüfungsfragen
- myportal.utt.edu.tt, learn.eggdemy.com, 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, 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, cfdbaba.com, 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, Disposable vapes

BONUS!!! Laden Sie die vollständige Version der ITZert ISO-IEC-27001-Lead-Auditor Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1hUPO1pvHoAF1N6f0pz4MEUJK1ta_Gm4g