ISO-IEC-27001-Lead-Implementer Übungsmaterialien & ISO-IEC-27001-Lead-Implementer Echte Fragen

P.S. Kostenlose und neue ISO-IEC-27001-Lead-Implementer Prüfungsfragen sind auf Google Drive freigegeben von Zertpruefung verfügbar: https://drive.google.com/open?id=1fGIW7TBsZQNKy-Jt9H_mrzBlJjnXdoed

Vielleicht können Sie auch die relevanten PECB ISO-IEC-27001-Lead-Implementer Schulungsunterlagen in anderen Büchern oder auf anderen Websites finden. Aber wenn Sie die Produkte von Zertpruefung mit ihnen vergleichen, würden Sie herausfinden, dass unsere Produkte mehr Wissensgebiete umfassen. Sie können auch im Internet teilweise die Fragen und Antworten zur PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung kostenlos herunterladen, so dass Sie die Qualität unserer Produkte testen können. Die Gründe, dass Zertpruefung exklusiv umfassende Materialien von guter Qualität bieten können, liegt darin, dass wir ein exzellentes Expertenteam hat. Sie bearbeiten die neuesten Fragen und Antworten zur PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung nach ihren IT-Kenntnissen und Erfahrungen. Deshalb sind die Fragen und Antworten zur PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung von Zertpruefung bei den Kandidaten ganz beliebt.

Der ISO/IEC 27001-Standard ist ein weltweit anerkannter Rahmen für die Verwaltung von Informationssicherheitsrisiken und den Schutz sensibler Informationen. Die PECB ISO-IEC-27001-Lead-Implementer-Zertifizierungsprüfung umfasst die wesentlichen Komponenten des ISO/IEC 27001-Standards, einschließlich des Risikobewertungsprozesses, der Implementierung von Sicherheitskontrollen und der laufenden Überwachung und Überprüfung des ISMS.

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

ISO-IEC-27001-Lead-Implementer Echte Fragen & ISO-IEC-27001-Lead-Implementer Unterlage

Die Feedbacks von den IT-Kandidaten, die die schulungsunterlagen zur PECB ISO-IEC-27001-Lead-Implementer (PECB Certified ISO/IEC 27001 Lead Implementer Exam) IT-Prüfung von Zertpruefung benutzt haben, haben sich bewiesen, dass es leicht ist, die Prüfung mit Hilfe unserer Zertpruefung Produkten zu bestehen. Zur Zeit hat Zertpruefung die Schulungsprogramme zur beliebten PECB ISO-IEC-27001-Lead-Implementer (PECB Certified ISO/IEC 27001 Lead Implementer Exam) Zertifizierungsprüfung, die zielgerichteten Prüfungen beinhalten, entwickelt, um Ihr Know-How zu konsolidieren und sich gut auf die Prüfung vorzubereiten.

Einzelne Personen, die die PECB ISO-IEC-27001-Lead-Implementer-Prüfung bestehen, werden als zertifizierte ISO/IEC 27001 Lead Implementers anerkannt. Diese Zertifizierung zeigt, dass die Person das notwendige Wissen und die Fähigkeiten besitzt, um eine Organisation bei der Implementierung eines ISMS auf Basis des ISO/IEC 27001 Standards zu führen. Diese Zertifizierung wird von Organisationen, die Informationssicherheit priorisieren, sehr geschätzt und ist ein wichtiger Unterscheidungsmerkmal für Personen, die in diesem Bereich eine Anstellung suchen.

Der ISO/IEC 27001 -Standard ist einer der am weitesten verbreiteten und angesehensten Standards für Informationssicherheitsmanagement der Welt. Es bietet einen Rahmen für das Verwalten und Schutz sensibler Informationen und hilft Unternehmen, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten zu gewährleisten. Die ISO/IEC 27001 Lead

Implementierer -Zertifizierungsprüfung soll die Fähigkeit einer Person testen, diesen Standard effektiv in einer Organisation zu implementieren.

PECB Certified ISO/IEC 27001 Lead Implementer Exam ISO-IEC-27001-Lead-Implementer Prüfungsfragen mit Lösungen (Q49-Q54):

49. Frage
Which of the following statements regarding information security risk is NOT correct?

- A. Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats
- B. Information security risk can be expressed as the effect of uncertainty on information security objectives
- C. Information security risk cannot be accepted without being treated or during the process of risk treatment

Antwort: C

Begründung:
According to ISO/IEC 27001:2022, information security risk can be accepted as one of the four possible options for risk treatment, along with avoiding, modifying, or sharing the risk12. Risk acceptance means that the organization decides to tolerate the level of risk without taking any further action to reduce it3. Risk acceptance can be done before, during, or after the risk treatment process, depending on the organization's risk criteria and the residual risk level4.
1: ISO 27001 Risk Assessments | IT Governance UK 2: ISO 27001 Risk Assessment: 7 Step Guide - IT Governance UK Blog 3: ISO 27001 Clause 6.1.2 Information security risk assessment process 4: ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide - Advisera

50. Frage
Scenario:
Jane is a developer deploying an application using a language supported by her cloud provider. She doesn't manage the underlying infrastructure but needs control over the application and its environment.
Which cloud service model does Jane need?

- A. Software as a Service
- B. Infrastructure as a Service
- C. Platform as a Service

Antwort: C

51. Frage
An organization documented each security control that it Implemented by describing their functions in detail.
Is this compliant with ISO/IEC 27001?

- A. No, the standard requires to document only the operation of processes and controls, so no description of each security control is needed
- B. Yes, but documenting each security control and not the process in general will make it difficult to review the documented information
- C. No, because the documented information should have a strict format, including the date, version number and author identification

Antwort: B

Begründung:
According to ISO/IEC 27001:2022, clause 7.5, an organization is required to maintain documented information to support the operation of its processes and to have confidence that the processes are being carried out as planned. This includes documenting the information security policy, the scope of the ISMS, the risk assessment and treatment methodology, the statement of applicability, the risk treatment plan, the information security objectives, and the results of monitoring, measurement, analysis, evaluation, internal audit, and management review. However, the standard does not specify the level of detail or the format of the documented information, as long as it is suitable for the organization's needs and context. Therefore, documenting each security control that is implemented by describing their functions in detail is not a violation of the standard, but it may not be the most efficient or effective way to document the ISMS. Documenting each security control separately may make it harder to review, update, and communicate

the documented information, and may also create unnecessary duplication or inconsistency. A better approach would be to document the processes and activities that involve the use of security controls, and to reference the relevant controls from Annex A or other sources. This way, the documented information would be more aligned with the process approach and the Plan-Do-Check-Act cycle that the standard promotes.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clauses 4.3, 5.2, 6.1, 6.2, 7.5, 8.2, 8.3, 9.1, 9.2, 9.3, and Annex A ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

52. Frage
Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.
Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible. Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.
To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.
Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.
Based on scenario 3. which information security control of Annex A of ISO/IEC 27001 did Socket Inc. implement by establishing a new system to maintain, collect, and analyze information related to information security threats?

- A. Annex A 5 7 Threat Intelligence
- B. Annex A 5.5 Contact with authorities
- C. Annex A 5.13 Labeling of information

Antwort: A

53. Frage
Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs. computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.
Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security- related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.
One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on the scenario above, answer the following question:
How should Colin have handled the situation with Lisa?

- A. Promise Lisa that future training and awareness sessions will be easily understandable
- B. Deliver training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company
- C. Extend the duration of the training and awareness session in order to be able to achieve better results

Antwort: B

Begründung:
According to the ISO/IEC 27001:2022 standard, the organization should determine the necessary competence of persons doing work under its control that affects the performance and effectiveness of the ISMS. The organization should also ensure that these persons are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming with the ISMS requirements, and the benefits of improved information security performance. The organization should

also provide information security awareness, education, and training to all employees and, where relevant, contractors and third-party users, as relevant for their job function. The awareness, education, and training programs should be planned, implemented, and maintained according to the needs of the organization and the results of the risk assessment and risk treatment.
Therefore, Colin should have handled the situation with Lisa by delivering training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company.
This would ensure that the content and the language of the sessions are appropriate and understandable for the target audience, and that the sessions are effective and efficient in achieving the desired learning outcomes.
By doing so, Colin would also avoid wasting time and resources on delivering sessions that are too technical or too basic for some employees, and that do not address their specific information security challenges and responsibilities.
ISO/IEC 27001:2022, Clause 7.2 Competence and Clause 7.3 Awareness
ISO/IEC 27002:2022, Clause 7.2.2 Information security awareness, education and training PECB ISO/IEC 27001 Lead Implementer Course, Module 4: Leadership, Commitment, and Support of Top Management.

54. Frage
.....

myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.notebook.ai, Disposable vapes

P.S. Kostenlose 2026 PECB ISO-IEC-27001-Lead-Implementer Prüfungsfragen sind auf Google Drive freigegeben von Zertpruefung verfügbar: https://drive.google.com/open?id=1fGIW7TBsZQNKy-Jt9H_mrzBlJjnXdoed