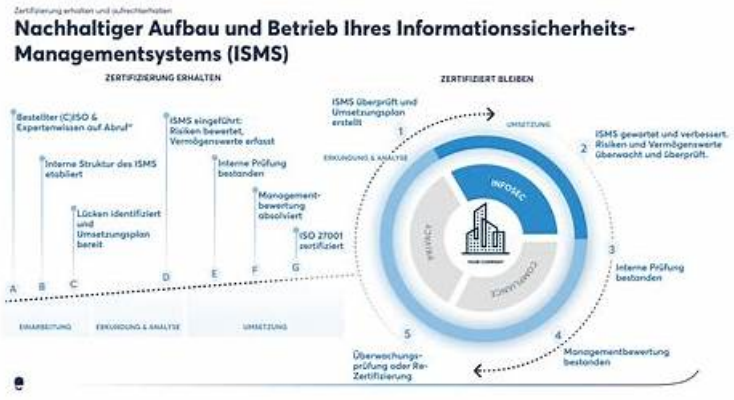
Sie können so einfach wie möglich - ISO-IEC-27001-Lead-Implementer bestehen!



P.S. Kostenlose 2026 PECB ISO-IEC-27001-Lead-Implementer Prüfungsfragen sind auf Google Drive freigegeben von ExamFragen verfügbar: https://drive.google.com/open?id=1i-pkWwOVCB6PGMcOnfidki4HgcRK0nJZ

Schulungsunterlagen zur PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung von ExamFragen sind effizient, die von manchen Experten und einigen bestandenen Kandidaten bewiesen sind. Sie sind fast gleich wie die echten ISO-IEC-27001-Lead-Implementer Prüfungsfragen. Sie können Ihnen dabei helfen, die ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung zu bestehen. Wir werden Ihnen alle Ihren bezahlten Summe zurückgeben, entweder Sie die ISO-IEC-27001-Lead-Implementer Prüfung nicht bestehen, oder die Testaufgaben von PECB ISO-IEC-27001-Lead-Implementer irgend ein Qualitätsproblem haben. Vertrauen Sie bitte auf ExamFragen, denn wir werden Ihnen stets begleiten.

Die Zertifizierungsprüfung PECB ISO-IEC-27001-Lead-Implementer ist eine wichtige Referenz für Fachleute, die ihre Expertise im Informations-Sicherheitsmanagement und ihre Fähigkeit zur Implementierung und Aufrechterhaltung eines ISMS auf der Grundlage des ISO/IEC 27001 Standards demonstrieren wollen. Diese Zertifizierung ist weltweit hoch angesehen und kann zu besseren Jobmöglichkeiten und höheren Gehältern für zertifizierte Fachleute führen.

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

ISO-IEC-27001-Lead-Implementer Schulungsangebot, ISO-IEC-27001-Lead-Implementer Testing Engine, PECB Certified ISO/IEC 27001 Lead Implementer Exam Trainingsunterlagen

Nun ist eine Gesellschaft, die mit den fähigen Leuten überschwemmt. Aber viele Fachleute fehlen trotzdem doch. Beispielsweise fehlen in der IT-Branche Techniker. Und die PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung sit eine Prüfung, die IT-Technik testet. ExamFragen ist eine Website, die Ihnen Kenntnise zur PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung liefert.

PECB Certified ISO/IEC 27001 Lead Implementer Exam ISO-IEC-27001-Lead-Implementer Prüfungsfragen mit Lösungen (Q204-Q209):

204. Frage
Who should be involved, among others, in the draft, review, and validation of information security procedures?

- A. An external expert
- B. The employees in charge of ISMS operation
- C. The information security committee

Antwort: C

Begründung:
Explanation

According to ISO/IEC 27001:2022, clause 7.5.1, the organization shall ensure that the documented information required by the ISMS and by this document is controlled to ensure that it is available and suitable for use, where and when it is needed, and that it is adequately protected. This includes ensuring that the documented information is reviewed and approved for suitability and adequacy. The information security procedures are part of the documented information that supports the operation of the ISMS processes and the implementation of the information security controls. Therefore, they should be drafted, reviewed, and validated by the information security committee, which is the group of people responsible for overseeing the ISMS and ensuring its alignment with the organization's objectives and strategy. The information security committee should include representatives from different functions and levels of the organization, as well as external experts if needed. The information security committee should also ensure that the information security procedures are communicated to the relevant employees and other interested parties, and that they are periodically reviewed and updated as necessary.
References:
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clauses 5.3, 7.5.1, and 9.3 ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

205. Frage
Which statement is an example of risk retention?

- A. An organization terminates work in the construction site during a severe storm
- B. An organization has implemented a data loss protection software
- C. An organization has decided to release the software even though some minor bugs have not been fixed yet

Antwort: C

Begründung:
According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, either because the bugs are not critical or because the cost of fixing them would outweigh the benefits.
ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process
3, ISO 27001: Top risk treatment options and controls explained

206. Frage
Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.
Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company's departments within the ISMS scope.
The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.
Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.
Operaze decided to migrate Its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.
Based on scenario 5. which committee should Operaze create to ensure the smooth running of the ISMS?

- A. Information security committee
- B. Operational committee
- C. Management committee

Antwort: A

Begründung:
According to ISO/IEC 27001:2022, clause 5.1, the top management of an organization is responsible for ensuring the leadership and commitment for the ISMS. However, the top management may delegate some of its responsibilities to an information security committee, which is a group of people who oversee the ISMS and provide guidance and support for its implementation and operation. The information security committee may include representatives from different departments, functions, or levels of the organization, as well as external experts or consultants. The information security committee may have various roles and responsibilities, such as:
Establishing the information security policy and objectives
Approving the risk assessment and risk treatment methodology and criteria Reviewing and approving the risk assessment and risk treatment results and plans Monitoring and evaluating the performance and effectiveness of the ISMS Reviewing and approving the internal and external audit plans and reports Initiating and approving corrective and preventive actions Communicating and promoting the ISMS to all interested parties Ensuring the alignment of the ISMS with the strategic direction and objectives of the organization Ensuring the availability of resources and competencies for the ISMS Ensuring the continual improvement of the ISMS Therefore, in scenario 5, Operaze should create an information security committee to ensure the smooth running of the ISMS, as this committee would provide the necessary leadership, guidance, and support for the ISMS implementation and operation.
ISO/IEC 27001:2022, clause 5.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 9.

207. Frage
Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [