# Die seit kurzem aktuellsten PECB ISO-IEC-27001-Lead-Implementer Prüfungsinformationen, 100% Garantie für Ihen Erfolg in der Prüfungen!


Außerdem sind jetzt einige Teile dieser ITZert ISO-IEC-27001-Lead-Implementer Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=16X9BT6RCX38QnfgFv8QLK2nxEk3d3A9k

Wissen Sie PECB ISO-IEC-27001-Lead-Implementer Dumps von ITZert? Warum sind diese Dumps von den Benutzern gut bewertet? Wollen Sie diese Dumps probieren? Klicken Sie bitte ITZert Website und die Demo herunterladen. Und jedr Fragenkatalog hat eine kostlose Demo. Wenn Sie es gut finden, können Sie diese Dumps sofort kaufen. Nach dem Kauf können Sie auch einen einjährigen kostlosen Aktualisierungsservice bekommen. Innerhalb eines Jahres können Sie die neuesten PECB ISO-IEC-27001-Lead-Implementer Prüfungsunterlagen besitzen. Damit können Sie PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung sehr leicht bestehen und dieses Zertifikat bekommen.

Die PECB ISO-IEC-27001-Lead-Implementer Prüfung ist ein Zertifizierungsprogramm, das entwickelt wurde, um Einzelpersonen das notwendige Wissen und die Fähigkeiten zur Implementierung und Verwaltung eines Informationssicherheitsmanagementsystems (ISMS) auf der Grundlage des ISO/IEC 27001 Standards zu vermitteln. Diese Zertifizierung wird von der Professional Evaluation and Certification Board (PECB) verliehen, einer international anerkannten Organisation, die die berufliche Entwicklung und Zertifizierung in verschiedenen Bereichen fördert und unterstützt.

**>> ISO-IEC-27001-Lead-Implementer Schulungsunterlagen <<**

## ISO-IEC-27001-Lead-Implementer Examengine - ISO-IEC-27001-Lead-Implementer Deutsch Prüfung

Wollen Sie an PECB ISO-IEC-27001-Lead-Implementer Zertifizierungsprüfung teilnehmen? Sorgen Sie sich um diese Prüfung? Wünschen Sie sich an der ISO-IEC-27001-Lead-Implementer Prüfung melden aber Fürchten Sie Misserfolg an dieser Prüfung? Das macht nichts, melden Sie getrost an. Wenn Sie ITZert Prüfungsunterlagen benutzen, sind keine Probleme in Ihrer Prüfung vorhanden. Obwohl Sie keine Zuversicht dieser Prüfung haben, können Sie einmal diese Prüfung bestehen, wenn Sie ISO-IEC-27001-Lead-Implementer Dumps von ITZert benutzen. Glauben Sie nicht? Kommen Sie bitte zu ITZert und Informieren Sie sich. Außerdem können Sie einen Teil der PECB ISO-IEC-27001-Lead-Implementer Dumps probieren. Damit können Sie finden, dass

die Prüfungsunterlagen die Garantie für den Erfolg der PECB ISO-IEC-27001-Lead-Implementer Prüfung sind.

## PECB Certified ISO/IEC 27001 Lead Implementer Exam ISO-IEC-27001-Lead-Implementer Prüfungsfragen mit Lösungen (Q343-Q348):

**343. Frage**
Infralink is a medium-sized IT consultancy firm headquartered in Dublin, Ireland. It specializes in secure cloud infrastructure, software integration, and data analytics, serving a diverse client base in the healthcare, financial services, and legal sectors, including hospitals, insurance providers, and law firms. To safeguard sensitive client data and support business continuity, Infralink has implemented an information security management system (ISMS) aligned with the requirements of ISO/IEC 27001.
In developing its security architecture, the company adopted services to support centralized user identification and shared authentication mechanisms across its departments. These services also governed the creation and management of credentials within the company. Additionally, Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity across its systems.
In preparation for implementing information security controls, the company ensured the availability of necessary resources, personnel competence, and structured planning. It conducted a cost-benefit analysis, scheduled implementation phases, and prepared documentation and activity checklists for each phase. The intended outcomes were clearly defined to align security controls with business objectives.
Infralink started by implementing several controls from Annex A of ISO/IEC 27001. These included regulating physical and logical access to information and assets in accordance with business and information security requirements, managing the identity life cycle, and establishing procedures for providing, reviewing, modifying, and revoking access rights. However, controls related to the secure allocation and management of authentication information, as well as the establishment of rules or agreements for secure information transfer, have not yet been implemented. During the documentation process, the company ensured that all ISMS- related documents supported traceability by including titles, creation or update dates, author names, and unique reference numbers. Based on the scenario above, answer the following question.
Which security services did infralink implement as part of its security architecture?

- A. Integrity services
- B. Access control and cryptographic services
- C. Boundary control and audit monitoring services

**Antwort: B**

Begründung:
Based on the scenario, Infralink implemented access control and cryptographic services as part of its security architecture, making Option A the correct and fully verified answer.
The scenario explicitly describes the deployment of centralized user identification, shared authentication mechanisms, and credential creation and management. These characteristics align directly with access control services, whose purpose is to ensure that only authorized users, devices, and processes can access information and systems in accordance with business and security requirements. This is consistent with Annex A controls implemented by Infralink, including:
A).5.15 - Access control: regulating physical and logical access based on business and information security requirements A).5.16 - Identity management: managing the full identity life cycle A).5.18 - Access rights: provisioning, reviewing, modifying, and revoking access rights Additionally, the scenario states that Infralink deployed solutions to protect sensitive data in transit and at rest, maintaining confidentiality and integrity. This is a defining characteristic of cryptographic services, which use encryption and cryptographic mechanisms to protect information from unauthorized disclosure or modification. This aligns with:
A).8.24 - Use of cryptography, which requires cryptographic controls to protect information based on risk and classification The scenario also explicitly notes that controls related to authentication information (A.5.17) and information transfer rules or agreements (A.5.14) have not yet been implemented, confirming that the services in place are not boundary monitoring or audit-focused.
Therefore:
Option B (Boundary control and audit monitoring services) is incorrect, as no monitoring, logging, or boundary protection services are described.
Option C (Integrity services alone) is incomplete, as integrity protection is only one outcome of cryptographic services, not the full scope described.

**344. Frage**
We can acquire and supply information in various ways. The value of the information depends on whether it is reliable. What are the reliability aspects of information?

- A. Availability, Integrity and Completeness

- B. Timeliness, Accuracy and Completeness
- C. Availability, Integrity and Confidentiality
- D. Availability, Information Value and Confidentiality

**Antwort: C**

**345. Frage**
ISO 27002 provides guidance in the following area

- A. Information handling recommendations
- B. Detailed lists of required policies and procedures
- C. Framework for an overall security andcompliance program
- D. PCI environment scoping

**Antwort: C**

**346. 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.
Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001' Refer to scenario 3.

- A. Yes, the control for the effective use of the cryptography can include cryptographic key management
- B. No, the control should be implemented only for defining rules for cryptographic key management
- C. No, because the standard provides a separate control for cryptographic key management

**Antwort: A**

Begründung:
According to ISO/IEC 27001:2022, Annex A.8.24, the control for the effective use of cryptography is intended to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This control can include cryptographic key management, which is the process of generating, distributing, storing, using, and destroying cryptographic keys in a secure manner. Cryptographic key management is essential for ensuring the security and functionality of cryptographic solutions, such as encryption, digital signatures, or authentication.
The standard provides the following guidance for implementing this control:
A policy on the use of cryptographic controls should be developed and implemented.
The policy should define the circumstances and conditions in which the different types of cryptographic controls should be used, based on the information classification scheme, the relevant agreements, legislation, and regulations, and the assessed risks.
The policy should also define the standards and techniques to be used for each type of cryptographic control, such as the algorithms, key lengths, key formats, and key lifecycles.
The policy should be reviewed and updated regularly to reflect the changes in the technology, the business environment, and the legal requirements.
The cryptographic keys should be managed through their whole lifecycle, from generation to destruction, in a secure and controlled manner, following the principles of need-to-know and segregation of duties.
The cryptographic keys should be protected from unauthorized access, disclosure, modification, loss, or theft, using appropriate physical and logical security measures, such as encryption, access control, backup, and audit.

The cryptographic keys should be changed or replaced periodically, or when there is a suspicion of compromise, following a defined process that ensures the continuity of the cryptographic services and the availability of the information.
The cryptographic keys should be securely destroyed when they are no longer required, or when they reach their end of life, using methods that prevent their recovery or reconstruction.
Reference:
ISO/IEC 27001:2022 Lead Implementer Course Guide1
ISO/IEC 27001:2022 Lead Implementer Info Kit2
ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 Understanding Cryptographic Controls in Information Security5

**347. 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
[