

# Real ISO-IEC-27001-Lead-Implementer Exam Dumps, ISO-IEC-27001-Lead-Implementer Exam prep, Valid ISO-IEC-27001-Lead-Implementer Braindumps



BONUS!!! Download part of TorrentVCE ISO-IEC-27001-Lead-Implementer dumps for free: [https://drive.google.com/open?id=1XwzB0d503YcVOunBAvOCB8OkQv\\_ydpG7](https://drive.google.com/open?id=1XwzB0d503YcVOunBAvOCB8OkQv_ydpG7)

Our experts are constantly looking for creative way to immortalize our ISO-IEC-27001-Lead-Implementer actual exam in this line. Their masterpieces are instrumental to offer help and improve your performance in the real exam. Being dedicated to these practice materials painstakingly and pooling useful points into our ISO-IEC-27001-Lead-Implementer Exam Materials with perfect arrangement and scientific compilation of messages, our ISO-IEC-27001-Lead-Implementer practice materials can propel the exam candidates to practice with efficiency.

PECB ISO-IEC-27001-Lead-Implementer Certification is a globally recognized certification that validates the knowledge and skills of individuals in the implementation of information security management systems (ISMS) according to ISO/IEC 27001. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification is issued by the Professional Evaluation and Certification Board (PECB), which is a leading certification body in the field of information security and management systems.

Earning the PECB Certified ISO/IEC 27001 Lead Implementer certification demonstrates a professional's commitment to information security and their ability to implement and manage an ISMS based on the ISO/IEC 27001 standard. It is a globally recognized certification that can help professionals advance their careers and increase their earning potential. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification also demonstrates an organization's commitment to information security and can help build trust with customers and stakeholders.

>> ISO-IEC-27001-Lead-Implementer Pass Guaranteed <<

## Latest ISO-IEC-27001-Lead-Implementer Study Materials - ISO-IEC-27001-Lead-Implementer Reliable Study Guide

If you are preparing the exam, you will save a lot of troubles with the guidance of our ISO-IEC-27001-Lead-Implementer training engine. Our company is aimed at relieving your pressure from heavy study load. So we strongly advise you to have a try on our ISO-IEC-27001-Lead-Implementer Study Guide. If you want to know them before your purchase, you can free download the demos of our ISO-IEC-27001-Lead-Implementer exam braindumps on the website, which are the small part of the learning questions.

## PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q230-Q235):

### NEW QUESTION # 230

FinanceX, a well-known financial institution, uses an online banking platform that enables clients to easily and securely access their bank accounts. To log in, clients are required to enter the one-time authorization code sent to their smartphone. What can be concluded from this scenario?

- A. FinanceX has incorrectly implemented a security control that could become a vulnerability
- **B. FinanceX has implemented a security control that ensures the confidentiality of information**
- C. FinanceX has implemented an integrity control that avoids the involuntary corruption of data

**Answer: B**

Explanation:

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. A security control is a measure that is put in place to protect the confidentiality, integrity, and availability of information assets. In this scenario, FinanceX has implemented a security control that ensures the confidentiality of information by requiring clients to enter a one-time authorization code sent to their smartphone when they log in to their online banking platform. This control prevents unauthorized access to the clients' bank accounts and protects their sensitive information from being disclosed to third parties. The one-time authorization code is a form of two-factor authentication, which is a security technique that requires two pieces of evidence to verify the identity of a user. In this case, the two factors are something the user knows (their username and password) and something the user has (their smartphone). Two-factor authentication is a recommended security control for online banking platforms, as it provides a higher level of security than single-factor authentication, which relies only on one piece of evidence, such as a password.

**NEW QUESTION # 231**

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.

Based on scenario - 1. which methodology did AegisCure use to implement its ISMS?

- A. PMBOK
- B. ISO 10006
- **C. IMS2**

**Answer: C**

Explanation:

The correct and verified answer is Option A - IMS2, which is the methodology specifically designed to support the implementation of ISO/IEC management system standards, including ISO/IEC 27001.

IMS2 (Integrated Management System methodology) is structured to align directly with Annex SL, the harmonized high-level structure used by ISO/IEC 27001:2022. It emphasizes:

- \* Understanding organizational context
- \* Planning based on risks and objectives
- \* Resource and competence management
- \* Phased implementation
- \* Documented information and traceability
- \* Continual improvement

Scenario 3 clearly reflects these elements: Infralink conducted planning, cost-benefit analysis, phased implementation, documentation with traceability, and alignment with business objectives-all hallmarks of the IMS2 methodology.

The other options are not appropriate:

\* PMBOK is a generic project management framework and does not specifically address ISMS or ISO Annex SL requirements.

\* ISO 10006 provides guidance on quality management in projects, not ISMS implementation.

ISO/IEC 27001:2022 requires a systematic, standards-aligned methodology for implementation, which IMS2 is designed to provide.

### NEW QUESTION # 232

Scenario 2: NyvMarketing is a marketing firm that provides different services to clients across various industries. With expertise in digital marketing, branding, and market research, NyvMarketing has built a solid reputation for delivering innovative and impactful marketing campaigns. With the growing Significance Of data Security and information protection within the marketing landscape, the company decided to implement an ISMS based on 27001.

While implementing its ISMS NyvMarketing encountered a significant challenge; the threat of insufficient resources. This challenge posed a risk to effectively executing its ISMS objectives and could potentially undermine the company's efforts to safeguard Sensitive information. To address this threat, NyvMarketing adopted a proactive approach by appointing Michael to manage the risks related to resource Constraints.

Michael was pivotal in identifying and addressing resource gaps, strategizing risk mitigation, and allocating resources effectively for ISMS implementation at NyvMarketing, strengthening the company's resilience against resource challenges.

Furthermore, NyvMarketing prioritized industry standards and best practices in information security, diligently following ISO/IEC 27002 guidelines. This commitment, driven by excellence and ISO/IEC 27001 requirements, underscored NyvMarketing's dedication to upholding the highest Standards Of information security governance.

While working on the ISMS implementation, NyvMarketing opted to exclude one Of the requirements related to competence (as stipulated in ISO/IEC 27001, Clause 7.2). The company believed that its existing workforce possessed the necessary competence to fulfill ISMS-related tasks. However, it did not provide a valid justification for this omission. Moreover, when specific controls from Annex A Of ISO/IEC 27001 were not implemented, NyvMarketing neglected to provide an acceptable justification for these exclusions.

During the ISMS implementation, NyvMarketing thoroughly assessed vulnerabilities that could affect its information Security. These vulnerabilities included insufficient maintenance and faulty installation Of storage media, insufficient periodic replacement schemes for equipment, Inadequate software testing, and unprotected communication lines. Recognizing that these vulnerabilities could pose risks to its data security, NyvMarketing took steps to address these specific weaknesses by implementing the necessary controls and countermeasures. Based on the scenario above, answer the following question.

In the scenario 2, NyvMarketing faced the threat of insufficient resources during the ISMS implementation. In which of the following categories does this threat fall?

According to scenario 2, what is Michael's role at NyvMarketing?

- A. ISMS auditor
- B. Risk owner
- C. Crisis manager
- D. Incident manager

### Answer: B

Explanation:

A risk owner is defined in ISO/IEC 27001:2022 as the person or entity with the accountability and authority to manage a risk. In the scenario, Michael was appointed to manage the risks related to resource constraints- identifying gaps, strategizing mitigation, and allocating resources-demonstrating that he is assigned responsibility and authority for a specific risk area.

"Risk owner: person or entity with the accountability and authority to manage a risk."

- ISO/IEC 27000:2018, 3.32 (referenced by ISO/IEC 27001:2022, Section 3)

"The organization shall assign risk owners to ensure that risks are managed."

- ISO/IEC 27001:2022, Clause 6.1.2

### NEW QUESTION # 233

According to ISO/IEC 27001 controls, why should the use of privileged utility programs be restricted and tightly controlled?

- A. To enable the correlation and analysis of security-related events
- B. To prevent misuse of utility programs that could override system and application controls
- C. To ensure that utility programs are compatible with existing system software

### Answer: B

## NEW QUESTION # 234

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on ISO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly. Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.

Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever. Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management. Based on the scenario above, answer the following question:

What caused SunDee's workforce disruption?

- A. The voluminous written reports
- B. The inconsistency of reports written by different employees
- C. The negligence of performance evaluation and monitoring and measurement procedures

### Answer: C

Explanation:

According to ISO/IEC 27001:2013, clause 9.1, an organization must monitor, measure, analyze and evaluate its information security performance and effectiveness. This includes determining what needs to be monitored and measured, the methods for doing so, when and by whom the monitoring and measurement shall be performed, when the results shall be analyzed and evaluated, and who shall be responsible for ensuring that the actions arising from the analysis and evaluation are taken 1.

SunDee failed to comply with this requirement and did not monitor or measure the performance and effectiveness of its ISMS for the past two years. As a result, the company did not have any objective evidence or indicators to demonstrate the achievement of its information security objectives, the effectiveness of its controls, the satisfaction of its interested parties, or the identification and treatment of its risks. This also meant that the company did not conduct regular management reviews of its ISMS, as required by clause 9.3, which would provide an opportunity for the top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS, and to decide on any changes or improvements needed 1.

Just before the recertification audit, the company decided to conduct an internal audit, as required by clause 9.2, which is a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled 1. However, the company did not have a well-defined audit program, scope, criteria, or methodology, and relied on the written reports of its staff for the past two years. This caused a disruption in the workforce, as most of the staff had to compile their reports for their departments, leaving the Production Department with less than the optimum workforce, which decreased the company's stock. Moreover, the internal audit process was very inconsistent, as the reports were written by different employees with different styles, formats, and levels of detail. The internal audit process also lacked any qualitative measures, such as performance indicators, metrics, or benchmarks, to evaluate the performance and effectiveness of the ISMS.

Therefore, the cause of SunDee's workforce disruption was the negligence of performance evaluation and monitoring and measurement procedures, which led to a lack of objective evidence, a poorly planned and executed internal audit, and a decrease in the company's productivity and stock value.

## NEW QUESTION # 235

.....

Everyone has different learning habits, ISO-IEC-27001-Lead-Implementer exam simulation provide you with different system versions: PDF version, Software version and APP version. Based on your specific situation, you can choose the version that is most suitable for you, or use multiple versions at the same time. After all, each version of ISO-IEC-27001-Lead-Implementer Preparation questions have its own advantages. If you are very busy, you can only use some of the very fragmented time to use our ISO-IEC-27001-Lead-Implementer study materials. And each of our ISO-IEC-27001-Lead-Implementer exam questions can help you pass the exam for sure.

**Latest ISO-IEC-27001-Lead-Implementer Study Materials:** <https://www.torrentvce.com/ISO-IEC-27001-Lead-Implementer-valid-vce-collection.html>

- ISO-IEC-27001-Lead-Implementer Valid Exam Forum  ISO-IEC-27001-Lead-Implementer Free Vce Dumps   
ISO-IEC-27001-Lead-Implementer Free Vce Dumps  Simply search for ➡ ISO-IEC-27001-Lead-Implementer

for free download on ▷ [www.troyecdumps.com](http://www.troyecdumps.com) ◁ ☐ New ISO-IEC-27001-Lead-Implementer Exam Price

P.S. Free & New ISO-IEC-27001-Lead-Implementer dumps are available on Google Drive shared by TorrentVCE.

[https://drive.google.com/open?id=1XwzBOd503YcVOunBAvOCB8OkQv\\_ydpG7](https://drive.google.com/open?id=1XwzBOd503YcVOunBAvOCB8OkQv_ydpG7)