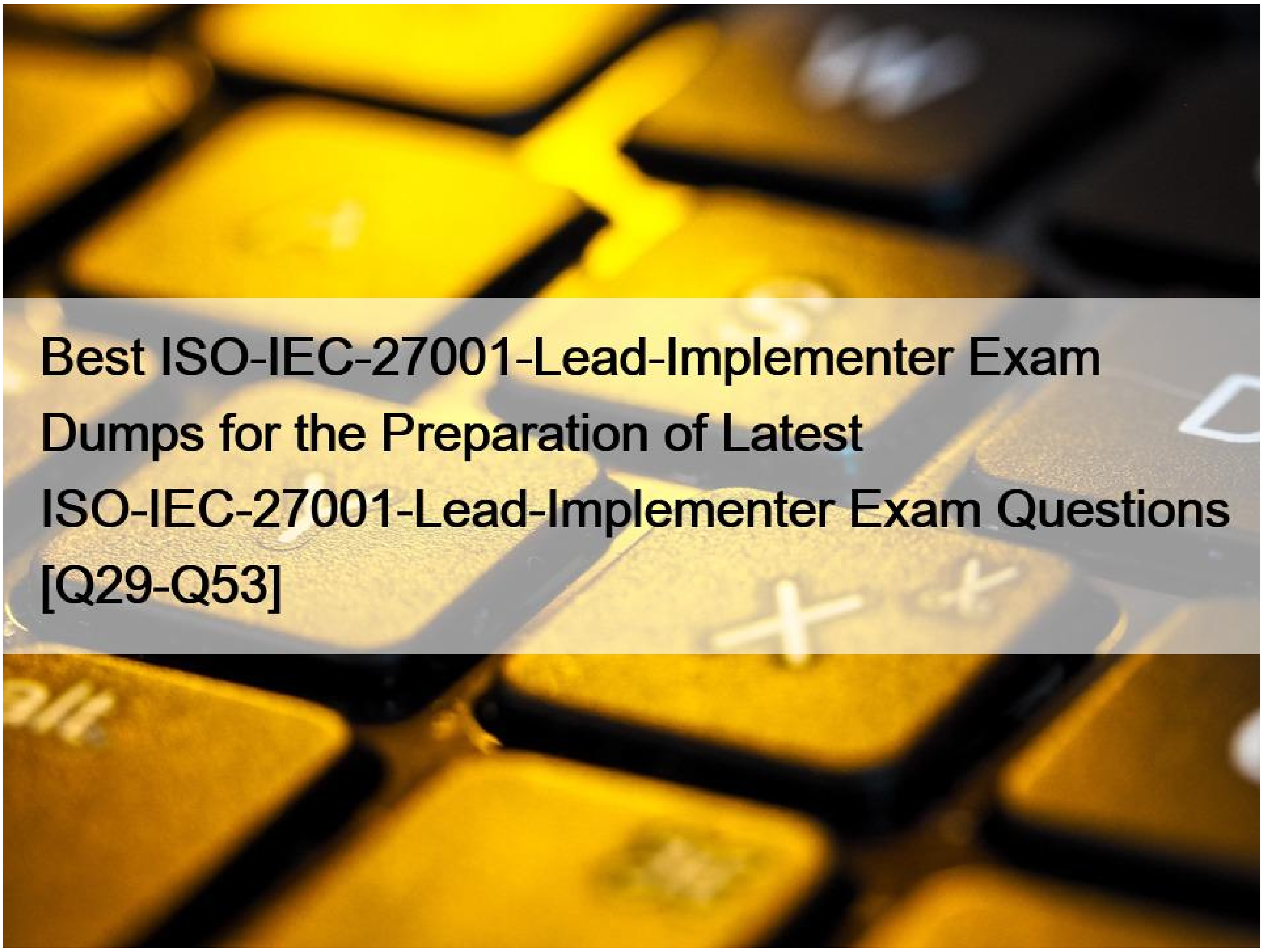
Best ISO-IEC-27001-Lead-Implementer Exam Dumps for the Preparation of Latest ISO-IEC-27001-Lead-Implementer Exam Questions [Q29-Q53



Best ISO-IEC-27001-Lead-Implementer Exam Dumps for the Preparation of Latest ISO-IEC-27001-Lead-Implementer Exam Questions
Download Latest & Valid Questions For PECB ISO-IEC-27001-Lead-Implementer exam

QUESTION 29

An organization wants to enable the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. Which control should it implement7
* Use of privileged utility programs
* Clock synchronization
* Installation of software on operational systems

QUESTION 30

What do employees need to know to report a security incident?
* How to report an incident and to whom.
* Whether the incident has occurred before and what was the resulting damage.
* The measures that should have been taken to prevent the incident in the first place.
* Who is responsible for the incident and whether it was intentional.

QUESTION 31

Midwest Insurance grades the monthly report of all claimed losses per insured as confidential. What is accomplished if all other reports from this insurance office are also assigned the appropriate grading?
* The costs for automating are easier to charge to the responsible departments.
* A determination can be made as to which report should be printed firstand which ones can wait a little longer.
* Everyone can easily see how sensitive the reports&#8217; contents are by consulting the grading label.
* Reports can be developed more easily and with fewer errors.

QUESTION 32

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?
* ISO/IEC 27001:2005
* Intellectual Property Rights
* ISO/IEC 27002:2005
* Personal data protection legislation

QUESTION 33

Select the controls that correspond to thedomain &#8220;9. ACCESS CONTROL&#8221; of ISO / 27002 (Choose three)
* Restriction of access to information
* Return of assets
* Management of access rights with special privileges
* Withdrawal or adaptation of access rights

QUESTION 34

Based on scenario 10. NetworkFuse did not conduct a self-evaluation of the ISMS before the audit. Is this compliant to ISO/IEC 27001?
* No, the auditee must review the requirements of clauses 4 to 10 before the conduct of a certification audit
* Yes, the standard indicates that the auditee shall rely only on internal audit and management review reports to prepare for the certification audit
* Yes, the standard does not require to conduct a self-evaluation before the audit but it is a good practice to follow

QUESTION 35

An organization documented each security control that it Implemented by describing their functions in detail.

Is this compliant with ISO/IEC 27001?
* No, the standard requires to document only the operation of processes and controls, so no description of each security control is needed
* No, because the documented information should have a strict format, including the date, version number and author identification
* Yes, but documenting each security control and not the process in general will make it difficult to review the documented information

QUESTION 36

Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001&#8242; Refer to scenario 3.
* No, the control should be implemented only for defining rules for cryptographic key management
* Yes, the control for the effective use of the cryptography can include cryptographic key management
* No, because the standard provides a separate control for cryptographic key management

QUESTION 37

Companies use 27002 for compliance for which of the following reasons:
* A structured program that helps with security and compliance
* Explicit requirements for all regulations
* Compliance with ISO 27002 is sufficient to comply with all regulations

QUESTION 38

Who is accountable to classify information assets?
* the CEO
* the CISO
* the Information Security Team
* theasset owner

QUESTION 39

Based on scenario 9, OpenTech has taken all the actions needed, except____________.
* Corrective actions
* Preventive actions
* Permanent corrections

QUESTION 40

What should TradeB do in order to deal with residual risks? Refer to scenario 4.
* TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment
* TradeB should immediately implement new controls to treat all residual risks
* TradeB should accept the residual risks only above the acceptance level

QUESTION 41

Which tool is used to identify, analyze, and manage interested parties?
* The probability/impact matrix
* The power/interest matrix
* The likelihood/severity matrix

QUESTION 42

What should an organization allocate to ensure the maintenance and improvement of the information security management system?
* The appropriate transfer to operations
* Sufficient resources, such as the budget, qualified personnel, and required tools

* The documented information required by ISO/IEC 27001

QUESTION 43

Which of the following measures is a correctivemeasure?

* Incorporating an Intrusion Detection System (IDS) in the design of a computer center
* Installing a virus scanner in an information system
* Making a backup of the data that has been created or altered that day
* Restoring a backup of the correct database after a corrupt copy of the database was written over the original

QUESTION 44

A non-human threat for computer systems is a flood. In which situation is a flood always a relevant threat?

* If the riskanalysis has not been carried out.
* When computer systems are kept in a cellar below ground level.
* When the computer systems are not insured.
* When the organization is located near a river.

QUESTION 45

According to scenario 10, NetworkFuse requested from the certification body to review all the documentation only on-site. Is this acceptable?

* Yes, the auditee may request that the review of the documentation takes place on-site
* Yes, only if a confidentiality agreement is formerly signed by the audit team
* No, the certification body decides whether the documentation review takes place on-site or off-site

QUESTION 46

Based on scenario 5. after migrating to cloud. Operaze&#8217;s IT team changed the ISMS scope and implemented all the required modifications Is this acceptable?

* Yes, because the ISMS scope should be changed when there are changes to the external environment
* No, because the company has already defined the ISMS scope
* No, because any change in ISMS scope should be accepted by the management

QUESTION 47

Based on scenario 6. Lisa found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. What does this indicate?

* Lisa did not take actions to acquire the necessary competence
* The effectiveness of the training and awareness session was not evaluated
* Skyver did not determine differing team needs in accordance to the activities they perform and the intended results

QUESTION 48

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&#8217;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&#8217;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&#8217;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 the scenario above, answer the following question:

What led Operaze to implement the ISMS?
* Identification of vulnerabilities
* Identification of threats
* Identification of assets

QUESTION 49

&#8216;The ISMS covers all departments within Company XYZ that have access to customers&#8217; data. The purpose of the ISMS is to ensure the confidentiality, integrity, and availability of customers&#8217; data, and ensure compliance with the applicable regulatory requirements regarding information security.&#8221; What does this statement

&#8221;describe?
* The information systems boundary of the ISMS scope
* The organizational boundaries of the ISMS scope
* The physical boundary of the ISMS scope

QUESTION 50

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 SO/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&#8217;s stock.

Tessa was SunDee&#8217;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&#8217;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&#8217;s workforce disruption?
* The negligence of performance evaluation and monitoring and measurement procedures
* The inconsistency of reports written by different employees
* The voluminous written reports

QUESTION 51

What is the next step that Operaze&#8217;s ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.
* Implement the information security policy
* Obtain top management&#8217;s approval for the information security policy
* Communicate the information security policy to all employees

QUESTION 52

According to scenario 7, a demilitarized zone (DMZ) is deployed within InfoSec&#8217;s network. What type of control has InfoSec implemented in this case?
* Detective
* Preventive
* Corrective

QUESTION 53

You are the owner of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks. What is this risk strategy called?
* Risk bearing
* Risk avoiding
* Risk neutral
* Risk passing

Exam Materials for You to Prepare & Pass ISO-IEC-27001-Lead-Implementer Exam:
https://www.validexam.com/ISO-IEC-27001-Lead-Implementer-latest-dumps.html]