PassQueen
a.k.a dumpsqueen.com

Beingcert ISO/IEC 20000 Lead Implementer Exam

ISO ISOIEC20000LI

Version Demo

Total Demo Questions: 10

Total Premium Questions: 104

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Fundamental principles and concepts of a Service Management System (SMS)	21
Topic 2, Service Management System (SMS)	2
Topic 3, Planning of an SMS based on ISO/IEC 20000	6
Topic 4, Implementation of an SMS based on ISO/IEC 20000	28
Topic 5, Performance evaluation, monitoring and measurement of an SMS based on ISO/IEC 20000	13
Topic 6, Continual improvement of an SMS based on ISO/IEC 20000	5
Topic 7, Preparing for an SMS certification audit	8
Topic 8, Mix Questions	21
Total	104

QUESTION NO: 1

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

According to scenario 2. Beauty has reviewed all user access rights. What type of control is this?

A. Detective and administrative

B. Corrective and managerial

C. Legal and technical

D. Preventive and administrative

ANSWER: D

Explanation:

Reviewing user access rights so that sensitive files are available only to authorized personnel is a preventive and administrative control. It is preventive because the review occurs to reduce the likelihood of unauthorized access before an information-security incident occurs. By checking that access remains appropriate to each person’s role, responsibilities, and business need, Beauty can remove excessive, obsolete, or inappropriate permissions and thereby protect the confidentiality of customer information.

It is administrative because the activity is governed by management-defined rules and operating procedures for access authorization, review, approval, and removal. Although access permissions are ultimately enforced by technical systems, the stated activity is the organizational process of reviewing who should retain access, rather than a technical mechanism such as authentication software or anti-malware. The scenario’s objective—ensuring that only authorized personnel can access sensitive files—directly reflects access-control governance and least-privilege practice.

ISO/IEC 27002 includes requirements and guidance for managing access rights and reviewing access to ensure it remains appropriate. ISO/IEC 27001 also requires organizations to select and operate controls based on information-security risks. See the ISO/IEC 27002:2022 standard page and NIST’s SP 800-53 access-control guidance.

QUESTION NO: 2

Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.

Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and

selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:

A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department

The approved action plan was implemented and all actions described in the plan were documented.

Based on scenario 9, OpenTech has taken all the actions needed, except_____.

A. Corrective actions

B. Preventive actions

C. Permanent corrections

D. Reviewing the effectiveness of the corrective action taken

ANSWER: D

Explanation:

Reviewing the effectiveness of the corrective action taken is the missing required activity. The scenario shows that OpenTech identified the nonconformity, investigated its root cause, selected actions intended to prevent recurrence, obtained management approval, implemented the plan, and retained documentation. Those steps establish and carry out a corrective action, but implementation alone does not demonstrate that the action actually resolved the underlying problem or will prevent its recurrence.

Under ISO management-system corrective-action requirements, an organization must review the effectiveness of action taken after implementing corrective action. For this case, OpenTech should define and obtain objective evidence that the revised access-control policy and new network restrictions work in practice. Suitable evidence could include follow-up checks that unique user IDs are assigned, access authorizations comply with the revised policy, monitoring is operating as intended, and no further instances of reused IDs occur. The organization should retain documented information on both the corrective action and the result of its effectiveness review. This final verification closes the nonconformity process based on evidence rather than assuming success merely because the plan was completed. See the ISO overview of ISO/IEC 27001 and the ISO overview of ISO/IEC 20000-1.

QUESTION NO: 3

What risk treatment option has Company A implemented if it has required from its employees the change of email passwords at least once every 60 days?

A. Risk modification

B. Risk avoidance

C. Risk retention

ANSWER: A

Explanation:

Risk modification is correct because Company A has introduced a security control—mandatory periodic email-password changes—to alter the level of information-security risk. In ISO/IEC 27001 risk treatment, modifying risk means selecting and implementing controls intended to reduce the likelihood of an unwanted event, its consequences, or both. A password-management requirement is an administrative and technical access-control measure aimed at limiting the period during which a compromised, guessed, or improperly retained credential can be used. It therefore represents an active treatment action within the organization's risk treatment plan rather than merely documenting a risk decision.

The precise password policy should be based on Company A's risk assessment, applicable legal and contractual requirements, the sensitivity of the email environment, and complementary controls such as multifactor authentication, monitoring, and secure password storage. Modern guidance also emphasizes that forced periodic password changes should be applied where there is evidence of compromise or a defined risk rationale, rather than automatically in every context. That

consideration affects the suitability and effectiveness of the selected control, but not its classification: where the organization implements it to reduce email-account compromise risk, it is risk modification. ISO describes ISO/IEC 27001's risk-based ISMS approach at ISO/IEC 27001; password-management considerations are discussed in NIST SP 800-63B.

QUESTION NO: 4

Which approach should organizations use to implement an ISMS based on ISO/IEC 27001?

A. An approach that is suitable for organization's scope

B. Any approach that enables the ISMS implementation within the 12month period

C. Only the approach provided by the standard

ANSWER: A

Explanation:

An approach that is suitable for organization's scope is correct because ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system, rather than mandating one fixed implementation methodology. The organization must determine the ISMS scope in light of its context, including internal and external issues, relevant interested-party requirements, interfaces and dependencies, and the activities, locations, and assets to be covered. The chosen implementation approach should therefore be proportionate to that defined scope and enable the organization to meet all applicable ISMS requirements and intended information-security outcomes. In practice, this permits an organization to phase work, use an existing management-system framework, or adopt a project method that fits its size, complexity, risk profile, resources, and business environment. What matters is that the resulting ISMS conforms to ISO/IEC 27001 requirements and is effective in managing information-security risks within the stated scope. ISO describes ISO/IEC 27001 as the standard defining ISMS requirements and emphasizes that it is applicable to organizations of all types and sizes. See ISO/IEC 27001:2022 on ISO.org and ISO's overview of ISO/IEC 27001.

QUESTION NO: 5

A service provider has identified that loss of its primary data centre would interrupt a customer-facing service. The customer agreement requires the service to be restored within eight hours. The provider has a technical backup solution, but the continuity documentation does not identify the people authorized to invoke recovery, the order in which service components are restored, or how customers will be informed.

What is the main weakness in the provider's service continuity arrangements?

A. The arrangements lack defined recovery responsibilities, restoration priorities, and communication procedures

B. The arrangements should remove the eight-hour recovery requirement from the customer agreement

C. The arrangements should retain only technical backup records because continuity decisions are made during an incident

ANSWER: A

Explanation:

The continuity arrangements do not provide a complete, coordinated capability to meet the agreed continuity requirements. A technical backup solution is only one element of service continuity management. The provider also needs defined responsibilities, invocation criteria, recovery procedures and priorities, communication arrangements, and validation that the arrangements can achieve the required recovery outcome.

Changing the recovery target without customer agreement would not address the weakness. Similarly, documenting only the backup technology would not establish who makes decisions, how service restoration is coordinated, or how relevant interested parties are kept informed during a disruption.

QUESTION NO: 6

Which tool is used to identify, analyze, and manage interested parties?

A. The probability/impact matrix

B. The power/interest matrix

C. The likelihood/severity matrix

ANSWER: B

Explanation:

The power/interest matrix is correct because it is a practical stakeholder-analysis tool for identifying relevant interested parties and deciding how the organization should engage with them. The matrix maps each party according to two meaningful factors: its ability to influence the service management system or its outcomes (power), and its degree of concern with or attention to those outcomes (interest). This gives the organization a clear, proportionate basis for determining who requires close management, active communication, monitoring, or routine information.

For an ISO/IEC 20000-1 service management system, understanding interested parties is part of understanding the organization and its context. The organization must determine relevant interested parties and their requirements that are relevant to the service management system. Using a power/interest matrix helps turn that requirement into documented, usable management information: it supports prioritization of stakeholder needs, assignment of communication approaches, and ongoing review when stakeholder influence or expectations change. ISO standards do not mandate one specific diagram, but this matrix is widely accepted as an effective method for implementing stakeholder analysis in a structured and risk-aware way. See the ISO/IEC 20000-1:2018 standard overview and ISO's management system standards guidance.

QUESTION NO: 7

Why should the security testing processes be defined and implemented in the development life cycle?

A. To protect the production environment and data from compromise by development and test activities

B. To validate if information security requirements are met when applications are deployed to the production environment

C. To Identify organizational assets and define appropriate protection responsibilities

ANSWER: B

Explanation:

Security testing processes should be defined and implemented throughout the development life cycle to validate that information security requirements are satisfied before an application is deployed into the production environment. Integrating testing into development and transition activities provides evidence that required security controls have been designed, built, configured, and verified as part of the service being released. This makes security a planned quality characteristic of the service rather than an issue discovered only after deployment.

For an ISO/IEC 20000 service management system, this supports controlled service design, build, transition, and deployment. Testing should be appropriate to the service and its risks, and can include checking authentication and authorization controls, secure configuration, vulnerability remediation, protection of data, and conformity with defined security requirements. The resulting test evidence supports an informed release and deployment decision, helping ensure the production service meets the organization's agreed requirements. ISO describes ISO/IEC 20000-1 as specifying requirements for establishing, implementing, maintaining, and continually improving a service management system: ISO/IEC 20000-1:2018. Guidance on integrating security activities across the software development life cycle is also provided by NIST SP 800-218, Secure Software Development Framework.

QUESTION NO: 8

Why is the power/interest matrix used for?

A. Define the information security and physical boundaries

B. identify business requirements

C. Determine and manage interested parties

ANSWER: C

Explanation:

The power/interest matrix is used to determine and manage interested parties. It is a stakeholder-analysis tool that maps parties according to the level of power or influence they have over an initiative and the degree of interest they have in its outcomes. This allows the organization to choose an appropriate engagement approach: parties with high power and high interest generally require close management, while those with high power but less day-to-day interest should be kept satisfied. Interested parties with lower power may instead require proportionate monitoring and communication.

In an ISO/IEC 20000 service management system implementation, understanding relevant interested parties supports the organization's context and planning activities. Their needs and expectations can affect service-management objectives, service requirements, governance, risks, communications, and the ongoing suitability of the management system. The matrix is therefore a practical way to prioritize stakeholder engagement rather than merely listing stakeholders. ISO guidance on understanding the organization and its interested parties is available through the ISO 9001 online browsing platform, and stakeholder mapping methods are summarized by the Association for Project Management.

QUESTION NO: 9

Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management [^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.

First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity

Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted

Based on scenario 4, what type of assets were identified during risk assessment?

A. Supporting assets

B. Primary assets

C. Business assets

ANSWER: A

Explanation:

Supporting assets is correct because the scenario expressly identifies hardware, software, and networks during the risk assessment. These are resources that enable information processing and support the delivery of TradeB's banking services. In information-security risk management, they are therefore supporting assets: they provide the technological capability on which the organization's valuable information and business processes depend. For example, a hardware failure can interrupt a banking system, and a network or software weakness can affect the confidentiality, integrity, or availability of information handled by that system.

ISO/IEC 27001 requires the organization to establish and apply an information-security risk assessment process that identifies risks associated with loss of confidentiality, integrity, and availability of information within the ISMS scope. Identifying the resources involved—including IT infrastructure—is an important practical input to that process, since threats and vulnerabilities can be associated with those resources and their use. The scenario's focus on administrator-rights misuse and hardware-related interruptions also confirms that the assessment considered infrastructure that supports the bank's operations. ISO's overview of ISO/IEC 27001 describes the standard as a framework for managing information-security risks, while ISO's page for ISO/IEC 27005 identifies guidance for managing information-security risks.

QUESTION NO: 10

A university's learning platform performs well during most of the year. At the start of each academic term, however, thousands of students register simultaneously and the platform becomes unavailable. The organization has sufficient technical staff to resolve incidents quickly, but the same disruption occurs every term.

Which action is most likely to address the recurring service issue?

A. Increase the number of service desk analysts during registration periods

B. Forecast peak demand and plan, test, and provide sufficient service capacity before registration begins

C. Close registration when the first performance incident is reported

ANSWER: B

Explanation:

The organization should use capacity management to assess forecast demand, current capacity, and the resources required for the expected registration peak. The repeated and predictable nature of the disruption indicates that the service has not been planned to meet anticipated demand. Increasing incident-response staffing may shorten recovery time but does not ensure that the service can perform at the required level when demand occurs.

Capacity planning can include analysing registration patterns, performing load testing, defining capacity thresholds, and arranging appropriate application, database, network, or supplier capacity before the academic term begins. These actions should be coordinated with service-level requirements and financial or supplier decisions where relevant.