PassQueen
a.k.a dumpsqueen.com

ISO / IEC 27002 - Lead Implementer

GAQM ISO-IEC-LI

Version Demo

Total Demo Questions: 7

Total Premium Questions: 76

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Select the measures that help ensure the security of network services. (Choose three)

A. Defining security features and service levels for network services

B. Monitoring network services for security and performance issues

C. Segregating networks according to business and security requirements

D. Using one unrestricted network for all users, systems and external services

E. Disabling network-event monitoring to reduce the volume of records

ANSWER: A B C

Explanation:

Network-service security is supported by defining security features and service levels, monitoring network services, and separating networks where appropriate. Security requirements for networks should address such matters as access restrictions, authentication, encryption, availability, logging, resilience and responsibilities for operation and support.

Segmentation can limit the effect of a compromise by restricting communication between network zones, while monitoring helps identify service degradation and suspicious activity. ISO/IEC 27002 includes controls for network security, security of network services and segregation of networks. See ISO/IEC 27002:2022.

QUESTION NO: 2

Susan sends an email to Paul. Who determines the meaning and the value of information in this email?

A. Paul, the recipient of the information.

B. Paul and Susan, the sender and the recipient of the information.

C. Susan, the sender of the information.

ANSWER: A

Explanation:

Paul, the recipient of the information, determines its meaning and value because information acquires practical significance when it is interpreted in the recipient's context. Susan may select the content, wording, and intended message, but Paul assesses what the message means in relation to his responsibilities, prior knowledge, current circumstances, and the decision or action it may support. The same email can therefore have high value to Paul—for example, if it enables an important business decision—while having little or no value to another person. This distinction is relevant to information security because the protection required for information should reflect its value, sensitivity, and importance to the organization and to those using it. ISO/IEC 27002 provides guidance for establishing information-security controls in accordance with organizational risks and protection needs, rather than treating all information identically. See the ISO/IEC 27002:2022 overview and NIST's definition of information for related information-security terminology and context.

QUESTION NO: 3

What does the Information Security Policy describe?

A. how the InfoSec-objectives will be reached

B. which InfoSec-controls have been selected and taken

C. what the implementation-planning of the information security management system is

D. which Information Security-procedures are selected

E. a framework for setting information-security objectives

ANSWER: E

Explanation:

The information security policy establishes the organization's overall direction and intentions for information security. Under ISO/IEC 27001 clause 5.2, it must be appropriate to the organization's purpose, support its strategic direction, provide a framework for setting information-security objectives, and include commitments to satisfy applicable requirements and to continually improve the information security management system. Therefore, the correct statement is that the policy provides a framework for setting information-security objectives. The policy is a high-level management document: it communicates leadership's commitments and gives a consistent basis on which measurable objectives can subsequently be set, reviewed, and aligned with business needs and risk treatment. The detailed activities, resources, responsibilities, timescales, and evaluation methods for achieving individual objectives are determined when planning those objectives, rather than being the defining content of the policy itself. This distinction helps ensure that the policy remains stable and strategic while objective plans can be adjusted as risks, priorities, technology, and organizational conditions change. ISO's overview of ISO/IEC 27001 is available at https://www.iso.org/standard/27001, and ISO's description of information-security management systems is available at https://www.iso.org/isoiec-27001-information-security.html.

QUESTION NO: 4

Select the activities that should be performed when an information-security incident is identified. (Choose three)

A. Assessing and classifying the incident

B. Containing the incident where appropriate

C. Preserving relevant evidence

D. Deleting all logs immediately

E. Waiting for the next scheduled audit before taking action

ANSWER: A B C

Explanation:

The correct activities are assessing and classifying the incident, containing the incident where appropriate, and preserving relevant evidence. Once an event is identified as a possible information-security incident, the organization needs to determine its nature, scope, affected assets, severity, and potential business impact. This assessment supports prioritization and escalation according to defined incident-management procedures.

Containment aims to limit further damage, such as isolating a compromised device, disabling an exposed account, or blocking malicious network traffic. Evidence should be collected and protected in a manner that supports investigation, legal obligations, disciplinary processes, and lessons learned. Actions must be coordinated carefully so that containment does not unnecessarily destroy evidence or disrupt essential business operations. ISO/IEC 27002 addresses information-security incident management planning and preparation, assessment and decision, response, learning from incidents, and collection of evidence. See ISO/IEC 27002:2022 and ISO/IEC 27035-1.

QUESTION NO: 5

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?

A. Risk bearing

B. Risk avoidingÂ

C. Risk neutral

D. Risk passing

ANSWER: C

Explanation:

Risk neutral is the appropriate strategy because it applies proportionate treatment based on the significance of each identified risk. After analysing likelihood and impact, SpeeDelivery addresses risks whose potential consequences exceed its acceptable threshold, such as major disruption to deliveries, loss of customer data, or substantial financial loss. Lower-level risks are consciously tolerated where the anticipated impact does not justify the cost, effort, or operational disruption of additional controls. This is a practical, balanced approach: risk decisions are based on an evaluation of the risk level and the organization's defined acceptance criteria, rather than attempting to eliminate every possible risk. ISO/IEC 27005 describes risk treatment as a process in which organizations select and implement treatment options according to risk evaluation and acceptance decisions. NIST likewise explains that risk responses should be selected in relation to assessed risk and organizational risk tolerance. See ISO/IEC 27005:2022—Information security risk management and NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

QUESTION NO: 6

Select the activities that support effective information-security awareness, education and training. (Choose three)

A. Providing training that is relevant to personnel roles and responsibilities

B. Communicating how suspected security events can be reported

C. Repeating awareness activities at planned intervals

D. Providing security training only after a serious incident has occurred

E. Limiting awareness information to the information-security team

ANSWER: A B C

Explanation:

Awareness and training should be relevant to personnel roles, provided before access to information or systems is granted where appropriate, and repeated regularly to address changing threats and responsibilities. Personnel need practical knowledge of organizational policies, expected behavior, incident reporting channels and the security risks associated with their work.

ISO/IEC 27002 identifies information-security awareness, education and training as a people control. Training should be maintained and updated as roles, technologies, threats and organizational requirements change. See ISO/IEC 27002:2022.

QUESTION NO: 7

A development team needs to introduce an urgent change to a customer-facing application. What is the most important information-security requirement before the change is implemented in production?

A. The change should be assessed, authorized, tested and documented before implementation.

B. The change should be implemented immediately if the project manager requests it.

C. The change should be made only by the system administrator, without involving the business owner.

D. The change should be postponed until the next annual risk assessment.

ANSWER: A

Explanation:

The change should be assessed, authorized, tested and documented before implementation in production. Change management protects the confidentiality, integrity and availability of systems by ensuring that modifications are understood, approved by an appropriate authority, evaluated for security effects, and capable of being reversed if necessary. Urgency may justify an expedited process, but it does not remove the need for controlled authorization and subsequent review.

ISO/IEC 27002 includes configuration management and change-management guidance to ensure that changes to information-processing facilities and systems are controlled. See ISO/IEC 27002:2022.