PassQueen
a.k.a dumpsqueen.com

Information Security Foundation based on ISO/IEC 27002

Exin EX0-105

Version Demo

Total Demo Questions: 14

Total Premium Questions: 147

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Information security	18
Topic 2, Threats and risks	35
Topic 3, The approach	7
Topic 4, Organization	16
Topic 5, Measures	58
Topic 6, Legislation and regulations	13
Total	147

QUESTION NO: 1

Your organization has an office with space for twenty five (25) workstations. These workstations are all fully equipped and in use. Due to a

reorganization ten (10) extra workstations are added, five (5) of which are used for a call center 24 hours per day. Five (5) workstations must always be available.

What physical security measures must be taken in order to ensure this?

A. Obtain an extra office and set up ten (10) workstations. You would therefore have spare equipment that can be used to replace any non-functioning equipment.

B. Obtain an extra office and set up ten (10) workstations. Ensure that there are security personnel both in the evenings and at night, so that staff can work there safely and securely.

C. Obtain an extra office and connect all ten (10) new workstations to an emergency power supply and UPS (Uninterruptible Power Supply). Adjust the access control system to the working hours of the new staff. Inform the building security personnel that work will also be carried out in the evenings and at night.

D. Obtain an extra office and provide a UPS (Uninterruptible Power Supply) for the five most important workstations.

ANSWER: C

Explanation:

“Obtain an extra office and connect all ten (10) new workstations to an emergency power supply and UPS (Uninterruptible Power Supply). Adjust the access control system to the working hours of the new staff. Inform the building security personnel that work will also be carried out in the evenings and at night.” is correct because it addresses the complete physical-security and availability requirement created by the reorganization. An additional office provides the necessary secure accommodation for the ten added workstations. Emergency power and UPS protection reduce the risk that a mains-power disruption prevents the continuously operating call-centre service, and the five workstations that must remain available, from functioning. Availability is a core information-security objective and requires supporting facilities to be protected from power failures and similar physical threats.

The measure also recognizes that physical security must match actual operations. Access-control permissions need to support authorized evening and night work while retaining controlled entry to the new area. Notifying building security ensures that out-of-hours activity is expected, monitored, and can be supported through incident response or access procedures. This combination applies the ISO/IEC 27002 physical-controls principle of protecting premises, equipment, and supporting utilities in a way that is proportionate to operational needs. See the ISO/IEC 27002 standard overview and NIST’s guidance on physical and environmental protection controls.

QUESTION NO: 2

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A. ISO/IEC 27001:2005

B. Intellectual Property Rights

C. ISO/IEC 27002:2005

D. Personal data protection legislation

ANSWER: D

Explanation:

Personal data protection legislation is correct because it creates legally enforceable duties for organizations that collect, use, store, disclose, or otherwise process personal information. Such duties are imposed through legislation or regulations, rather than being voluntary technical guidance or a certification standard. Information security is directly relevant because personal-data laws normally require organizations to protect personal data against unauthorized access, accidental loss, alteration,

destruction, and unlawful disclosure. They also commonly require appropriate governance, accountability, incident handling, and safeguards proportionate to the risk.

For example, the EU General Data Protection Regulation requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This illustrates how data-protection law can impose mandatory security obligations on organizations within its scope, including organizations outside the EU when they offer goods or services to, or monitor, individuals in the EU. The relevant requirements are set out in Article 32 of the General Data Protection Regulation. The broader legal framework and individual rights protected by this legislation are also described by the European Commission's data-protection overview.

QUESTION NO: 3

Why is compliance important for the reliability of the information?

A. Compliance is another word for reliability. So, if a company indicates that it is compliant, it means that the information is managed properly.

B. By meeting the legislative requirements and the regulations of both the government and internal management, an organization shows that it manages its information in a sound manner.

C. When an organization employs a standard such as the ISO/IEC 27002 and uses it everywhere, it is compliant and therefore it guarantees the reliability of its information.

D. When an organization is compliant, it meets the requirements of privacy legislation and, in doing so, protects the reliability of its information.

ANSWER: B

Explanation:

By meeting the legislative requirements and the regulations of both the government and internal management, an organization shows that it manages its information in a sound manner. Compliance is important because it demonstrates that information handling is subject to defined, relevant requirements rather than being performed inconsistently or solely at individual discretion. These requirements can include laws, sector regulations, contractual obligations, and management-approved internal policies. Meeting them requires the organization to establish and operate controls, assign responsibilities, retain evidence where necessary, and review whether requirements continue to be met. This creates confidence that information is handled in a controlled and dependable way, supporting its reliability for business operations and stakeholders.

ISO/IEC 27002 provides guidance on information security controls that organizations can use as part of an information security management approach; it supports the implementation of appropriate organizational practices but does not itself guarantee any outcome. Compliance therefore provides assurance through demonstrable adherence to applicable obligations and governance requirements. ISO describes the standard and its role in guidance for information security controls at ISO/IEC 27002:2022. Further information on the value of managing compliance obligations within an information security program is available from NIST SP 800-53.

QUESTION NO: 4

What is the most common risk strategy besides Risk bearing and Risk neutral?

A. Risk acceptance

B. Risk avoidance

C. Risk insurance

D. Risk transference

ANSWER: B

Explanation:

Risk avoidance is correct. It is a risk strategy in which an organization decides not to begin, continue, or participate in an activity that creates an unacceptable level of risk. In an information-security context, this can mean retiring a vulnerable system, declining to process particularly sensitive information in an unsuitable environment, or changing a business process so that the threatening situation no longer exists. The strategy is appropriate where the potential impact exceeds the organization's defined risk appetite and the risk cannot be reduced to an acceptable level through feasible controls.

ISO risk-management guidance recognizes avoiding risk as a treatment approach: the organization can remove the source of risk or choose not to undertake the activity that gives rise to it. This reflects a cautious, risk-averse approach and is a common strategic position alongside bearing risk and taking a neutral stance. The decision should be made through the organization's established risk-management process, considering business objectives, legal obligations, and the residual risk that management is prepared to accept. See ISO 31000 risk management and NIST SP 800-30 Rev. 1.

QUESTION NO: 5

Why should an organization maintain an inventory of its information assets?

A. To identify assets that require ownership, protection and management.

B. To ensure that every asset has the same financial value.

C. To allow all employees to use every asset.

D. To remove the need to perform risk assessments.

ANSWER: A

Explanation:

An inventory enables the organization to identify the information assets for which protection, ownership, maintenance, and risk assessment are required. Assets can include information, software, devices, systems, storage media, and supporting services. Without an inventory, assets may be overlooked when responsibilities are assigned, access is reviewed, controls are applied, or risks are assessed.

Asset identification and ownership support the management of information throughout its life cycle. ISO/IEC 27002 includes controls for inventory of information and other associated assets and for assigning their ownership. See ISO/IEC 27002:2022.

QUESTION NO: 6

Which of the following measures is a preventive measure?

A. Installing a logging system that enables changes in a system to be recognized

B. Shutting down all internet traffic after a hacker has gained access to the company systems

C. Putting sensitive information in a safe

D. Classifying a risk as acceptable because the cost of addressing the threat is higher than the value of the information at risk

ANSWER: C

Explanation:

Putting sensitive information in a safe is a preventive measure because it is designed to stop, or substantially hinder, an unauthorized event before it occurs. A safe provides a physical barrier that restricts access to valuable paper records, storage media, backup devices, cryptographic material, or other sensitive assets. Its locks, controlled key or combination access, and resistance to forced entry reduce the opportunity for theft, unauthorized disclosure, damage, or tampering. This

directly supports the confidentiality and integrity of information by ensuring that only authorized people can physically obtain the protected material.

In information-security control terminology, preventive controls operate proactively: they reduce the likelihood that a threat can exploit a vulnerability. Physical security is an important part of an information-security management system, since information can be compromised through physical access as well as through technical means. The ISO/IEC 27002 guidance includes physical-security controls intended to protect offices, rooms, facilities, and physical media against unauthorized access and related risks. A properly selected safe, combined with appropriate access management and secure operating procedures, is therefore a clear example of a control whose principal purpose is prevention. See ISO/IEC 27002:2022 overview and NIST SP 800-53 physical and media protection controls.

QUESTION NO: 7

A system administrator needs to perform maintenance on a production server during the weekend. What is the most appropriate organizational measure before the maintenance starts?

A. Obtain authorization and follow the approved change-management procedure.

B. Give all users administrator rights before the maintenance begins.

C. Remove the server from the asset register.

D. Disable all logging so that the maintenance can be completed faster.

ANSWER: A

Explanation:

The maintenance should be authorized and planned through the organization's change-management procedure. The procedure ensures that the purpose, expected effect, risks, implementation steps, rollback arrangements, responsibilities, and timing are considered before a change is made. This reduces the risk that an unplanned or poorly controlled activity affects the availability or integrity of the production system.

Operational procedures and change management are important controls for maintaining secure and reliable information-processing systems. See ISO/IEC 27002:2022 and NIST SP 800-128.

QUESTION NO: 8

A company moves into a new building. A few weeks after the move, a visitor appears unannounced in the office of the director. An investigation shows that visitors passes grant the same access as the passes of the companys staff. Which kind of security measure could have prevented this?

A. A physical security measure

B. An organizational security measure

C. A technical security measure

ANSWER: A

Explanation:

A physical security measure is correct because the incident concerns unauthorized physical entry into areas of the building. Visitor badges and staff badges are part of physical access control: they are used to identify people entering premises and to enforce their permitted access to rooms or zones. A suitable physical measure would ensure that visitor passes are issued with restricted access rights, such as access only to reception, meeting rooms, or designated visitor areas, while staff passes are assigned only the access necessary for each employee's role. Physical access-control systems can also limit the validity period of visitor credentials, require escorting, and produce entry logs for review. These controls apply protection at the building boundary and internal secure areas, preventing a visitor credential from opening doors intended for authorized personnel. ISO/IEC 27002 addresses physical security through controls for physical entry and

security monitoring, including managing access to premises and protected areas. Guidance on these controls is available from ISO's ISO/IEC 27002 overview and the UK National Cyber Security Centre physical security guidance. Correctly separating visitor and employee access permissions would therefore have prevented the visitor from reaching the director's office unannounced.

QUESTION NO: 9

Which approach does/did the United States take with regard to privacy legislation?

A. Create legislation as it is needed

B. Proactively create legislation on upcoming technologies

C. Rely purely on self-regulation

D. Translate the convention on human rights into privacy laws

ANSWER: A

Explanation:

"Create legislation as it is needed" is correct because the United States has historically used a sectoral, issue-driven approach to privacy regulation rather than adopting one comprehensive, economy-wide privacy law. Federal privacy requirements have generally been enacted to address particular risks, industries, populations, or types of information as they emerged or became significant. Examples include protections for children's online information, health information, consumer financial data, and certain educational records. This produces a framework of targeted statutes and regulatory responsibilities, supplemented by state privacy and consumer-protection laws. The approach reflects the United States' development of privacy law through specific legislative responses and enforcement mechanisms, instead of translating a general human-rights convention directly into a single privacy regime. The Federal Trade Commission also plays an important role in this framework through its authority to address unfair or deceptive practices affecting consumers' privacy. The FTC describes the principal federal privacy laws and its privacy enforcement role at https://www.ftc.gov/business-guidance/privacy-security. A Congressional Research Service overview of the United States' sector-specific federal privacy framework is available at https://crsreports.congress.gov/product/pdf/R/R45631.

QUESTION NO: 10

Your company is concerned about the effect of global warming on sea levels and asks you to make preparations that prevents downtime of the billing process.

What will you create?

A. Business Continuity Plan

B. Disaster Recovery Plan

ANSWER: A

Explanation:

Business Continuity Plan is correct because the stated objective is to maintain the availability of the billing process and prevent unacceptable interruption when a foreseeable environmental threat, such as sea-level rise and associated flooding, affects the organization. A business continuity plan documents the arrangements needed to sustain prioritized products, services, and critical business activities through a disruption. For billing, this would be informed by a business impact analysis and could include identifying the maximum tolerable outage, assigning roles and escalation procedures, arranging alternate work locations or processing capability, ensuring supplier dependencies are addressed, and exercising the continuity arrangements.

ISO 22301 describes business continuity management as helping organizations continue delivering products and services at an acceptable predefined capacity during disruption. This makes continuity planning appropriate for preparing the business operation itself against long-term climate-related physical risks as well as more immediate incidents. The plan should be

maintained, tested, and updated as risk conditions, such as flood exposure at facilities or data-centre locations, change. See ISO 22301:2019—Business continuity management systems and NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

QUESTION NO: 11

What is an example of a good physical security measure?

A. All employees and visitors carry an access pass.

B. Printers that are defective or have been replaced are immediately removed and given away as garbage for recycling.

C. Maintenance staff can be given quick and unimpeded access to the server area in the event of disaster.

ANSWER: A

Explanation:

All employees and visitors carry an access pass. This is a good physical security measure because it supports the controlled identification of people in organizational premises and makes it easier to distinguish authorized personnel from people who require escorting or further verification. Access passes can be linked to role-based access rights, restricted areas, and time limits; visitor passes can additionally identify a visitor's host and expiry date. Staff and security personnel can then promptly challenge someone who is not visibly authorized to be present. This measure also supports accountability, especially where passes are used with electronic access-control systems that record entry and exit events. ISO/IEC 27002 includes physical security controls addressing physical entry, secure areas, and the protection of information-processing facilities. A visible pass process is a practical implementation of those controls, provided that pass issuance, return, revocation, and lost-pass reporting are managed consistently. NIST similarly describes physical access authorization as allowing entry only to individuals with an approved business need. See ISO/IEC 27002:2022 and NIST SP 800-53 Physical Access Authorizations.

QUESTION NO: 12

Midwest Insurance controls access to its offices with a passkey system. What kind of security measure is this?

A. Corrective

B. Detective

C. Preventive

D. Repressive

ANSWER: C

Explanation:

A passkey system used to control entry to offices is a preventive security measure. Its purpose is to stop unauthorized people from gaining physical access before an incident can occur. By requiring a valid passkey, the organization enforces authorization at the boundary of the office area and limits access to people who have been granted the appropriate rights. This supports physical access control, which ISO/IEC 27002 treats as an important component of protecting facilities, information, and other assets from unauthorized access, damage, or interference.

Preventive controls operate in advance of a security event: they reduce the likelihood that a threat can be realized. In this case, the passkey mechanism restricts entry at the point of access, rather than merely recording entry after it happens or restoring conditions following an incident. The control may also produce access logs, but the central function described—controlling access through a passkey—is prevention. See ISO's overview of ISO/IEC 27002 at ISO/IEC 27002:2022 and NIST's physical and environmental protection control family at NIST SP 800-53 Physical and Environmental Protection.

QUESTION NO: 13

The term ‘big data’ is commonly used. However data itself has less (or no) value for an organization. Which process adds value to the data and turns data into ‘information’?

A. Analysis

B. Archiving

C. Back-up

D. Duplication

ANSWER: A

Explanation:

Analysis is correct because data consists of raw facts, observations, measurements, or records that have not yet been interpreted in a meaningful context. Analysis processes that raw data by examining it, identifying patterns or relationships, applying context, and deriving conclusions that support understanding and decision-making. The resulting information has value to an organization because it can be used to assess risks, monitor performance, make operational decisions, or support security controls.

In an information-security context, the distinction matters because an organization must protect information according to its value, sensitivity, and business purpose. Analysis may turn technical records such as authentication events, network logs, or access records into meaningful information about suspicious activity, operational trends, or compliance status. This supports informed risk management and appropriate information handling. ISO/IEC 27002 guidance addresses information security controls designed to preserve the confidentiality, integrity, and availability of information throughout its use and processing. For background on the data-to-information concept, see Encyclopaedia Britannica: information systems. For ISO/IEC 27002’s scope and purpose, see ISO/IEC 27002:2022.

QUESTION NO: 14

Someone sends an e-mail. The sender wants the recipient to be able to verify who wrote and sent the email.

What does the sender attach to the email?

A. A digital signature

B. A PKI certificate

C. Her private key

D. Her public key

ANSWER: A

Explanation:

A digital signature is attached to provide assurance of the sender’s identity and the message’s origin. The sender creates the signature using her private key and the message data. The recipient can then validate that signature with the corresponding public key, usually obtained through the sender’s certificate. Successful validation demonstrates that the message was signed by the holder of the private key associated with that public key, supporting authentication of the claimed sender. It also protects integrity: if the email content were changed after it was signed, signature validation would fail because the calculated message digest would no longer match the signed digest.

For secure email implementations such as S/MIME, the signed email commonly carries the signer’s certificate as part of the signed message structure so that the recipient can obtain the public key and evaluate the certificate chain. Nevertheless, the security mechanism that supplies the proof of origin and integrity is the digital signature itself. NIST describes digital signatures as providing origin authentication, data integrity, and non-repudiation support; S/MIME defines the use of cryptographic signatures for secure email. See NIST’s definition of a digital signature and RFC 8551, S/MIME Version 4.0.