Sample Exam

Edition 202302

Content

Introduction

This is the EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth 1 point. You need 26 points or more to pass the exam.

The time allowed for this exam is 60 minutes.

Good luck!

Sample exam

1 / 40
A database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) Data
B) Information
C) Data and information

2 / 40
What is the difference between data and information?

A) Data can be any facts or figures. Information is data that has meaning.
B) Data consists of unstructured figures. Information consists of structured figures.
C) Data does not require security. Information requires security.
D) Data has no value. Information, which is processed data, has value.

3 / 40
What is the focus of information management?

A) Allowing business activities and processes to continue without interruption
B) Ensuring that the value of information is identified and exploited
C) Preventing unauthorized persons from having access to automated systems
D) Understanding how information flows through an organization

4 / 40
An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) The likelihood of something happening and its consequences to the organization
B) The most common dangers and how to mitigate these as defined in best practices
C) The threats an organization faces and how vulnerable the organization is to them
D) The unplanned events an organization faces and what to do in case of such an event

5 / 40
Besides integrity and confidentiality, what is the third reliability aspect of information?

A) Accuracy
B) Availability
C) Completeness
D) Value

6 / 40
An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) The availability of the information is no longer guaranteed.
B) The confidentiality of the information is no longer guaranteed.
C) The integrity of the information is no longer guaranteed.

7 / 40
What is the difference between accountability and auditability?

A) Accountability means an organization has their financial accounts well-administered.
Auditability means an organization passed an audit.
B) Accountability means being liable for the results of an organization's activities.
Auditability refers to an organization's readiness for being independently reviewed.
C) Accountability means having responsibility for an individual's actions.
Auditability means having responsibility for an organization's actions.
D) Accountability means that an organization complies with Sarbanes-Oxley (SOX).
Auditability refers to an organization complying with ISO/IEC 27001.

8 / 40
How is the purpose of an information security policy **best** described?

A) An information security policy documents the analysis of risks and the search for appropriate controls.
B) An information security policy gives direction and support to the organization regarding information security.
C) An information security policy makes the security plan concrete by providing it with the necessary details.
D) An information security policy provides insight into threats and the possible consequences.

9 / 40
Sara has been tasked with ensuring that the organization complies with personal data legislation.

What is the **first** thing she should do?

A) Appoint a person responsible for supporting managers in adhering to the policy
B) Issue a ban on collecting and storing personal information
C) Make employees responsible for submitting their personal data
D) Translate the personal data protection legislation into a privacy policy

10 / 40
An organization decides to outsource some of its IT.

How can information security **best** be ensured when working with a supplier?

A) Appoint a new information security officer (ISO) in the supplier's organization
B) Formalize the information security requirements for the supplier in an agreement
C) Keep both organizations fully separated to make everyone accountable for their data
D) Require the supplier to follow the customer organization's processes and procedures

11 / 40
Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) Chief information security officer (CISO)
B) General management
C) Information security officer (ISO)
D) Information security policy officer

12 / 40
Which is a human threat?

A) A leak causes a failure of the electricity supply.
B) A USB-stick passes on a virus to a network.
C) There is too much dust in the server room.

13 / 40
A database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) Impact
B) Risk
C) Threat
D) Vulnerability

14 / 40
There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

What **indirect** damage is caused by this fire?

A) Burned computer systems
B) Burned documents
C) Melted backup tapes
D) Water damage

15 / 40
Companies can have different risk strategies depending on the type of business.

Which risk strategy is **most** suitable for a hospital?

A) Risk accepting
B) Risk avoiding
C) Risk bearing
D) Risk neutral

16 / 40
A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives.

What is **not** a main objective of a risk analysis?

A) Balance the costs of an incident and the costs of a control
B) Determine relevant vulnerabilities and threats
C) Identify assets and their value
D) Implement measures and controls

17 / 40
What is a repressive control in case of a fire?

A) Putting out a fire after it has been detected
B) Repairing damage caused by the fire
C) Taking out a fire insurance

18 / 40
What is the goal of classification of information?

A) Applying labels to make the information easier to recognize
B) Creating a manual on how to handle mobile devices
C) Structuring information according to its sensitivity

19 / 40
What is the **most** important reason to apply segregation of duties?

A) Ensuring that employees do the same work at the same time
B) Holding all employees jointly responsible for the mistakes they make
C) Making clear who is responsible for what tasks and activities
D) Minimizing the chance of unauthorized or unintended changes

20 / 40
What is the **best** way to ensure appropriate access to information?

A) Automate workflows
B) Define operating procedures
C) Develop work instructions for all tasks
D) Provide training

21 / 40
A fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) Between the damage and recovery stages
B) Between the incident and damage stages
C) Between the recovery and threat stages
D) Between the threat and incident stages

22 / 40
An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.

The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) The name of the person reporting the incident
B) The name of the software package
C) The PC number

23 / 40
Why is it important to regularly audit the organization's information security management system (ISMS)?

A) Audits are a common requirement in customer contracts to ensure information security.
B) Audits are a required element in order to comply with legal or regulatory requirements.
C) Audits uncover issues with the ability to meet an organization's financial targets.
D) Audits uncover weaknesses in the implementation of information security controls.

24 / 40
Which document would include a rule that forbids the use of company computers for private e-mail?

A) Certificate of good character
B) Code of conduct
C) General Data Protection Regulation (GDPR)
D) Non-disclosure agreement (NDA)

25 / 40
When an employee detects an incident, to whom should it typically be reported **first**?

A) The help desk
B) The information security manager (ISM)
C) The information security officer (ISO)
D) The manager

26 / 40
What is the **most** effective way to create information security awareness among employees?

A) Focus awareness training on the management team
B) Send all employees to an external information security training
C) Set up an organization-specific awareness program
D) Use a generic, online information security training course

27 / 40
What physical control manages access to an organization's information?

A) Installing air conditioning
B) Prohibiting the use of USB sticks
C) Requiring username and password
D) Using unbreakable glass

28 / 40
A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) The main power may not come up again automatically when restored, because this needs a power generator.
B) The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.
C) The battery packs' lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.
D) The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

29 / 40
Why is air conditioning placed in the server room?

A) Back-up tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in a server room, they may get damaged.
B) Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.
C) In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.
D) The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

30 / 40
In physical security, multiple protection rings can be applied in which different measures can be taken.

What is **not** a protection ring?

A) Building ring
B) Middle ring
C) Secure room ring
D) Outer ring

31 / 40
The control to secure an asset depends on the asset.

What is the **most** appropriate way to secure the asset?

A) Secure a form by having it filled out and signed off
B) Secure a laptop by assigning it to a single user
C) Secure a USB-stick with encryption
D) Secure an internet connection with a backup

32 / 40
What information security control helps to develop systems with information security in mind?

A) Ensuring redundancy of the servers
B) Implementing physical entry controls
C) Performing background checks on employees
D) Using data classification on information assets

33 / 40
An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) Create V-LANs to segment the corporate network
B) Encrypt the information on the corporate network
C) Install firewalls on the corporate network
D) Use a VPN to connect to the corporate network

34 / 40
The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair.

If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) When the private key becomes known
B) When the public key becomes known
C) When the public key infrastructure (PKI) becomes known

35 / 40
What sort of security does a public key infrastructure (PKI) offer?

A) A PKI ensures that backups of company data are made on a regular basis.
B) A PKI shows customers that a web-based business is secure.
C) A PKI verifies which person or system belongs to a specific public key.

36 / 40
Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) Logic bomb
B) Spyware
C) Trojan
D) Worm

37 / 40
Which type of malware builds a network of contaminated computers?

A) Logic bomb
B) Spyware
C) Trojan
D) Worm

38 / 40
Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) General Data Protection Regulation (GDPR)
B) Intellectual property (IP) rights
C) ISO/IEC 27001
D) ISO/IEC 27002

39 / 40
Which ISO standard is focused on the implementation of information security controls?

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

40 / 40
The standards of which organization is **most** commonly used in Europe?

A) American National Standards Institute (ANSI)
B) International Organization for Standardization (ISO)
C) National Institute of Standards and Technology (NIST)

Answer key

1 / 40
A database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) Data
B) Information
C) Data and information

A) Incorrect. The database contains data. However, when an invoice is generated and sent to a recipient, it is information for the recipient.
B) Correct. The value of information is determined by the recipient. The invoice contains valuable data for the recipient, and therefore it is information. (Literature: A, Chapter 4.8.5)
C) Incorrect. The invoice contains only information for the recipient.

2 / 40
What is the difference between data and information?

A) Data can be any facts or figures. Information is data that has meaning.
B) Data consists of unstructured figures. Information consists of structured figures.
C) Data does not require security. Information requires security.
D) Data has no value. Information, which is processed data, has value.

A) Correct. Information is derived from data by giving it meaning in a certain context. (Literature: A, Chapter 3.1)
B) Incorrect. Data can be either structured or unstructured. Information is usually structured.
C) Incorrect. Both data and information require security.
D) Incorrect. Both data and information have value.

3 / 40
What is the focus of information management?

A) Allowing business activities and processes to continue without interruption
B) Ensuring that the value of information is identified and exploited
C) Preventing unauthorized persons from having access to automated systems
D) Understanding how information flows through an organization

A) Incorrect. This is the focus of business continuity management (BCM). The purpose of BCM is to prevent business activities from being disrupted, to protect critical processes against the consequences of far-reaching disruptions in information systems, and to allow for speedy recovery.
B) Correct. Information management describes how an organization efficiently plans, collects, organizes, uses, controls, disseminates, and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent. (Literature: A, Chapter 4.9)
C) Incorrect. This is the focus of access management. It ensures that unauthorized persons or processes do not have access to automated systems, databases, and programs.
D) Incorrect. This is the focus of information analysis. It provides a clear picture of how an organization handles information, and how the information flows through the organization.

4 / 40
An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) The likelihood of something happening and its consequences to the organization
B) The most common dangers and how to mitigate these as defined in best practices
C) The threats an organization faces and how vulnerable the organization is to them
D) The unplanned events an organization faces and what to do in case of such an event

A) Correct. Two high-level factors determine risk: the likelihood of something happening and its impact on the business. If either of these is very low, the business should rather focus on something more important. (Literature: A, Chapter 3.1)
B) Incorrect. It is unwise to have this as a starting point when an organization defines their risks. Doing what other organizations do does not make this organization safe.
C) Incorrect. This is a description of the term likelihood. Although it is important to understand likelihood, an important aspect is missing: how it will affect the business.
D) Incorrect. Eventually, matching risks and controls are needed, but this is rather a response to risk than a way to understand risk in the first place.

5 / 40
Besides integrity and confidentiality, what is the third reliability aspect of information?

A) Accuracy
B) Availability
C) Completeness
D) Value

A) Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Accuracy is a part of integrity.
B) Correct. The three reliability aspects of information are availability, integrity, and confidentiality. (Literature: A, Chapter 3.4.3)
C) Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Completeness is a part of integrity.
D) Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality.

6 / 40
An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) The availability of the information is no longer guaranteed.
B) The confidentiality of the information is no longer guaranteed.
C) The integrity of the information is no longer guaranteed.

A) Incorrect. The information is still available in the system that was used to create and print it.
B) Correct. The information can end up with, or be read by, persons who should not have access to this information. (Literature: A, Chapter 3.4.1)
C) Incorrect. The integrity of the information on the prints is still guaranteed since it is on paper.

7 / 40
What is the difference between accountability and auditability?

A) Accountability means an organization has their financial accounts well-administered.
Auditability means an organization passed an audit.
B) Accountability means being liable for the results of an organization's activities.
Auditability refers to an organization's readiness for being independently reviewed.
C) Accountability means having responsibility for an individual's actions.
Auditability means having responsibility for an organization's actions.
D) Accountability means that an organization complies with Sarbanes-Oxley (SOX).
Auditability refers to an organization complying with ISO/IEC 27001.

A) Incorrect. Accountability has no direct relationship with financial accounting. Auditability has no relationship with having passed an audit.
B) Correct. These are the correct definitions of accountability and auditability. (Literature: A, Chapter 3.4.4)
C) Incorrect. The definition of accountability is correct, but the definition of auditability is not. Auditability has nothing to do with responsibility for the organization's actions.
D) Incorrect. Neither accountability nor auditability refer to compliance with SOX or ISO/IEC standards.

8 / 40
How is the purpose of an information security policy **best** described?

A) An information security policy documents the analysis of risks and the search for appropriate controls.
B) An information security policy gives direction and support to the organization regarding information security.
C) An information security policy makes the security plan concrete by providing it with the necessary details.
D) An information security policy provides insight into threats and the possible consequences.

A) Incorrect. The analysis of risks and the search for controls is the purpose of risk analysis and risk management.
B) Correct. With the security policy, management provides direction and support regarding information security. (Literature: A, Chapter 4.2.1)
C) Incorrect. The security plan makes the information security policy concrete. The plan includes which controls have been chosen, who is responsible for what, the guidelines for the implementation of controls, etc.
D) Incorrect. The purpose of a threat analysis is to provide insight into threats and the possible consequences.

9 / 40
Sara has been tasked with ensuring that the organization complies with personal data legislation.

What is the **first** thing she should do?

A) Appoint a person responsible for supporting managers in adhering to the policy
B) Issue a ban on collecting and storing personal information
C) Make employees responsible for submitting their personal data
D) Translate the personal data protection legislation into a privacy policy

A) Incorrect. A person to support managers is not a requirement to become compliant with personal data protection legislation. In addition, the policy should first align with the legislation.
B) Incorrect. This is not the best way to comply with personal data protection legislation.
C) Incorrect. This is not a way to become compliant with personal data protection legislation.
D) Correct. The first step to becoming compliant is to create an internal policy for the organization. (Literature: A, Chapter 5.1)

10 / 40
An organization decides to outsource some of its IT.

How can information security **best** be ensured when working with a supplier?

A) Appoint a new information security officer (ISO) in the supplier's organization
B) Formalize the information security requirements for the supplier in an agreement
C) Keep both organizations fully separated to make everyone accountable for their data
D) Require the supplier to follow the customer organization's processes and procedures

A) Incorrect. It is not necessary to appoint a new ISO in the supplier's organization if the organization already has one.
B) Correct. Although entering into an agreement is not a fail-safe mechanism to manage supplier risk, it is the most effective way of doing so. (Literature: A, Chapter 5.20)
C) Incorrect. The customer organization remains accountable for all information. Keeping the organizations fully separated often implies the customer organization does not know how to ensure or influence information security in the supplier's organization.
D) Incorrect. This is not the best way because a supplier should be allowed to have their own information security process in place.

11 / 40
Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) Chief information security officer (CISO)
B) General management
C) Information security officer (ISO)
D) Information security policy officer

A) Correct. The CISO is at the highest management level of the organization and develops the general security strategy for the entire business. (Literature: A, Chapter 5.2)
B) Incorrect. General management defines the strategy that is input for the CISO to define the general security strategy.
C) Incorrect. The ISO develops the information security policy of a business unit based on the company policy and ensures that it is observed.
D) Incorrect. The information security policy officer is responsible for maintaining the policy that is derived from the security strategy.

12 / 40
Which is a human threat?

A) A leak causes a failure of the electricity supply.
B) A USB-stick passes on a virus to a network.
C) There is too much dust in the server room.

A) Incorrect. A leak is not a human threat, but a non-human threat.
B) Correct. A USB-stick is always inserted by a person. If this causes a virus entering the network, it is a human threat. (Literature: A, Chapter 3.9.1)
C) Incorrect. Dust is not a human threat, but a non-human threat.

13 / 40
A database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) Impact
B) Risk
C) Threat
D) Vulnerability

A) Incorrect. Impact is the effect an event has on the organization or its information.
B) Incorrect. A risk is the combination of the likelihood and impact of an event happening.
C) Incorrect. An example of a threat is an external entity trying to exploit a vulnerability. In this case, the hackers form the threat.
D) Correct. An example of a vulnerability is a lack of protection. (Literature: A, Chapter 3.5.3)

14 / 40
There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

What **indirect** damage is caused by this fire?

A) Burned computer systems
B) Burned documents
C) Melted backup tapes
D) Water damage

A) Incorrect. Burned computer systems are direct damage caused by the fire.
B) Incorrect. Burned documents are direct damage caused by the fire.
C) Incorrect. Melted backup tapes are direct damage caused by the fire.
D) Correct. Water damage due to the fire extinguishers is indirect damage caused by the fire. This is a side effect of putting out the fire, which is aimed at minimizing the damage caused by the fire. (Literature: A, Chapter 3.10)

15 / 40
Companies can have different risk strategies depending on the type of business.

Which risk strategy is **most** suitable for a hospital?

A) Risk accepting
B) Risk avoiding
C) Risk bearing
D) Risk neutral

A) Incorrect. A hospital cannot easily accept risks due to financial losses or dying patients.
B) Correct. Hospitals should try to avoid any risk. (Literature: A, Chapter 3.11)
C) Incorrect. Risk bearing means that certain risks are accepted. This could be because the costs of controls exceed the possible damage. In a hospital, this is not the best way to handle risks.
D) Incorrect. Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. Damage to clients is never a good idea, so hospitals should be risk avoiding.

16 / 40
A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives.

What is **not** a main objective of a risk analysis?

A) Balance the costs of an incident and the costs of a control
B) Determine relevant vulnerabilities and threats
C) Identify assets and their value
D) Implement measures and controls

A) Incorrect. This is one of the main objectives of a risk analysis.
B) Incorrect. This is one of the main objectives of a risk analysis.
C) Incorrect. This is one of the main objectives of a risk analysis.
D) Correct. This is not an objective of a risk analysis. (Literature: A, Chapter 3.7)

17 / 40
What is a repressive control in case of a fire?

A) Putting out a fire after it has been detected
B) Repairing damage caused by the fire
C) Taking out a fire insurance

A) Correct. This repressive control minimizes the damage caused by a fire. (Literature: A, Chapter 3.8)
B) Incorrect. This is not a repressive control. It does not minimize the damage caused by the fire.
C) Incorrect. Taking out an insurance protects against the financial consequences of a fire and is risk insurance.

18 / 40
What is the goal of classification of information?

A) Applying labels to make the information easier to recognize
B) Creating a manual on how to handle mobile devices
C) Structuring information according to its sensitivity

A) Incorrect. Applying labels to information is designation, which is a special form of categorizing information that follows on the classification of information.
B) Incorrect. Creating a manual relates to user guidelines and is not classification of information.
C) Correct. Classification of information is used to define the different levels of sensitivity into which information can be structured. (Literature: A, Chapter 5.12)

19 / 40
What is the **most** important reason to apply segregation of duties?

A) Ensuring that employees do the same work at the same time
B) Holding all employees jointly responsible for the mistakes they make
C) Making clear who is responsible for what tasks and activities
D) Minimizing the chance of unauthorized or unintended changes

A) Incorrect. Segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. It does not define when activities should be performed.
B) Incorrect. Segregation of duties separates tasks and responsibilities. It does not make a group of people jointly responsible.
C) Incorrect. The segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. Its objective is not to make clear who is responsible for what.
D) Correct. Duties must be segregated to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. (Literature: A, Chapter 5.3)

20 / 40
What is the **best** way to ensure appropriate access to information?

A) Automate workflows
B) Define operating procedures
C) Develop work instructions for all tasks
D) Provide training

A) Incorrect. Automating workflows will certainly contribute to information security, but it does not help appropriate access.
B) Correct. The use of procedures to guide how work is done in an appropriate, safe, and responsible manner is an effective way to achieve effective information security. (Literature: A, Chapter 5.36.1)
C) Incorrect. This is too detailed and prescriptive, and therefore not the best way.
D) Incorrect. Training is important but it does not ensure appropriate access to information.

21 / 40
A fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) Between the damage and recovery stages
B) Between the incident and damage stages
C) Between the recovery and threat stages
D) Between the threat and incident stages

A) Incorrect. Damage and recovery are limited by the stand-by arrangement.
B) Correct. A stand-by arrangement is a repressive measure that is initiated to limit the damage. (Literature: A, Chapter 3.8.4)
C) Incorrect. The recovery stage takes place after putting a stand-by arrangement into operation.
D) Incorrect. Carrying out a stand-by arrangement without an incident is very expensive.

22 / 40
An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.

The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) The name of the person reporting the incident
B) The name of the software package
C) The PC number

A) Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. (Literature: A, Chapter 5.25)
B) Incorrect. This is additional information that may be added later.
C) Incorrect. This is additional information that may be added later.

23 / 40
Why is it important to regularly audit the organization's information security management system (ISMS)?

A) Audits are a common requirement in customer contracts to ensure information security.
B) Audits are a required element in order to comply with legal or regulatory requirements.
C) Audits uncover issues with the ability to meet an organization's financial targets.
D) Audits uncover weaknesses in the implementation of information security controls.

A) Incorrect. Customer contracts rarely contain audit requirements.
B) Incorrect. Legal or regulatory requirements usually do not require audits to be done.
C) Incorrect. Audits are not commonly used to verify financial performance.
D) Correct. The purpose of audits is to find weaknesses in implemented controls. (Literature: A, Chapter 5.35)

24 / 40
Which document would include a rule that forbids the use of company computers for private e-mail?

A) Certificate of good character
B) Code of conduct
C) General Data Protection Regulation (GDPR)
D) Non-disclosure agreement (NDA)

A) Incorrect. A certificate of good character is issued by an organization such as the Department of Justice and indicates that no criminal offences were committed by the individual.
B) Correct. The code of conduct is a document (often part of the employee manual) that describes the company policies that are applicable to personnel. (Literature: A, Chapter 6.2)
C) Incorrect. The GDPR is about the protection of personal information.
D) Incorrect. An NDA is a contract that forbids the disclosure of certain information. The use of company e-mail for private purposes is not controlled by such a document.

25 / 40
When an employee detects an incident, to whom should it typically be reported **first**?

A) The help desk
B) The information security manager (ISM)
C) The information security officer (ISO)
D) The manager

A) Correct. Typically, incidents should be reported to the help desk for evaluation, application of initial procedures and escalation if required. They should not be escalated vertically immediately. (Literature: A, Chapter 6.8)
B) Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
C) Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
D) Incorrect. Incidents should not be escalated vertically immediately.

26 / 40
What is the **most** effective way to create information security awareness among employees?

A) Focus awareness training on the management team
B) Send all employees to an external information security training
C) Set up an organization-specific awareness program
D) Use a generic, online information security training course

A) Incorrect. All employees need awareness of information security, not only managers.
B) Incorrect. External training may not be fully applicable to a specific organization's needs.
C) Correct. Adapting a security awareness program to the specific organizational needs is most effective. (Literature: A, Chapter 6.3)
D) Incorrect. Generic information security training may not be fully applicable to a specific organization's needs.

27 / 40
What physical control manages access to an organization's information?

A) Installing air conditioning
B) Prohibiting the use of USB sticks
C) Requiring username and password
D) Using unbreakable glass

A) Incorrect. Air conditioning does not manage access to an organization's information.
B) Incorrect. This is an organizational control.
C) Incorrect. This is a technical control.
D) Correct. The use of unbreakable glass is an example of a physical control to prevent unauthorized persons from entering the building. (Literature: A, Chapter 7.4)

28 / 40
A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) The main power may not come up again automatically when restored, because this needs a power generator.
B) The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.
C) The battery packs' lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.
D) The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

A) Incorrect. A power generator is not used to trigger the main power supply.
B) Correct. Battery packs only protect against temporary power outages and surges, whereas a power generator protects for longer-duration outages. (Literature: A, Chapter 7.11.1)
C) Incorrect. Diesel is used to power the generator; a battery pack is powered by batteries.
D) Incorrect. The battery packs will only work for a short period but are not powered by the generator. The generator simply takes over from the battery pack.

29 / 40
Why is air conditioning placed in the server room?

A) Back-up tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in a server room, they may get damaged.
B) Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.
C) In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.
D) The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

A) Incorrect. Back-up tapes should not be stored in the server room. A fire would then destroy both the information in use and the back-up.
B) Incorrect. This is not the reason why air conditioning should be installed in the server room.
C) Correct. Server rooms must be approached separately when considering physical security. Server rooms contain sensitive equipment that is vulnerable to humidity and warmth and produce heat themselves. (Literature: A, Chapter 7.11.2)
D) Incorrect. The server room is not the place to cool the air in the entire office.

30 / 40
In physical security, multiple protection rings can be applied in which different measures can be taken.

What is **not** a protection ring?

A) Building ring
B) Middle ring
C) Secure room ring
D) Outer ring

A) Incorrect. The building is a ring that deals with access to the premises.
B) Correct. There are four protection rings: outer ring, building, workspaces, and secure room. (Literature: A, Chapter 7.0.1)
C) Incorrect. The secure room ring is a valid zone and deals with the asset that is to be protected.
D) Incorrect. The outer ring is a valid zone and deals with the area around the premises.

31 / 40
The control to secure an asset depends on the asset.

What is the **most** appropriate way to secure the asset?

A) Secure a form by having it filled out and signed off
B) Secure a laptop by assigning it to a single user
C) Secure a USB-stick with encryption
D) Secure an internet connection with a backup

A) Incorrect. Filing a piece of paper with information is not an appropriate control.
B) Incorrect. It is obviously better if a single person uses a single laptop, but this is not the most appropriate option. User account management and password control are better controls.
C) Correct. Encryption is a valid control for securing a USB-stick. Many organizations apply this control regardless of the classification of the information stored on the USB-stick. (Literature: A, Chapter 8.12)
D) Incorrect. Using a backup is not the best, direct way to secure the internet connection.

32 / 40
What information security control helps to develop systems with information security in mind?

A) Ensuring redundancy of the servers
B) Implementing physical entry controls
C) Performing background checks on employees
D) Using data classification on information assets

A) Correct. Server redundancy is a control that should be considered during system development. (Literature: A, Chapter 8.14)
B) Incorrect. This is a valid control to enhance information security but is not related to system development.
C) Incorrect. This is a valid control to enhance information security but is not related to system development.
D) Incorrect. This is a valid control to enhance information security but is not related to system development.

33 / 40
An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) Create V-LANs to segment the corporate network
B) Encrypt the information on the corporate network
C) Install firewalls on the corporate network
D) Use a VPN to connect to the corporate network

A) Incorrect. Segmenting networks to ensure confidentiality and segregation of duties should already be in place. This does not specifically apply to changing the remote-working policy.
B) Incorrect. Encryption is a vital tool to use to protect information, but it does not specifically apply to allowing employees to work remotely.
C) Incorrect. Firewalls between the corporate network and the outside world are important but these should already be in place. Also, firewalls do not directly secure remote connections.
D) Correct. The use of VPNs is a control that should be put in place when employees are allowed to work remotely. (Literature: A, Chapter 8.2)

34 / 40
The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair.

If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) When the private key becomes known
B) When the public key becomes known
C) When the public key infrastructure (PKI) becomes known

A) Correct. In asymmetric encryption, it is important to keep the private key private. The public key may be known. (Literature: A, Chapter 8.24.5)
B) Incorrect. The public key may be open to the whole world. The private key should be kept secret to ensure integrity and availability.
C) Incorrect. PKI is used for the exchange of keys for asymmetrical encryption systems.

35 / 40
What sort of security does a public key infrastructure (PKI) offer?

A) A PKI ensures that backups of company data are made on a regular basis.
B) A PKI shows customers that a web-based business is secure.
C) A PKI verifies which person or system belongs to a specific public key.

A) Incorrect. A PKI does not ensure making backups.
B) Incorrect. A PKI provides guarantees regarding which person or system belongs to a specific public key.
C) Correct. A characteristic of a PKI is that through agreements, procedures, and an organization structure, it provides guarantees regarding which person or system belongs to a specific public key. (Literature: A, Chapter 8.24.6)

36 / 40
Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) Logic bomb
B) Spyware
C) Trojan
D) Worm

A) Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes. It does not always conduct secondary activities.
B) Incorrect. Spyware is a computer program that collects information on the user's computer and sends this information to another party.
C) Correct. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system. (Literature: A, Chapter 8.7.2)
D) Incorrect. A worm, also called botnet, is a collection of internet-connected programs communicating with other similar programs to perform tasks on someone's computer.

37 / 40
Which type of malware builds a network of contaminated computers?

A) Logic bomb
B) Spyware
C) Trojan
D) Worm

A) Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes.
B) Incorrect. Spyware is a computer program that collects information on the computer user and sends this information to another party.
C) Incorrect. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system.
D) Correct. This is what a worm does. (Literature: A, Chapter 8.7)

38 / 40
Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) General Data Protection Regulation (GDPR)
B) Intellectual property (IP) rights
C) ISO/IEC 27001
D) ISO/IEC 27002

A) Correct. All organizations should have a policy and procedures for personal data protection, which should be known by everybody who processes personal data. (Literature: A, Chapter 5.33)
B) Incorrect. This regulation is not related to information security for organizations.
C) Incorrect. This is a standard with guidelines for organizations on how to deal with the set-up of an information security process.
D) Incorrect. This standard, also known as 'Information security, cybersecurity and privacy protection - Information security controls', contains guidelines for information security policy and controls.

39 / 40
Which ISO standard is focused on the implementation of information security controls?

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

A) Incorrect. This is the general introduction to the ISO/IEC 27000 series of standards.
B) Incorrect. This is the standard with requirements for an information security management system.
C) Correct. This is the standard specifying information security controls with guidance on their implementation. (Literature A, Chapter 4.12)
D) Incorrect. ISO/IEC 27005 focuses on information security risk management.

40 / 40
The standards of which organization is **most** commonly used in Europe?

A) American National Standards Institute (ANSI)
B) International Organization for Standardization (ISO)
C) National Institute of Standards and Technology (NIST)

A) Incorrect. The ANSI standards are more common in the United States of America.
B) Correct. In Europe, the ISO standards are the most common. (Literature: A, Chapter 5.36)
C) Incorrect. The NIST standard is more common in the United States of America.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	B	21	B
2	A	22	A
3	B	23	D
4	A	24	B
5	B	25	A
6	B	26	C
7	B	27	D
8	B	28	B
9	D	29	C
10	B	30	B
11	A	31	C
12	B	32	A
13	D	33	D
14	D	34	A
15	B	35	C
16	D	36	C
17	A	37	D
18	C	38	A
19	D	39	C
20	B	40	B

Contact EXIN

www.exin.com