EXIN

EXIN Information Security ISO/IEC 27001

ESSENTIALS

Certified by EXIN

Sample Exam

Edition 202602

Content

Introduction

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

This exam consists of 20 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 20. Each correct answer is worth 1 point. You need 13 points or more to pass the exam.

The time allowed for this exam is 30 minutes.

Good luck!

Sample exam

1 / 20
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

2 / 20
Besides integrity and confidentiality, what is the third reliability aspect of information?

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

3 / 20
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.

4 / 20
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.

5 / 20
Sara has been tasked with ensuring that the organization complies with personal data protection 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

6 / 20
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

7 / 20
Which is the **best** example of 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.

8 / 20
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

9 / 20
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

10 / 20
A well-executed risk analysis provides a great deal of useful information. A risk analysis has different 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

11 / 20
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

12 / 20
What is the **most** important reason to apply segregation of duties?

A) Ensuring that employees do not 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

13 / 20
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

14 / 20
When an employee detects an incident, to whom should it typically be reported **first**?

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

15 / 20
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

16 / 20
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

17 / 20
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

18 / 20
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

19 / 20
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

20 / 20
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

Answer key

1 / 20
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.

2 / 20
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.

3 / 20
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.

4 / 20
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 are 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.

5 / 20
Sara has been tasked with ensuring that the organization complies with personal data protection 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)

6 / 20
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.

7 / 20
Which is the **best** example of 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.

8 / 20
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)

9 / 20
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.

10 / 20
A well-executed risk analysis provides a great deal of useful information. A risk analysis has different 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)

11 / 20
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)

12 / 20
What is the **most** important reason to apply segregation of duties?

A) Ensuring that employees do not 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)

13 / 20
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.

14 / 20
When an employee detects an incident, to whom should it typically be reported **first**?

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

A) Correct. Typically, incidents should be reported to the helpdesk 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.

15 / 20
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)

16 / 20
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.

17 / 20
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. These do 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)

18 / 20
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.

19 / 20
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 builds a network of contaminated computers by replicating itself.

20 / 20
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.

Evaluation

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

Question	Answer	Question	Answer
1	B	**11**	C
2	B	**12**	D
3	B	**13**	B
4	B	**14**	A
5	D	**15**	D
6	A	**16**	C
7	B	**17**	D
8	D	**18**	A
9	B	**19**	C
10	D	**20**	A

EXIN

Certified for what’s next

Contact EXIN

www.exin.com