EXIN Information Security Management ISO/IEC 27001

FOUNDATION

Certified by EXIN

Sample Exam

Edition 201804

Content

Introduction

This is the sample exam EXIN Information Security Foundation based on ISO/IEC 27001. The EXIN exam rules and regulations apply to this exam.

The Rules and Regulations for EXIN's examinations apply to this exam.

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

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for these sample questions is 60 minutes.

Good luck!

Sample Exam

1 / 40
What is the relationship between data and information?

A. Data is structured information.
B. Information is the meaning and value assigned to a collection of data.

2 / 40
In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is **not** important for determining the value of data for an organization?

A. The content of data.
B. The degree to which missing, incomplete or incorrect data can be recovered.
C. The indispensability of data for the business processes.
D. The importance of the business processes that make use of the data.

3 / 40
A hacker gains access to a webserver and can view a file on the server containing credit card numbers.

Which of the Confidentiality, Integrity, Availability (CIA) principles of the credit card file are violated?

A. Availability
B. Confidentiality
C. Integrity

4 / 40
There is a network printer in the hallway of the company where you work. Many employees don’t pick up their printouts immediately and leave them on the printer.

What are the consequences of this to the reliability of the information?

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

5 / 40
A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives.

What is **not** one of the four main objectives of a risk analysis?

A. Identifying assets and their value
B. Implementing counter measures
C. Establishing a balance between the costs of an incident and the costs of a security measure
D. Determining relevant vulnerabilities and threats

6 / 40
An administration office is going to determine the dangers to which it is exposed.

What do we call a possible event that can have a disruptive effect on the reliability of information?

A. dependency
B. threat
C. vulnerability
D. risk

7 / 40
What is the purpose of risk management?

A. To determine the probability that a certain risk will occur.
B. To determine the damage caused by possible security incidents.
C. To outline the threats to which IT resources are exposed.
D. To implement measures to reduce risks to an acceptable level.

8 / 40
A couple of years ago you started your company which has now grown from 1 to 20 employees. Your company's information is worth more and more and gone are the days when you could keep control yourself. You are aware that you have to take measures, but what should they be? You hire a consultant who advises you to start with a qualitative risk analysis.

What is a qualitative risk analysis?

A. This analysis follows a precise statistical probability calculation in order to calculate exact loss caused by damage.
B. This analysis is based on scenarios and situations and produces a subjective view of the possible threats.

9 / 40
There was a fire in a branch of the company Midwest Insurance. 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 for good.

What is an example of the indirect damage caused by this fire?

A. Melted backup tapes
B. Burned computer systems
C. Burned documents
D. Water damage due to the fire extinguishers

10 / 40
You are the owner of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks.

What is this risk strategy called?

A. Risk bearing
B. Risk avoidance
C. Risk neutral

11 / 40
What is an example of a human threat?

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

12 / 40
What is an example of a human threat?

A. a lightning strike
B. fire
C. phishing

13 / 40
You work in the office of a large company. You receive a call from a person claiming to be from the Helpdesk. He asks you for your password.

What kind of threat is this?

A. Natural threat
B. Organizational threat
C. Social Engineering

14 / 40
A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.

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

A. between threat and incident
B. between recovery and threat
C. between damage and recovery
D. between incident and damage

15 / 40
Information has a number of reliability aspects. Reliability is constantly being threatened. Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.

Which of these examples is a threat to integrity?

A. a loose cable
B. accidental alteration of data
C. private use of data

16 / 40
A member of staff denies sending a particular message.

Which reliability aspect of information is in danger here?

A. availability
B. correctness
C. integrity
D. confidentiality

17 / 40
How is the purpose of information security policy **best** described?

A. An information security policy documents the analysis of risks and the search for countermeasures.
B. An information security policy provides direction and support to the management 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.

18 / 40
A security incident regarding a webserver is reported to a helpdesk employee. His colleague has more experience on webservers, so he transfers the case to her.

Which term describes this transfer?

A. Functional escalation
B. Hierarchical escalation

19 / 40
A worker from an insurance company discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this. She 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 **most** 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
D. a list of people who were informed about the incident

20 / 40
In the incident cycle there are four successive steps.

Which step follows after the step Incident?

A. Threat
B. Damage
C. Recovery

21 / 40
Which measure 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

22 / 40
What is a repressive measure in case of a fire?

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

23 / 40
What is the goal of classification of information?

A. To create a manual about how to handle mobile devices
B. Applying labels making the information easier to recognize
C. Structuring information according to its sensitivity

24 / 40
Who is authorized to change the classification of a document?

A. The author of the document
B. The administrator of the document
C. The owner of the document
D. The manager of the owner of the document

25 / 40
The computer room is protected by a pass reader. Only the System Management department has a pass.

What type of security measure is this?

A. a corrective security measure
B. a physical security measure
C. a logical security measure
D. a repressive security measure

26 / 40
Strong authentication is needed to access highly protected areas. In case of strong authentication the identity of a person is verified by using three factors.

Which factor is verified when we must show our access pass?

A. something you are
B. something you have
C. something you know

27 / 40
In physical security multiple expanding zones (protection rings) can be applied in which different measures can be taken.

What is **not** a protection ring?

A. Building
B. Middle ring
C. Object
D. Outer ring

28 / 40
Which threat can occur as a result of the absence of a physical measure?

A. A user can view the files belonging to another user.
B. A server shuts down because of overheating.
C. A confidential document is left in the printer.
D. Hackers can freely enter the computer network.

29 / 40
Which security measure is a technical measure?

A. Allocating information to an owner
B. Encryption of files
C. Creating a policy defining what is and is not allowed in e-mail
D. Storing system management passwords in a safe

30 / 40
The backups of the central server are kept in the same locked room as the server.

What risk does the organization face?

A. If the server crashes, it will take a long time before the server is again operational.
B. In the event of fire it is impossible to get the system back to its former state.
C. No one is responsible for the backups.
D. Unauthorized persons have easy access to the backups.

31 / 40
Which type of malware builds a network of contaminated computers?

A. Logic Bomb
B. Storm Worm or Botnet
C. Trojan
D. Spyware

32 / 40
Within an organization the security officer detects that a workstation of an employee is infected with malicious software. The malicious software was installed due to a targeted Phishing attack.

Which action is the **most** beneficial to prevent such incidents in the future?

A. Implementing MAC technology
B. Start a security awareness program
C. Update the firewall rules
D. Update the signatures of the spam filter

33 / 40
You work in the IT department of a medium-sized company. Confidential information has come into the wrong hands several times. This has hurt the image of the company. You have been asked to propose organizational security measures for laptops at your company.

What is the **first** step that you should take?

A. Formulate a policy regarding mobile media (PDAs, laptops, smartphones, USB sticks)
B. Appoint security personnel
C. Encrypt the hard disks of laptops and USB sticks
D. Set up an access control policy

34 / 40
What is the name of the system that guarantees the coherence of information security in the organization?

A. Information Security Management System (ISMS)
B. Rootkit
C. Security regulations for special information for the government

35 / 40
What is 'establishing whether someone's identity is correct' called?

A. Authentication
B. Authorization
C. Identification

36 / 40
Why is it necessary to keep a disaster recovery plan up to date and to test it regularly?

A. In order to always have access to recent backups that are located outside the office.
B. In order to be able to cope with daily occurring faults.
C. Because otherwise, in the event of a far-reaching disruption, the measures taken and the incident procedures planned may not be adequate or may be outdated.
D. Because this is required by Personal Data Protection legislation.

37 / 40
On the basis of which legislation can someone request to inspect the data that has been registered about him or her?

A. Public records legislation
B. Personal data protection legislation
C. Computer criminality legislation
D. Government information (public access) legislation

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

A. Intellectual Property Rights
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Personal data protection legislation

39 / 40
You are the owner of the courier company SpeeDelivery. You employ a few people who, while waiting to make a delivery, can carry out other tasks. You notice, however, that they use this time to send and read their private mail and surf the Internet.

In legal terms, in which way can the use of the Internet and e-mail facilities be **best** regulated?

A. Installing an application that makes certain websites no longer accessible and that filters attachments in e-mails
B. Drafting a code of conduct for the use of the Internet and e-mail in which the rights and obligations of both the employer and staff are set down
C. Implementing privacy regulations
D. Installing a virus scanner

40 / 40
Under which condition is an employer permitted to check if Internet and e-mail services in the workplace are being used for private purposes?

A. The employer is permitted to check this if the employee is informed after each instance of checking.
B. The employer is permitted to check this if the employees are aware that this could happen.
C. The employer is permitted to check this if a firewall is also installed.

Answer Key

1 / 40
What is the relationship between data and information?

A. Data is structured information.

B. Information is the meaning and value assigned to a collection of data.

A. Incorrect. Information is structured data.
B. Correct. Information is data that has a meaning in some context for its receiver. (Chapter 3)

2 / 40
In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is not important for determining the value of data for an organization?

A. The content of data.

B. The degree to which missing, incomplete or incorrect data can be recovered.

C. The indispensability of data for the business processes.

D. The importance of the business processes that make use of the data.

A. Correct. The content of data does not determine its value. (Chapter 4)
B. Incorrect. Missing, incomplete or incorrect data that can be easily recovered is less valuable than data that is difficult or impossible to recover.
C. Incorrect. The indispensability of data for business processes in part determines the value.
D. Incorrect. Data critical to important business processes is therefore valuable.

3 / 40
A hacker gains access to a webserver and can view a file on the server containing credit card numbers.

Which of the Confidentiality, Integrity, Availability (CIA) principles of the credit card file are violated?

A. Availability

B. Confidentiality

C. Integrity

A. Incorrect. The hacker did not delete the file or denied access for authorized entities in any way, therefore the availability was not harmed.
B. Correct. The hacker was able to read the file (confidentiality). (Chapter 3)
C. Incorrect. There was no information altered in the credit card file; therefore the integrity of the file was not violated.

4 / 40
There is a network printer in the hallway of the company where you work. Many employees don’t pick up their printouts immediately and leave them on the printer.

What are the consequences of this to the reliability of the information?

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

A. Incorrect. The integrity of the information on the prints is still guaranteed, for it is on paper.
B. Incorrect. The information is still available in the system that was used to create and print it.
C. Correct. The information can end up or be read by persons who should not have access to the information. (Chapter 3)

5 / 40
A well-executed risk analysis provides a great deal of useful information. A risk analysis has four main objectives.

What is not one of the four main objectives of a risk analysis?

A. Identifying assets and their value
B. Implementing counter measures
C. Establishing a balance between the costs of an incident and the costs of a security measure
D. Determining relevant vulnerabilities and threats

A. Incorrect. This is one of the main objectives of a risk analysis.
B. Correct. This is not an objective of a risk analysis. Measures can be selected when in a risk analysis is determined which risks require a security measure. (Chapter 3)
C. Incorrect. This is one of the main objectives of a risk analysis.
D. Incorrect. This is one of the main objectives of a risk analysis.

6 / 40
An administration office is going to determine the dangers to which it is exposed.

What do we call a possible event that can have a disruptive effect on the reliability of information?

A. dependency
B. threat
C. vulnerability
D. risk

A. Incorrect. A dependency is not an event.
B. Correct. A threat is a possible event that can have a disruptive effect on the reliability of information. (Chapter 3)
C. Incorrect. Vulnerability is the degree to which an object is susceptible to a threat.
D. Incorrect. A risk is the average expected damage over a period of time as a result of one or more threats leading to disruption(s).

7 / 40
What is the purpose of risk management?

A. To determine the probability that a certain risk will occur.
B. To determine the damage caused by possible security incidents.
C. To outline the threats to which IT resources are exposed.
D. To implement measures to reduce risks to an acceptable level.

A. Incorrect. This is part of risk analysis.
B. Incorrect. This is part of risk analysis.
C. Incorrect. This is part of risk analysis.
D. Correct. The purpose of risk management is to reduce risks to an acceptable level. (Chapter 3)

8 / 40
A couple of years ago you started your company which has now grown from 1 to 20 employees. Your company's information is worth more and more and gone are the days when you could keep control yourself. You are aware that you have to take measures, but what should they be? You hire a consultant who advises you to start with a qualitative risk analysis.

What is a qualitative risk analysis?

A. This analysis follows a precise statistical probability calculation in order to calculate exact loss caused by damage.
B. This analysis is based on scenarios and situations and produces a subjective view of the possible threats.

A. Incorrect. In a quantitative risk analysis, an attempt is made to numerically determine the probabilities of various events and the likely extent of the losses if a particular event takes place.
B. Correct. A qualitative risk analysis involves defining the various threats, determining the extent of the vulnerabilities, and devising countermeasures, should an attack occur. (Chapter 3)

9 / 40
There was a fire in a branch of the company Midwest Insurance. 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 for good.

What is an example of the indirect damage caused by this fire?

A. Melted backup tapes
B. Burned computer systems
C. Burned documents
D. Water damage due to the fire extinguishers

A. Incorrect. Melted backup tapes are direct damage caused by the fire.
B. Incorrect. Burned computer systems are direct damage caused by the fire.
C. Incorrect. Burned documents 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. (Chapter 3)

10 / 40
You are the owner of the courier company SpeeDelivery. You have carried out a risk analysis and now want to determine your risk strategy. You decide to take measures for the large risks but not for the small risks.

What is this risk strategy called?

A. Risk bearing
B. Risk avoidance
C. Risk neutral

A. Correct. This means certain risks are accepted. (Chapter 3)
B. Incorrect. This means that measures are taken so that the threat is neutralized to such an extent that it no longer leads to an incident.
C. Incorrect. This means that the security measures are taken such that the threats either no longer manifest themselves, or if they do, the resulting damage is minimized.

11 / 40
What is an example of a human threat?

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

A. Correct. A USB-stick is always inserted by a person. Thus, if by doing so a virus enters the network, then it is a human threat. (Chapter 3)
B. Incorrect. Dust is not a human threat, but a non-human threat.
C. Incorrect. A leak is not a human threat, but a non-human threat.

12 / 40
What is an example of a human threat?

A. a lightning strike
B. fire
C. phishing

A. Incorrect. A lightning strike is an example of a non-human threat.
B. Incorrect. Fire is an example of a non-human threat.
C. Correct. Phishing (luring users to false websites) is one form of a human threat. (Chapter 3)

13 / 40
You work in the office of a large company. You receive a call from a person claiming to be from the Helpdesk. He asks you for your password.

What kind of threat is this?

A. Natural threat
B. Organizational threat
C. Social Engineering

A. Incorrect. A phone call is a human action so not a natural threat.
B. Incorrect. The term 'organizational threat' is not a common term for a kind of threat.
C. Correct. Using the right expressions or names of known people and their departments gives the impression of being a colleague trying to obtain company and trade secrets. You should check whether you are actually talking to the helpdesk. A helpdesk employee will never ask for your password. (Chapter 3)

14 / 40
A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.

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

A. between threat and incident
B. between recovery and threat
C. between damage and recovery
D. between incident and damage

A. Incorrect. Carrying out a stand-by arrangement without an incident is very expensive.
B. Incorrect. Recovery takes place after putting a stand-by arrangement into operation.
C. Incorrect. Damage and recovery are actually limited by the stand-by arrangement.
D. Correct. A stand-by arrangement is a corrective measure that is initiated in order to limit the damage. (Chapter 3)

15 / 40
Information has a number of reliability aspects. Reliability is constantly being threatened. Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.

Which of these examples is a threat to integrity?

A. a loose cable
B. accidental alteration of data
C. private use of data

A. Incorrect. A loose cable is a threat to the availability of information.
B. Correct. The unintended alteration of data is a threat to its integrity.
C. Incorrect. The use of data for private ends is a form of misuse and is a threat to confidentiality. (Chapter 3)

16 / 40
A member of staff denies sending a particular message.

Which reliability aspect of information is in danger here?

A. availability
B. correctness
C. integrity
D. confidentiality

A. Incorrect. Overloading the infrastructure is an example of a threat to availability.
B. Incorrect. Correctness is not a reliability aspect. It is a characteristic of integrity.
C. Correct. The denial of sending a message has to do with nonrepudiation, a threat to integrity. (Chapter 3)
D. Incorrect. Misuse and/or disclosure of data are threats to confidentiality.

17 / 40
How is the purpose of information security policy **best** described?

A. An information security policy documents the analysis of risks and the search for countermeasures.
B. An information security policy provides direction and support to the management 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 countermeasures is the purpose of risk analysis and risk management.
B. Correct. The security policy provides direction and support to the management regarding information security. (Chapter 5)
C. Incorrect. The security plan makes the information security policy concrete. The plan includes which measures have been chosen, who is responsible for what, the guidelines for the implementation of measures, etc.
D. Incorrect. The purpose of a threat analysis is to provide insight into threats and the possible consequences.

18 / 40
A security incident regarding a webserver is reported to a helpdesk employee. His colleague has more experience on webservers, so he transfers the case to her.

Which term describes this transfer?

A. Functional escalation
B. Hierarchical escalation

A. Correct. If the helpdesk employee is not able to deal with the incident personally, the incident can be reported to someone with more expertise who may be able to resolve the problem. This is called a functional (horizontal) escalation. (Chapter 16)
B. Incorrect. This is called a functional (horizontal) escalation. Hierarchical escalation is when a task is transferred to someone with more authority.

19 / 40
A worker from an insurance company discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this. She 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 most 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

D. a list of people who were informed about the incident

A. Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. (Chapter 16)
B. Incorrect. This is additional information that may be added later.
C. Incorrect. This is additional information that may be added later.
D. Incorrect. This is additional information that may be added later.

20 / 40
In the incident cycle there are four successive steps.

Which step follows after the step Incident?

A. Threat

B. Damage

C. Recovery

A. Incorrect. The damage follows after the incident. The correct order of steps is Threat, Incident, Damage, Recovery.
B. Correct. The order of steps in the incident cycle are: Threat, Incident, Damage, Recovery. (Chapter 16)
C. Incorrect. The damage follows the incident. The correct order of steps is Threat, Incident, Damage, Recovery.

21 / 40
Which measure 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

A. Incorrect. Via a logging system only after the incident is occurred can be researched what happened. This is a detective measure aimed at detecting incidents.
B. Incorrect. Shutting down all internet traffic is a repressive measure aimed at limiting an incident.
C. Correct. A safe is a preventive measure, which avoids damage can be done to the sensitive information stored in the safe. (Chapter 3)

22 / 40
What is a repressive measure in case of a fire?

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

A. Incorrect. Taking out an insurance protects against the financial consequences of a fire.
B. Correct. This repressive measure minimizes the damage caused by the fire. (Chapter 3)
C. Incorrect. This is not a repressive measure, it does not minimize the damage caused by the fire.

23 / 40
What is the goal of classification of information?

A. To create a manual about how to handle mobile devices
B. Applying labels making the information easier to recognize
C. Structuring information according to its sensitivity

A. Incorrect. Creating a manual has to do with user guidelines and is not classification of information.
B. Incorrect. Applying labels to information is designation, a special form of categorizing information which follows classification.
C. Correct. Classification of information is used to define the different levels of sensitivity into which information can be structured. (Chapter 3 and 8)

24 / 40
Who is authorized to change the classification of a document?

A. The author of the document
B. The administrator of the document
C. The owner of the document
D. The manager of the owner of the document

A. Incorrect. The author may change the content but not change the classification of a document.
B. Incorrect. The administrator may not change the classification of a document.
C. Correct. The owner must ensure the asset is classified or reclassified if necessary so is authorized to change the classification of a document. (Chapter 3 and 8)
D. Incorrect. The manager of the owner has no authority in this.

25 / 40
The computer room is protected by a pass reader. Only the System Management department has a pass.

What type of security measure is this?

A. a corrective security measure
B. a physical security measure
C. a logical security measure
D. a repressive security measure

A. Incorrect. A corrective security measure is a recovery measure.
B. Correct. This is a physical security measure. (Chapter 3 and 11)
C. Incorrect. A logical security measure controls the access to software and information, not the physical access to rooms.
D. Incorrect. A repressive security measure is intended to minimize the consequences of a disruption.

26 / 40
Strong authentication is needed to access highly protected areas. In case of strong authentication the identity of a person is verified by using three factors.

Which factor is verified when we must show our access pass?

A. something you are
B. something you have
C. something you know

A. Incorrect. An access pass is not an example of something that you are.
B. Correct. An access pass is an example of something that you have. (Chapter 11)
C. Incorrect. An access pass is not something that you know.

27 / 40
In physical security multiple expanding zones (protection rings) can be applied in which different measures can be taken.

What is not a protection ring?

A. Building
B. Middle ring
C. Object
D. Outer ring

A. Incorrect. A building is a valid zone and deals with access to the premises.
B. Correct. Protection rings: Outer ring (area around the premises), Building (access to the premises), Working space (the rooms in the premises, also known as 'Inner Ring'), Object (the asset that is to be protected).There is no such thing as a middle ring. (Chapter 11)
C. Incorrect. An object is a valid zone and deals with the asset that is to be protected.
D. Incorrect. An outer ring is a valid zone and deals with the area around the premises.

28 / 40
Which threat can occur as a result of the absence of a physical measure?

A. A user can view the files belonging to another user.
B. A server shuts down because of overheating.
C. A confidential document is left in the printer.
D. Hackers can freely enter the computer network.

A. Incorrect. Logical access control is a technical measure which prevents unauthorized access to documents of another user.
B. Correct. Physical security includes the protection of equipment through climate control (air conditioning, air humidity). (Chapter 11)
C. Incorrect. A security policy should cover the rules how to handle confidential documents. All employees should be aware of this policy and practice the rules. It is an organizational measure.
D. Incorrect. Preventing hackers to enter the computer or network is a technical measure.

29 / 40
Which security measure is a technical measure?

A. Allocating information to an owner
B. Encryption of files
C. Creating a policy defining what is and is not allowed in e-mail
D. Storing system management passwords in a safe

A. Incorrect. Allocating information to an owner is classification, which is an organizational measure.
B. Correct. This is a technical measure which prevents unauthorized persons from reading the information. (Chapter 6)
C. Incorrect. This is an organizational measure, a code of conduct that is written in the employment contract.
D. Incorrect. This is an organizational measure.

30 / 40
The backups of the central server are kept in the same locked room as the server.

What risk does the organization face?

A. If the server crashes, it will take a long time before the server is again operational.
B. In the event of fire it is impossible to get the system back to its former state.
C. No one is responsible for the backups.
D. Unauthorized persons have easy access to the backups.

A. Incorrect. On the contrary, this would help to make the system operational more quickly.
B. Correct. The chance that the back-ups may also be destroyed in a fire is very great. (Chapter 11)
C. Incorrect. The responsibility has nothing to do with the storage location.
D. Incorrect. The computer room is locked.

31 / 40
Which type of malware builds a network of contaminated computers?

A. Logic Bomb
B. Storm Worm or Botnet
C. Trojan
D. Spyware

A. Incorrect. A logic bomb is not always malware. It is a piece of code that is built into a software system.
B. Correct. A worm is a small computer program that purposely replicates itself, copies of the original are spread by making use of the network facilities of its host. (Chapter 12)
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 user.
D. Incorrect. Spyware is a computer program that collects information on the computer user and sends this information to another party.

32 / 40
Within an organization the security officer detects that a workstation of an employee is infected with malicious software. The malicious software was installed due to a targeted Phishing attack.

Which action is the most beneficial to prevent such incidents in the future?

A. Implementing MAC technology
B. Start a security awareness program
C. Update the firewall rules
D. Update the signatures of the spam filter

A. Incorrect. MAC is about access control; this does not prevent a user to be persuaded to execute some actions as a result from the targeted attack.
B. Correct. The underlying vulnerability of this threat is the unawareness of the user. Users are persuaded in these kinds of attacks to execute some code that violates the policy (e.g. install suspicious software). Addressing these kind of attacks in a security awareness program will reduce the chance of reoccurrence in the future. (Chapter 12)
C. Incorrect. Despite the firewall could e.g. block traffic that resulted from the installation of the malicious software. To prevent the threat from reoccurrence the firewall will not help.
D. Incorrect. The targeted attack does not necessary have to make use of e-mail. The attacker may for instance also use social media, or even the phone to make contact with the victim.

33 / 40
You work in the IT department of a medium-sized company. Confidential information has come into the wrong hands several times. This has hurt the image of the company. You have been asked to propose organizational security measures for laptops at your company.

What is the **first** step that you should take?

A. Formulate a policy regarding mobile media (PDAs, laptops, smartphones, USB sticks)
B. Appoint security personnel
C. Encrypt the hard disks of laptops and USB sticks
D. Set up an access control policy

A. Correct. The policy how to use mobile media is an organizational measure and security measures for laptops can be an obligation. (Chapter 6)
B. Incorrect. Appointing security personnel is a technical measure. When someone takes a laptop out the office the risk of leakage of information stays.
C. Incorrect. Encrypting the hard disks of laptops and USB sticks is a technical measure. This can be carried out based on an organizational measure.
D. Incorrect. Access control policy is an organizational measure, which only covers the access to buildings or IT-systems.

34 / 40
What is the name of the system that guarantees the coherence of information security in the organization?

A. Information Security Management System (ISMS)
B. Rootkit
C. Security regulations for special information for the government

A. Correct. The ISMS is described in ISO/IEC 27001. (Chapter 3)
B. Incorrect. A rootkit is a malicious set of software tools often used by a third party (usually a hacker).
C. Incorrect. This is a governmental set of rules how to handle special information.

35 / 40
What is 'establishing whether someone’s identity is correct' called?

A. Authentication
B. Authorization
C. Identification

A. Correct. Establishing whether someone’s identity is correct is called authentication. (Chapter 9)
B. Incorrect. When one is given the access rights for a computer or network is called authorization.
C. Incorrect. Identification is the process of making an identity known.

36 / 40
Why is it necessary to keep a disaster recovery plan up to date and to test it regularly?

A. In order to always have access to recent backups that are located outside the office.
B. In order to be able to cope with daily occurring faults.
C. Because otherwise, in the event of a far-reaching disruption, the measures taken and the incident procedures planned may not be adequate or may be outdated.
D. Because this is required by Personal Data Protection legislation.

A. Incorrect. This is one of the technical measures taken to recover a system.
B. Incorrect. For normal disruptions the measures usually taken and the incident procedures are sufficient.
C. Correct. A far-reaching disruption requires an up-to-date and tested plan. (Chapter 17)
D. Incorrect. Personal Data Protection legislation involves the privacy of personal data.

37 / 40
On the basis of which legislation can someone request to inspect the data that has been registered about him or her?

A. Public records legislation
B. Personal data protection legislation
C. Computer criminality legislation
D. Government information (public access) legislation

A. Incorrect. Public records legislation regulates the storage and destruction of archive documents.
B. Correct. The right to inspection is regulated in Personal data protection legislation. (Chapter 18)
C. Incorrect. Computer criminality legislation makes it easier to deal with offences perpetrated through advanced information technology. An example of a new offence is computer hacking.
D. Incorrect. Government information public access legislation regulates the inspection of written governmental documents. Personal data is not a governmental document.

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

A. Intellectual Property Rights
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Personal data protection legislation

A. Incorrect. This regulation is not related to information security for organizations.
B. Incorrect. This is a standard with guidelines for organizations how to deal with the set-up of an information security process.
C. Incorrect. This standard, also known as the 'Code of practice for Information Security', contains guidelines for information security policy and measures.
D. Correct. All organizations should have a policy and procedures for personal data protection, which should be known to everybody who processes personal data. (Chapter 18)

39 / 40
You are the owner of the courier company SpeeDelivery. You employ a few people who, while waiting to make a delivery, can carry out other tasks. You notice, however, that they use this time to send and read their private mail and surf the Internet.

In legal terms, in which way can the use of the Internet and e-mail facilities be **best** regulated?

A. Installing an application that makes certain websites no longer accessible and that filters attachments in e-mails
B. Drafting a code of conduct for the use of the Internet and e-mail in which the rights and obligations of both the employer and staff are set down
C. Implementing privacy regulations
D. Installing a virus scanner

A. Incorrect. Installing this kind of software regulates the use of internet and e-mail partly. It cannot regulate time spent on private use. This is a technical measure.
B. Correct. In a code of conduct the use of internet and e-mail can be documented which websites may or may not be visited and to which extend private use is permitted. These are internal regulations. (Chapter 18)
C. Incorrect. Privacy regulations only regulates the use of personal data of personnel and customers, not the use of internet and e-mail.
D. Incorrect. A virus scanner checks incoming e-mail and internet connections on malicious software. It does not regulate the use of internet and e-mail. It is a technical measure.

40 / 40
Under which condition is an employer permitted to check if Internet and e-mail services in the workplace are being used for private purposes?

A. The employer is permitted to check this if the employee is informed after each instance of checking.
B. The employer is permitted to check this if the employees are aware that this could happen.
C. The employer is permitted to check this if a firewall is also installed.

A. Incorrect. The employee does not have to be informed after each check.
B. Correct. The employees must know that the employer has the right to monitor the use of IT services. (Chapter 3 and 18)
C. Incorrect. A firewall protects against external intruders. This is not influencing the right of the employer to monitor the use of IT services.

Evaluation

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

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

Contact EXIN

www.exin.com

EXIN

YOUR ICT COMPETENCE PARTNER