EXIN Information Security Management ISO/IEC 27001 FOUNDATION

Certified by EXIN

Sample Exam

Edition 202101

Content

Introduction	4
Sample Exam	5
Answer Key	14
Evaluation	32

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
In order to take out a fire insurance, an organization 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 amount of storage required for the data
B) The degree to which missing data can be recovered
C) The indispensability of data for the business processes
D) The importance of the processes that use the data

2 / 40
Besides integrity and confidentiality, what is the third reliability aspect of information?

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

3 / 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.

4 / 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

5 / 40
What is the **best** description of 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

6 / 40
A database system has not had 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 patching?

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

7 / 40
An administration office is determining the dangers to which it is exposed.

What is a possible event that can have a disruptive effect on the reliability of information called?

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

8 / 40
What is a purpose of risk management?

A) To determine the probability that a certain risk will occur
B) To direct and control an organization with regard to risk
C) To investigate the damage caused by possible security incidents
D) To outline the threats to which IT resources are exposed

9 / 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.

10 / 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) Determine relevant vulnerabilities and threats
B) Establish a balance between the costs of an incident and the costs of a measure
C) Identify assets and their value
D) Implement measures and controls

11 / 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.

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

A) Burned computer systems
B) Burned documents
C) Melted back-up tapes
D) Water damage

12 / 40
An office is situated in an industrial area. The company next to the office works with flammable materials.

What is the relationship between the threat of fire and the risk of fire?

A) The threat of fire comes from the company next to the office, which poses a risk of fire by working with flammable materials in a vulnerable industrial area.
B) The threat of fire comes from the flammable materials, which poses a risk of fire to the office if the office has the vulnerability of not being fire-proof.
C) The threat of fire comes from the probability that the office will suffer damage because of the risk of fire the flammable materials pose.
D) The threat of fire comes from the vulnerable office in the industrial area, which is working close to a company that poses a risk of fire.

13 / 40
A fire breaks out in a branch office of a health insurance company. The employees are transferred to neighboring branches 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 / 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 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.

15 / 40
An employee from an insurance company discovers that the expiration date of a policy has been changed without his knowledge. He is the only person authorized to do this. He 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 names of the informed people
D) The PC number

16 / 40
Juliana is the owner of a courier company. She employs a few people who, while waiting to make a delivery, can carry out other tasks. She notices, however, that they use this time to send and read their private e-mail and surf the internet.

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

A) By blocking all websites
B) By drafting a code of conduct
C) By implementing privacy regulations
D) By installing a virus scanner

17 / 40
Which system guarantees the coherence of information security in the organization?

A) Information Security Management System (ISMS)
B) Intrusion detection system (IDS)
C) Rootkit
D) Security regulations for special information

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

Which term describes this transfer?

A) Functional escalation
B) Hierarchical escalation
C) Privilege escalation

19 / 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

20 / 40
What is a repressive measure 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

21 / 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

22 / 40
Which threat can occur as a result of the absence of a physical measure?

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

23 / 40
A 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

24 / 40
The back-ups of the central server are kept in the same locked room as the server.

What risk does the organization **most** likely face?

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

25 / 40
What is 'establishing whether someone's identity is correct' called?

A) Authentication
B) Authorization
C) Identification

26 / 40
What sort of security does a public key infrastructure (PKI) offer?

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

27 / 40
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. Therefore, the company is looking into organizational security measures to protect laptops at the company.

What is the **first** step that should be taken?

A) Appoint additional security employees
B) Encrypt storage devices and hard disks of laptops
C) Formulate a policy regarding mobile devices
D) Set up an access control policy

28 / 40
What is the **most** important reason for applying segregation of duties?

A) To create joint responsibility by all employees for the mistakes they make
B) To ensure that employees do the same work at the same time
C) To make clear who is responsible for what tasks and activities
D) To minimize the misuse of business assets or the chance of unauthorized or unintended changes

29 / 40
Which measure is a preventive measure?

A) Installing a logging system that enables changes in a system to be recognized
B) Putting all sensitive information in a safe after working hours
C) Shutting down all internet traffic after a hacker has gained access to the company systems

30 / 40
Which type of malware builds a network of contaminated computers?

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

31 / 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) Implement mandatory access control (MAC) technology
B) Start a security awareness program
C) Update the firewall rules
D) Update the signatures of the spam filter

32 / 40
What is the purpose of a disaster recovery plan (DRP)?

A) To identify the vulnerability underlying a disaster
B) To minimize the consequences in case of a disaster
C) To reduce the possibility of a disaster to occur
D) To restore the situation back to how this was before the disaster

33 / 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) Object ring
D) Outer ring

34 / 40
Measures taken to safeguard an information system from attacks.

Of which concept is this the definition?

A) Risk analysis
B) Risk management
C) Security controls

35 / 40
What is a characteristic of a security measure?

A) It describes a process for handling incidents.
B) It exposes an organization to possible damage.
C) It is put in place to mitigate against a potential risk.
D) It indicates the effect of uncertainty on objectives.

36 / 40
A data center uses an uninterruptible power supply (UPS) 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 UPS may run out of diesel and stop functioning after a couple of days, so its lifespan is limited.
D) The UPS must be powered by the power generator after a few hours, so only provides limited protection.

37 / 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) If a firewall is also installed.
B) If the employee is informed after each instance of checking.
C) If the employee is aware that this could happen.

38 / 40
Which standard or regulation is also known as the 'code of practice for information security controls'?

A) ISO/IEC 27001
B) ISO/IEC 27002
C) Payment Card Industry (PCI) compliance
D) Sarbanes-Oxley act

39 / 40
Legislation and regulations are important for the reliability of the information used within the organization.

What is the **first** step that an organization must take to become compliant?

A) Conducting a risk analysis to find out which legislation and regulations apply
B) Creating an acceptable use policy to make personnel aware of what they must do
C) Planning the compliance audits in advance in accordance with the PDCA cycle
D) Writing a policy that indicates which local laws and regulations must be followed

40 / 40
Which legislation may have an impact on information security requirements for all companies dealing with European Union (EU) residents?

A) European Convention on Human Rights (ECHR)
B) ISO/IEC 27001
C) NIST Cybersecurity Framework
D) Payment Card Industry Data Security Standard (PCI-DSS)

Answer Key

1 / 40
In order to take out a fire insurance, an organization 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 amount of storage required for the data
B) The degree to which missing data can be recovered
C) The indispensability of data for the business processes
D) The importance of the processes that use the data

A) Correct. The value of data is not determined by technical factors (such as storage) but by the significance it has to the users. (Literature: A, Chapter 4.10.4)
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.

2 / 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.
B) Correct. The three reliability aspects of information are availability, integrity, and confidentiality. (Literature: A, Chapter 3.3)
C) Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality.
D) Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality.

3 / 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)
C) Incorrect. The integrity of the information on the prints is still guaranteed, for it is on paper.

4 / 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 send to a recipient it becomes information for the recipient.
B) Correct. The invoice contains valuable data for the recipient, it has a meaning therefore it is information. (Literature: A, Chapter 4.10.5)
C) Incorrect. The invoice contains information for the recipient and not data.

5 / 40
What is the **best** description of 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 statement relates to 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 the means by which 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 4.11)
C) Incorrect. This is the focus of access management, which 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. Information analysis provides a clear picture of how an organization handles information – how the information flows through the organization.

6 / 40
A database system has not had 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 patching?

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 3.10)

7 / 40
An administration office is determining the dangers to which it is exposed.

What is a possible event that can have a disruptive effect on the reliability of information called?

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

A) Incorrect. A dependency is not an event.
B) Incorrect. A risk is the average expected damage over a period of time as a result of one or more threats leading to disruption.
C) Correct. A threat is a possible event that can have a disruptive effect on the reliability of information. (Literature: A, Chapter 3.9)
D) Incorrect. Vulnerability is the degree to which an object is susceptible to a threat.

8 / 40
What is a purpose of risk management?

A) To determine the probability that a certain risk will occur
B) To direct and control an organization with regard to risk
C) To investigate the damage caused by possible security incidents
D) To outline the threats to which IT resources are exposed

A) Incorrect. This is part of risk analysis.
B) Correct. Risk management are the coordinated activities to direct and control an organization with regard to risk. (Literature: A, Chapter 3.13)
C) Incorrect. This is part of risk analysis.
D) Incorrect. This is part of risk analysis.

9 / 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. Thus, if by doing so a virus enters the network, then it is a human threat. (Literature: A, Chapter 3.16)
C) Incorrect. Dust is not a human threat, but a non-human threat.

10 / 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) Determine relevant vulnerabilities and threats
B) Establish a balance between the costs of an incident and the costs of a measure
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 3.13.3)

11 / 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.

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

A) Burned computer systems
B) Burned documents
C) Melted back-up 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 back-up 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 3.17)

12 / 40
An office is situated in an industrial area. The company next to the office works with flammable materials.

What is the relationship between the threat of fire and the risk of fire?

A) The threat of fire comes from the company next to the office, which poses a risk of fire by working with flammable materials in a vulnerable industrial area.
B) The threat of fire comes from the flammable materials, which poses a risk of fire to the office if the office has the vulnerability of not being fire-proof.
C) The threat of fire comes from the probability that the office will suffer damage because of the risk of fire the flammable materials pose.
D) The threat of fire comes from the vulnerable office in the industrial area, which is working close to a company that poses a risk of fire.

A) Incorrect. The threat is the flammable materials, not the company. The flammable materials are not a risk.
B) Correct. The relationship is as explained in the answer. (Literature: A, Chapter 3.8, 3.9 and 3.10)
C) Incorrect. The probability that the office will suffer damage is a risk, not a threat. The flammable materials are a threat, not a risk.
D) Incorrect. The office is a vulnerability, not a threat.

13 / 40
A fire breaks out in a branch office of a health insurance company. The employees are transferred to neighboring branches 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 corrective measure that is initiated in order to limit the damage. (Literature: A, Chapter 16.5)
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 / 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 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 countermeasures 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 5.1.1)
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.

15 / 40
An employee from an insurance company discovers that the expiration date of a policy has been changed without his knowledge. He is the only person authorized to do this. He 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 names of the informed people
D) The PC number

A) Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. (Literature: A, Chapter 16.2)
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.

16 / 40
Juliana is the owner of a courier company. She employs a few people who, while waiting to make a delivery, can carry out other tasks. She notices, however, that they use this time to send and read their private e-mail and surf the internet.

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

A) By blocking all websites
B) By drafting a code of conduct
C) By implementing privacy regulations
D) By installing a virus scanner

A) Incorrect. Blocking all websites regulates the use of internet only. 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 extent private use is permitted. These are internal regulations. (Literature: A, Chapter 7)
C) Incorrect. Privacy regulations only regulate 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.

17 / 40
Which system guarantees the coherence of information security in the organization?

A) Information Security Management System (ISMS)
B) Intrusion detection system (IDS)
C) Rootkit
D) Security regulations for special information

A) Correct. The ISMS includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources. This creates coherence in the organization. (Literature: A, Chapter 3.1)
B) Incorrect. An IDS monitors the network traffic and host activities but does not create coherence.
C) Incorrect. A rootkit is a malicious set of software tools often used by a third party (usually a hacker) after having gained access to a system.
D) Incorrect. This is a governmental set of rules how to handle special information.

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

Which term describes this transfer?

A) Functional escalation
B) Hierarchical escalation
C) Privilege 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. (Literature: A, Chapter 16.1)
B) Incorrect. This is called a functional (horizontal) escalation. Hierarchical escalation is when a task is transferred to someone with more authority.
C) Incorrect. Privilege escalation is a step after gaining access to a computer system. This is typically a step during a hack or penetration test.

19 / 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 6.1)
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 to maintain policy that is derived from the security strategy.

20 / 40
What is a repressive measure 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 measure minimizes the damage caused by the fire. (Literature: A, Chapter 3.15.4)
B) Incorrect. This is not a repressive measure. 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.

21 / 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, a special form of categorizing information which follows on the classification of information.
B) Incorrect. Creating a manual has to do with 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 8.5)

22 / 40
Which threat can occur as a result of the absence of a physical measure?

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

A) 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. This is an organizational measure.
B) Correct. Physical security measures take care of the protection of equipment through climate control (air conditioning, air humidity). (Literature: A, Chapter 11.2)
C) Incorrect. Logical access control is a technical measure which prevents unauthorized access to documents of another user.
D) Incorrect. Preventing hackers to enter the computer or network is a technical measure.

23 / 40
A 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. This pass reader system does not recover the impact of an incident.
B) Correct. This is a physical security measure. (Literature: A, Chapter 11.1.2)
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.

24 / 40
The back-ups of the central server are kept in the same locked room as the server.

What risk does the organization **most** likely face?

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

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 high. (Literature: A, Chapter 3.6 and 11.2.1)
C) Incorrect. The responsibility has nothing to do with the storage location.
D) Incorrect. The server room should be locked.

25 / 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. (Literature: A, Chapter 9.2)
B) Incorrect. Authorization is the process of giving access rights for a computer or network.
C) Incorrect. Identification is the process of making an identity known.

26 / 40
What sort of security does a public key infrastructure (PKI) offer?

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

A) 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 10.2.3)
B) Incorrect. A PKI does not ensure making backups.
C) Incorrect. A PKI provides guarantees regarding which person or system belongs to a specific public key.

27 / 40
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. Therefore, the company is looking into organizational security measures to protect laptops at the company.

What is the **first** step that should be taken?

A) Appoint additional security employees
B) Encrypt storage devices and hard disks of laptops
C) Formulate a policy regarding mobile devices
D) Set up an access control policy

A) Incorrect. This might be a good solution in the end, but it is not a good thing to start with.
B) Incorrect. Encrypting the hard disks of laptops and storage devices is a technical measure. This can be carried out based on an organizational measure.
C) Correct. This policy is an organizational measure. (Literature: A, Chapter 6.2)
D) Incorrect. Access control policy is an organizational measure, which only covers the access to buildings or IT-systems. It does not solve the problem.

28 / 40
What is the **most** important reason for applying segregation of duties?

A) To create joint responsibility by all employees for the mistakes they make
B) To ensure that employees do the same work at the same time
C) To make clear who is responsible for what tasks and activities
D) To minimize the misuse of business assets or the chance of unauthorized or unintended changes

A) Incorrect. Segregation of duties separates tasks and responsibilities. It does not make a group of people jointly responsible.
B) 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.
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 6.1.1)

29 / 40
Which measure is a preventive measure?

A) Installing a logging system that enables changes in a system to be recognized
B) Putting all sensitive information in a safe after working hours
C) Shutting down all internet traffic after a hacker has gained access to the company systems

A) Incorrect. A logging system indicates an incident and helps research what happened after it happened, which is a detective measure.
B) Correct. A safe is a preventive measure, which avoids damage to the information stored in the safe. (Literature: A, Chapter 3.15.2)
C) Incorrect. Shutting down all internet traffic is a repressive measure aimed at limiting an incident.

30 / 40
Which type of malware builds a network of contaminated computers?

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

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) Correct. This is what a Worm does. (Literature: A, Chapter 12.5.7)
D) 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.

31 / 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) Implement mandatory access control (MAC) technology
B) Start a security awareness program
C) Update the firewall rules
D) Update the signatures of the spam filter

A) Incorrect. MAC addresses access control. This does not prevent a user from being 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. Addressing these kinds of attacks in a security awareness program will reduce the chance of reoccurrence in the future. (Literature: A, Chapter 12.4.3)
C) Incorrect. A firewall may be able to block traffic that resulted from the installation of the malicious software, but it does not prevent the threat from reoccurring.
D) Incorrect. The targeted attack does not necessarily have to make use of e-mail. The attacker can also use social media, or even the phone to contact the victim.

32 / 40
What is the purpose of a disaster recovery plan (DRP)?

A) To identify the vulnerability underlying a disaster
B) To minimize the consequences in case of a disaster
C) To reduce the possibility of a disaster to occur
D) To restore the situation back to how this was before the disaster

A) Incorrect. The DRP is aimed at minimizing the consequences of a disaster. The DRP has nothing to do with identifying vulnerabilities.
B) Correct. The DRP is aimed at minimizing the consequences of a disaster. (Literature: A, Chapter 17.2)
C) Incorrect. The DRP is aimed at limiting the consequences of a disaster and has nothing to do with reducing the possibility of a disaster occurring.
D) Incorrect. This is the objective of a business continuity plan (BCP).

33 / 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) Object 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 object. (Literature: A, Chapter 11.1.1)
C) Incorrect. The object 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.

34 / 40
Measures taken to safeguard an information system from attacks.

Of which concept is this the definition?

A) Risk analysis
B) Risk management
C) Security controls

A) Incorrect. Risk analysis is the process of defining and analyzing the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events.
B) Incorrect. Risk management is the process of planning, organizing, leading, and controlling the activities of an organization to minimize the effect of risk on an organization's capital and earnings.
C) Correct. Security controls are measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability (CIA) of the information system. (Literature: A, Chapter 3.14.1 and Appendix A)

35 / 40
What is a characteristic of a security measure?

A) It describes a process for handling incidents.
B) It exposes an organization to possible damage.
C) It is put in place to mitigate against a potential risk.
D) It indicates the effect of uncertainty on objectives.

A) Incorrect. This is a characteristic of information security incident management.
B) Incorrect. This is a characteristic of a vulnerability, which is a weakness of an asset or group of assets that can be exploited by one or more threats.
C) Correct. A countermeasure is put into place to mitigate against the potential risk. It may be a software configuration, a hardware device, or procedure that eliminates a vulnerability or reduces the likelihood that a threat agent will be able to exploit a vulnerability. (Literature: A, Chapter 3.12)
D) Incorrect. This is another explanation of a risk.

36 / 40
A data center uses an uninterruptible power supply (UPS) 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 UPS may run out of diesel and stop functioning after a couple of days, so its lifespan is limited.
D) The UPS must be powered by the power generator after a few hours, so only provides limited protection.

A) Incorrect. A power generator is not used to trigger the main power supply.
B) Correct. A UPS only protects for temporary power outages and surges, whereas a power generator protects for longer-duration outages. (Literature: A, Chapter 11.2.2)
C) Incorrect. Diesel is used to power the generator; a UPS is powered by batteries.
D) Incorrect. The UPS will only work for a short period of time but is not powered by the generator – the generator simply takes over from the UPS.

37 / 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) If a firewall is also installed.
B) If the employee is informed after each instance of checking.
C) If the employee is aware that this could happen.

A) Incorrect. A firewall protects against external intruders. This is not influencing the right of the employer to monitor the use of IT services.
B) Incorrect. The employee does not have to be informed after each check.
C) Correct. The employees must know that the employer has the right to monitor the use of IT services. (Literature: A, Chapter 7 and 18.2)

38 / 40
Which standard or regulation is also known as the 'code of practice for information security controls'?

A) ISO/IEC 27001
B) ISO/IEC 27002
C) Payment Card Industry (PCI) compliance
D) Sarbanes-Oxley act

A) Incorrect. This ISO standard is the standard for the Information Security Management System (ISMS).
B) Correct. This standard is also known as the code of practice for information security controls. (Literature: A, Chapter 18.1.4)
C) Incorrect. PCI compliance is a general standard for companies that process information of payment cards.
D) Incorrect. The American Sarbanes-Oxley Act is a US federal law that sets standards for all US public boards.

39 / 40
Legislation and regulations are important for the reliability of the information used within the organization.

What is the **first** step that an organization must take to become compliant?

A) Conducting a risk analysis to find out which legislation and regulations apply
B) Creating an acceptable use policy to make personnel aware of what they must do
C) Planning the compliance audits in advance in accordance with the PDCA cycle
D) Writing a policy that indicates which local laws and regulations must be followed

A) Incorrect. A risk analysis is carried out to find risks and define measures amongst other things. It is not used to find applicable legislation and regulations.
B) Incorrect. This step can only take place after knowing applicable law and regulations and incorporating these in a policy.
C) Incorrect. Audits to measure compliance can only be planned after is known what law and regulations are mandatory.
D) Correct. The first step for an organization is to produce a policy in which it declares that it must comply with the national and local legislation and regulations. (Literature: A, Chapter 18.1.1)

40 / 40
Which legislation may have an impact on information security requirements for all companies dealing with European Union (EU) residents?

A) European Convention on Human Rights (ECHR)
B) ISO/IEC 27001
C) NIST Cybersecurity Framework
D) Payment Card Industry Data Security Standard (PCI-DSS)

A) Correct. All EU member states are signatories of the ECHR. (Literature: A, Chapter 18.1.4)
B) Incorrect. Only organizations wanting to certify their information security management system (ISMS) need to conform to the requirements of ISO/IEC 27001.
C) Incorrect. NIST standards are only required for US Federal agencies and their suppliers.
D) Incorrect. Only organizations processing credit card data need to comply with PCI-DSS.

Evaluation

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

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

Contact EXIN

www.exin.com