information security

sample exam

ISFS.EN_1.1

Information Security Foundation based on ISO/IEC 27002
edition April 2009

content

EXIN International B.V.
Examination Institute for Information Science
Janssoenborch, Hoog Catharijne
Godebaldkwartier 365, 3511 DT Utrecht
P.O. Box 19147, 3501 DC Utrecht
The Netherlands
Telephone +31 30 234 48 25
Fax +31 30 231 59 86
E-mail info@exin.nl
Internet www.exin-exams.com

Introduction

This is the sample exam Information Security Foundation based on ISO/IEC 27002.

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 this exam is 60 minutes.

No rights may be derived from this information.

Good luck!

Sample exam

1 of 40

You have received a draft of your tax return from the accountant and you check whether the data is correct.

Which characteristic of reliability of information are you checking?

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

2 of 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 of 40

Our access to information is becoming increasingly easy. Still, information has to be reliable in order to be usable.

What is **not** a reliability aspect of information?

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

4 of 40

"Completeness" is part of which aspect of reliability of information?

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

5 of 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

6 of 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 use measures to reduce risks to an acceptable level.

7 of 40

Which statement about risk analysis is correct?

1. Risks that are stated in a risk analysis can be classified.
2. In a risk analysis all details have to be considered.
3. A risk analysis limits itself to availability.
4. A risk analysis is simple to carry out by completing a short standard questionnaire with standard questions.

A. 1
B. 2
C. 3
D. 4

8 of 40

Which of the examples given below can be classified as fraud?

1. Infecting a computer with a virus.
2. Carrying out an unauthorized transaction.
3. Tapping communication lines and networks.
4. Using the work internet for private ends.

A. 1
B. 2
C. 3
D. 4

9 of 40

A possible risk for a company is fire damage. If this threat occurs, that is to say that a fire actually breaks out, direct and indirect damage may result.

What is an example of direct damage?

A. a database is destroyed
B. image loss
C. loss of client trust
D. statutory obligations can no longer be met

10 of 40

In order to reduce risks, a company decides to opt for a strategy of a mix of measures. One of the measures is that a stand-by arrangement is organized for the company.

To which category of measures does a stand-by arrangement belong?

A. corrective measures
B. detective measures
C. preventive measures
D. repressive measures

11 of 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 of 40

What is an example of a human threat?

A. a lightning strike
B. fire
C. phishing

13 of 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 confidentiality?

A. a loose cable
B. accidental deletion of data
C. private use of data
D. falsifying data

14 of 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

15 of 40

In the incident cycle there are four successive steps.

What is the order of these steps?

A. Threat, Damage, Incident, Recovery
B. Threat, Incident, Damage, Recovery
C. Incident, Threat, Damage, Recovery
D. Incident, Recovery, Damage, Threat

16 of 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 lifecycle are such stand-by arrangements found?

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

17 of 40

How is the purpose of information security policy best described?

A. Policy documents the analysis of risks and the search for countermeasures.
B. Policy provides direction and support to the management regarding information security.
C. Policy makes the security plan concrete by providing it with the necessary details.
D. Policy provides insight into threats and the possible consequences.

18 of 40

The code of conduct for e-business is based on a number of principles.

Which of the following principles do **not** belong?

A. reliability
B. registration
C. confidentiality and privacy

19 of 40

A worker from insurance company Euregio 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 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 of 40

A company experiences the following incidents:
1. A smoke alarm does not work.
2. The network is hacked into.
3. Someone pretends to be a member of staff.
4. A file on the computer cannot be converted into a PDF file.

Which of these incidents is **not** a security incident?

A. 1
B. 2
C. 3
D. 4

21 of 40

Security measures can be grouped in various ways.

Which of the following is correct?

A. physical, logical, preventive
B. logical, repressive, preventive
C. organizational, preventive, corrective, physical
D. preventive, detective, repressive, corrective

22 of 40

A smoke alarm is placed in a computer room.

Under which category of security measures does this fall?

A. corrective
B. detective
C. organizational
D. preventive

23 of 40

The Information Security Officer (ISO) of insurance company Euregio wishes to have a list of security measures put together.

What does she first have to do before security measures can be selected?

A. Set up monitoring.
B. Carry out an evaluation.
C. Formulate information security policy.
D. Carry out a risk analysis.

24 of 40

What is the purpose of classifying information?

A. To determine what types of information may require different levels of protection.
B. To allocate information to an owner.
C. To reduce the risks of human error.
D. To prevent unauthorized access to information.

25 of 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 enter a personal identification number (PIN)?

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

26 of 40

Access to the computer room is closed off using 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

27 of 40

Four (4) staff members of the IT department share one (1) pass for the computer room.

What risk does this lead to?

A. If the power fails, the computers go off.
B. If fire breaks out the fire extinguishers can not be used.
C. If something disappears from the computer room it will not be clear who is responsible.
D. Unauthorized persons may gain access to the computer room without being seen.

28 of 40

In the reception hall of an administration office, there is a printer which all staff can use in case of emergency. The arrangement is that the printouts are to be collected immediately so that they cannot be taken away by a visitor.

What other risk for the company information does this situation have?

A. Files can remain in the memory of the printer.
B. Visitors would be able to copy and print out confidential information from the network.
C. The printer can become defective through excessive use, so that it is no longer available for use.

29 of 40

Which of the following security measures is a technical measure?

1. Allocating information to an owner
2. Encryption of files
3. Creating a policy defining what is and is not allowed in e-mail
4. Storing system management passwords in a safe

A. 1
B. 2
C. 3
D. 4

30 of 40

The backups of the central server are kept locked in the same enclosed 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 of 40

Which of the below technologies is malicious?

A. encryption
B. hash
C. Virtual Private Network (VPN)
D. viruses, worms and spyware

32 of 40

Which measure does **not** help against malicious software?

A. an active patch policy
B. an anti-spyware program
C. a spam filter
D. a password

33 of 40

What is an example of an organizational measure?

A. backup of data
B. encryption
C. segregation of duties
D. keeping network equipment and junction boxes in a locked room

34 of 40

Identification is establishing whether someone's identity is correct.

Is this statement correct?

A. yes
B. no

35 of 40

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

A. In order always to 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 the Personal Data Protection Act.

36 of 40

What is authorization?

A. The determination of a person's identity.
B. The registration of actions carried out.
C. The verification of a person's identity.
D. The granting of specific rights, such as selective access to a person.

37 of 40

Which important statutory norm in the area of information security does the government have to meet?

A. Dependency & Vulnerability analysis
B. ISO/IEC 20000
C. ISO/IEC 27002
D. national information security legislation or regulations

38 of 40

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

A. The Public Records Act
B. The Personal Data Protection Act
C. The Computer Criminality Act
D. The Government Information (Public Access) Act

39 of 40

The Code for Information Security (ISO/IEC 27002) is a description of a risk analysis method.

Is this statement correct?

A. yes
B. no

40 of 40

The Code for Information Security (ISO/IEC 27002) only applies to large companies.

Is this statement correct?

A. yes
B. no

Answer Key

1 of 40

You have received a draft of your tax return from the accountant and you check whether the data is correct.

Which characteristic of reliability of information are you checking?

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

A. Incorrect. Availability is the degree to which information is available for the users at the required times.
B. Incorrect. Exclusivity is a characteristic of confidentiality.
C. Correct. This concerns integrity. See section 4.5 of "*The basics of information security*".
D. Incorrect. This concerns the degree to which the access to information is restricted to only those who are authorized.

2 of 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. See section 4.3 of "*The basics of information security*".
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 of 40

Our access to information is becoming increasingly easy. Still, information has to be reliable in order to be usable.

What is **not** a reliability aspect of information?

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

A. Incorrect. Availability is a reliability aspect of information.
B. Incorrect. Integrity is a reliability aspect of information.
C. Correct. Quantity is not a reliability aspect of information. See section 4.5 of "*The basics of information security*".
D. Incorrect. Confidentiality is a reliability aspect of information.

4 of 40

"Completeness" is part of which aspect of reliability of information?

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

A. Incorrect. Information can be available without having to be complete.
B. Incorrect. Exclusivity is a characteristic of confidentiality.
C. Correct. Completeness is part of the integrity aspect. See section 4.5 of "*The basics of information security*".
D. Incorrect. Confidential information does not have to be complete.

5 of 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. See section 5 of "*The basics of information security*".
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).

6 of 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 use 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. See section 5 of "*The basics of information security*".

7 of 40

Which statement about risk analysis is correct?

1. Risks that are stated in a risk analysis can be classified.
2. In a risk analysis all details have to be considered.
3. A risk analysis limits itself to availability.
4. A risk analysis is simple to carry out by completing a short standard questionnaire with standard questions.

A. 1
B. 2
C. 3
D. 4

A. Correct. Not all risks are equal. As a rule the largest risks are tackled first. See section 5 of "*The basics of information security*".
B. Incorrect. It is impossible in a risk analysis to examine every detail.
C. Incorrect. A risk analysis considers all reliability aspects, including integrity and confidentiality along with availability.
D. Incorrect. In a risk analysis questions are seldom applicable to every situation.

8 of 40

Which of the examples given below can be classified as fraud?

1. Infecting a computer with a virus.
2. Carrying out an unauthorized transaction.
3. Tapping communication lines and networks.
4. Using the work internet for private ends.

A. 1
B. 2
C. 3
D. 4

A. Incorrect. A virus infection is classified as the threat "unauthorized change".
B. Correct. An unauthorized transaction is classified as "fraud". See section 10.6 of "*The basics of information security*".
C. Incorrect. Tapping is classified as the threat "disclosure".
D. Incorrect. Private use is classified as the threat "misuse".

9 of 40

A possible risk for a company is fire damage. If this threat occurs, that is to say that a fire actually breaks out, direct and indirect damage may result.

What is an example of direct damage?

A. a database is destroyed
B. image loss
C. loss of client trust
D. statutory obligations can no longer be met

A. Correct. A destroyed database is an example of direct damage. See section 5.5 of "*The basics of information security*".
B. Incorrect. Image loss is indirect damage.
C. Incorrect. Loss of client trust is indirect damage.
D. Incorrect. Being unable to meet statutory obligations is indirect damage.

10 of 40

In order to reduce risks, a company decides to opt for a strategy of a mix of measures. One of the measures is that a stand-by arrangement is organized for the company.

To which category of measures does a stand-by arrangement belong?

A. corrective measures
B. detective measures
C. preventive measures
D. repressive measures

A. Incorrect. Corrective measures focus on recovery after damage.
B. Incorrect. Detective measures only give a signal after detection.
C. Incorrect. Preventive measures are intended to avoid incidents.
D. Correct. Repressive measures, such as a stand-by arrangement, minimize the damage. See section 5.3.4 of "*The basics of information security*".

11 of 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. See section 5.4.1 of "*The basics of information security*".
B. Incorrect. Dust is not a human threat.
C. Incorrect. A leak is not a human threat.

12 of 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. See section 5.4.1 and 9.4.6 of "*The basics of information security*".

13 of 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 confidentiality?

A. a loose cable
B. accidental deletion of data
C. private use of data
D. falsifying data

A. Incorrect. A loose cable is a threat to the availability of information.
B. Incorrect. The unintended alteration of data is a threat to its integrity.
C. Correct. The use of data for private ends is a form of misuse and is a threat to confidentiality. See section 4.5 of "*The basics of information security*".
D. Incorrect. The falsification of data is a threat to its integrity.

14 of 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. See section 4.5 of "*The basics of information security*".
D. Incorrect. Misuse and/or disclosure of data are threats to confidentiality.

15 of 40

In the incident cycle there are four successive steps.

What is the order of these steps?

A. Threat, Damage, Incident, Recovery
B. Threat, Incident, Damage, Recovery
C. Incident, Threat, Damage, Recovery
D. Incident, Recovery, Damage, Threat

A. Incorrect. The damage follows after the incident.
B. Correct. The order of steps in the incident cycle are: Threat, Incident, Damage, Recovery. See section 6.4.4 of "*The basics of information security*".
C. Incorrect. The incident follows the threat.
D. Incorrect. Recovery is the last step.

16 of 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 lifecycle are such stand-by arrangements 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 there first being an incident is very expensive.
B. Incorrect. Recovery takes place after putting 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 repressive measure that is initiated in order to limit the damage. See section 6.4.4 and 9.3 of "*The basics of information security*".

17 of 40

How is the purpose of information security policy best described?

A. Policy documents the analysis of risks and the search for countermeasures.
B. Policy provides direction and support to the management regarding information security.
C. Policy makes the security plan concrete by providing it with the necessary details.
D. Policy provides insight into threats and the possible consequences.

A. Incorrect. This is the purpose of risk analysis and risk management.
B. Correct. The security policy provides direction and support to the management regarding information security. See section 9.1 of "*The basics of information security*".
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. This is the purpose of a threat analysis.

18 of 40

The code of conduct for e-business is based on a number of principles.

Which of the following principles do **not** belong?

A. reliability
B. registration
C. confidentiality and privacy

A. Incorrect. Reliability forms one of the bases of the code of conduct.
B. Correct. The code of conduct is based on the principles of reliability, transparency, confidentiality and privacy. Registration does not belong here. See section 9.4.12 of "*The basics of information security*".
C. Incorrect. The code of conduct is based on confidentiality and privacy among other things.

19 of 40

A worker from insurance company Euregio 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 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. See section 6.4.1 of "*The basics of information security*".
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 of 40

A company experiences the following incidents:
1. A smoke alarm does not work.
2. The network is hacked into.
3. Someone pretends to be a member of staff.
4. A file on the computer cannot be converted into a PDF file.

Which of these incidents is **not** a security incident?

A. 1
B. 2
C. 3
D. 4

A. Incorrect. A defective smoke alarm is an incident that can threaten the availability of data.
B. Incorrect. Hacking is an incident that can threaten the availability, integrity and confidentiality of data.
C. Incorrect. Misuse of identity is an incident that can threaten the aspect availability, integrity and confidentiality of data.
D. Correct. A security incident is an incident that threatens the confidentiality, reliability or availability of data. This is not a threat to the availability, integrity and confidentiality of data. See section 6.4 of "*The basics of information security*".

21 of 40

Security measures can be grouped in various ways.

Which of the following is correct?

A. physical, logical, preventive
B. logical, repressive, preventive
C. organizational, preventive, corrective, physical
D. preventive, detective, repressive, corrective

A. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
B. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
C. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
D. Correct. Preventive/detective/repressive/corrective is one appropriate group, as is organizational/logical/physical. See section 5.3 of "*The basics of information security*".

22 of 40

A smoke alarm is placed in a computer room.

Under which category of security measures does this fall?

A. corrective
B. detective
C. organizational
D. preventive

A. Incorrect. A smoke alarm detects and then sends an alarm, but does not take any corrective action.
B. Correct. A smoke alarm only has a signalling function; after the alarm is given, action is still required. See section 5.3 of "*The basics of information security*".
C. Incorrect. Only the measures that follow a smoke alarm signal are organizational; the placing of a smoke alarm is not organizational.
D. Incorrect. A smoke alarm does not prevent fire and is therefore not a preventive measure.

23 of 40

The Information Security Officer (ISO) of insurance company Euregio wishes to have a list of security measures put together.

What does she first have to do before security measures can be selected?

A. Set up monitoring.
B. Carry out an evaluation.
C. Formulate information security policy.
D. Carry out a risk analysis.

A. Incorrect. Monitoring is a possible measure.
B. Incorrect. Evaluation happens after the list of measures is assembled.
C. Incorrect. An information security policy is important, but is not necessary in order to select measures.
D. Correct. Before security measures can be selected, Euregio must know their risks to determine which risks require a security measure. See section 5 of "*The basics of information security*".

24 of 40

What is the purpose of classifying information?

A. To determine what types of information may require different levels of protection.
B. To allocate information to an owner.
C. To reduce the risks of human error.
D. To prevent unauthorized access to information.

A. Correct. The purpose of classifying information is to maintain an adequate protection. See section 6.3 of "*The basics of information security*".
B. Incorrect. Allocating information to an owner is the means of classification and not the purpose.
C. Incorrect. Reducing the risks of human error is part of the security requirements of the staff.
D. Incorrect. Preventing unauthorized access to information is part of access security.

25 of 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 enter a personal identification number (PIN)?

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

A. Incorrect. A PIN code is not an example of something that you are.
B. Incorrect. A PIN code is not something that you have.
C. Correct. A PIN code is something that you know. See section 7.2.2.1 of "*The basics of information security*".

26 of 40

Access to the computer room is closed off using 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. See section 7 of "*The basics of information security*".
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.

27 of 40

Four (4) staff members of the IT department share one (1) pass for the computer room.

What risk does this lead to?

A. If the power fails, the computers go off.
B. If fire breaks out the fire extinguishers can not be used.
C. If something disappears from the computer room it will not be clear who is responsible.
D. Unauthorized persons may gain access to the computer room without being seen.

A. Incorrect. Computers going off as a result of a power failure has nothing to do with access management.
B. Incorrect. Even with one pass, the IT staff can put out a fire with a fire extinguisher.
C. Correct. Though it would be clear that someone from the IT department had been inside, it would not be certain who. See section 7.2 of "*The basics of information security*".
D. Incorrect. No one has access to the computer room without a pass.

28 of 40

In the reception hall of an administration office, there is a printer which all staff can use in case of emergency. The arrangement is that the printouts are to be collected immediately so that they cannot be taken away by a visitor.

What other risk for the company information does this situation have?

A. Files can remain in the memory of the printer.
B. Visitors would be able to copy and print out confidential information from the network.
C. The printer can become defective through excessive use, so that it is no longer available for use.

A. Correct. If files remain in the memory they can be printed off and taken away by any passerby. See section 9.4.11 of "*The basics of information security*".
B. Incorrect. It is not possible to use a printer to copy information from the network.
C. Incorrect. The unavailability of a printer does not form a risk for company information.

29 of 40

Which of the following security measures is a technical measure?

1. Allocating information to an owner
2. Encryption of files
3. Creating a policy defining what is and is not allowed in e-mail
4. Storing system management passwords in a safe

A. 1
B. 2
C. 3
D. 4

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. See section 8.3 of "*The basics of information security*".
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 of 40

The backups of the central server are kept locked in the same enclosed 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 backups may also be destroyed in a fire is very great. See section 9.4.7 of "*The basics of information security*".
C. Incorrect. The responsibility has nothing to do with the storage location.
D. Incorrect. The computer room is locked.

31 of 40

Which of the below technologies is malicious?

A. encryption
B. hash
C. Virtual Private Network (VPN)
D. viruses, worms and spyware

A. Incorrect. Encryption is making information unreadable to anyone except those possessing special knowledge, usually referred to as a key.
B. Incorrect. Hash is a method for encrypting information.
C. Incorrect. VPN is a safe network connection over Internet.
D. Correct. These are all forms of malware, which establishes itself unrequested on a computer for malicious purposes. See section 9.4.6 of "*The basics of information security*".

32 of 40

Which measure does **not** help against malicious software?

A. an active patch policy
B. an anti-spyware program
C. a spam filter
D. a password

A. Incorrect. Malware often makes use of programming faults in popular software. Patches repair security leaks in the software, thereby reducing the chance of infection by malware.
B. Incorrect. Spyware is a malicious program that collects confidential information on the computer and then distributes it. An anti-spyware program can detect this malicious software on the computer.
C. Incorrect. Spam is unrequested e-mail. It is often simple advertising but can also have malicious software attached or a hyperlink to a web site with malicious software. A spam filter removes spam.
D. Correct. A password is a means of authentication. It does not block any malicious software. See section 8.1.2.1 of "*The basics of information security*".

33 of 40

What is an example of an organizational measure?

A. backup of data
B. encryption
C. segregation of duties
D. keeping network equipment and junction boxes in a locked room

A. Incorrect. Backing up data is a technical measure.
B. Incorrect. Encryption of data is a technical measure.
C. Correct. Segregation of duties is an organizational measure. The initiation, execution and control duties are allocated to different people. For example, the transfer of a large amount of money is prepared by a clerk, the financial director carries out the payment and an accountant audits the transaction. See section 9.4.3 of "*The basics of information security*".
D. Incorrect. Locking rooms is a physical security measure.

34 of 40

Identification is establishing whether someone's identity is correct.

Is this statement correct?

A. yes
B. no

A. Incorrect. Identification is the process of making an identity known.
B. Correct. Establishing whether someone's identity is correct is called authentication. See section 8.1 of "*The basics of information security*".

35 of 40

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

A. In order always to 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 the Personal Data Protection Act.

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. See section 9.3 of "*The basics of information security*".
D. Incorrect. The Personal Data Protection Act involves the privacy of personal data.

36 of 40

What is authorization?

A. The determination of a person's identity.
B. The registration of actions carried out.
C. The verification of a person's identity.
D. The granting of specific rights, such as selective access to a person.

A. Incorrect. The determination of a person's identity is called identification.
B. Incorrect. The registration of actions carried out is called logging.
C. Incorrect. The verification of a person's identity is called authentication.
D. Correct. The granting of specific rights, such as selective access to a person is called authorization. See section 8.1 of "*The basics of information security*".

37 of 40

Which important statutory norm in the area of information security does the government have to meet?

A. Dependency & Vulnerability analysis
B. ISO/IEC 20000
C. ISO/IEC 27002
D. national information security legislation or regulations

A. Incorrect. Dependency & Vulnerability analysis is a risk analysis method.
B. Incorrect. ISO/IEC 20000 is a standard for organizing IT Service Management and is not compulsory.
C. Incorrect. ISO/IEC 27002 is the Code for Information Security. It is a guideline for organizing Information Security and is not compulsory.
D. Correct. National information security legislation or regulations are intended for all national governments and are obligatory. See section 10 of "*The basics of information security*".

38 of 40

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

A. The Public Records Act
B. The Personal Data Protection Act
C. The Computer Criminality Act
D. The Government Information (Public Access) Act

A. Incorrect. The Public Records Act regulates the storage and destruction of archive documents.
B. Correct. The right to inspection is regulated in the Personal Data Protection Act. See section 10.5 of "*The basics of information security*".
C. Incorrect. The Computer Criminality Act is a change to the Criminal Code and Code of Criminal Procedure to make it easier to deal with offences perpetrated through advanced information technology. An example of a new offence is computer hacking.
D. Incorrect. The Government Information Public Access Act regulates the inspection of written governmental documents. Personal data is not a governmental document.

39 of 40

The Code for Information Security (ISO/IEC 27002) is a description of a risk analysis method.

Is this statement correct?

A. yes
B. no

A. Incorrect. The Code for Information Security is a collection of measures.
B. Correct. The Code for Information Security can be used in a risk analysis but is not a method.
See section 9.1 of "*The basics of information security*".

40 of 40

The Code for Information Security (ISO/IEC 27002) only applies to large companies.

Is this statement correct?

A. yes
B. no

A. Incorrect. The Code for Information Security is applicable to all types of organizations, large and small.
B. Correct. The Code for Information Security is applicable to all types of organizations, large and small. See section 9.1 of "*The basics of information security*".

Evaluation

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

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

number	answer	points
21	**D**	1
22	**B**	1
23	**D**	1
24	**A**	1
25	**C**	1
26	**B**	1
27	**C**	1
28	**A**	1
29	**B**	1
30	**B**	1
31	**D**	1
32	**D**	1
33	**C**	1
34	**B**	1
35	**C**	1
36	**D**	1
37	**D**	1
38	**B**	1
39	**B**	1
40	**B**	1