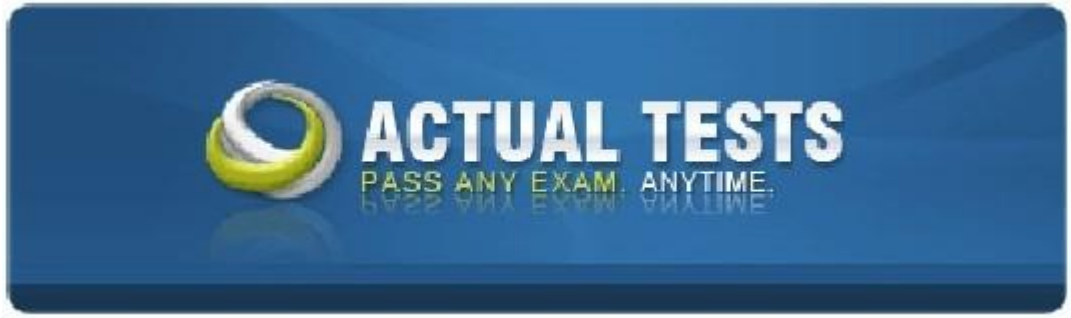
EX0-105 formatted (with explanations)

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exin EX0-105



EX0-105 Information Security Foundation based on

ISO/IEC 27002

Practice Test
Version 1.0
Exin EX0-105: Practice Exam

Exam A

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Why is air-conditioning placed in the server room?

A. In the server room the air has to be cooled and the heat produced by the equipment has to be extracted. The air in the room is also dehumidified and filtered.
B. When a company wishes to cool its offices, the server room is the best place. This way, no office space needs to be sacrificed for such a large piece of equipment.
C. It is not pleasant for the maintenance staff to have to work in a server room that is too warm.
D. Backup tapes are made from thin plastic which cannot withstand high temperatures.
Therefore, if it gets too hot in a server room, they may get damaged.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The owner of a business asset assigns an appropriate grading in accordance with an agreed list of classifications. The classification indicates the form of security that is necessary. This is determined in part by the sensitivity, value, statutory requirements and importance to the organization. The classification is in accordance with the manner in which the business asset is used in the business. The owner of the business asset must ensure it is reclassified if necessary. If business assets within an organization have been classified, only the owner is able to lower this classification (the grading) or give permission to do so.

QUESTION 4
The company Midwest Insurance has taken many measures to protect its information. It uses an Information Security Management System, the input and output of data in applications is validated, confidential documents are sent in encrypted form and staff use tokens to access information systems. Which of these is not a technical measure?

A. Information Security Management System
B. The use of tokens to gain access to information systems
C. Validation of input and output data in applications
D. Encryption of information

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Technical measures in automated environments are called IT security measures and are applied in the IT infrastructure
8.3 Logical access control
8.3.5 Granting access
Granting access to authorized users involves a number of steps which include identification of the user, authentication of this user and authorizing the user to access an asset. Identification is the first step in the process to granting access. In identification a person presents a token, for example an account number or username.

8.4 Security requirements for information systems
8.4.2. Validation of input and output data

8.5 Cryptography
The main reason to use cryptography is often seen as a means to keep information confidential

QUESTION 5
What is an example of a physical security measure?

A. A code of conduct that requires staff to adhere to the clear desk policy, ensuring that confidential information is not left visibly on the desk at the end of the work day
B. An access control policy with passes that have to be worn visibly
C. The encryption of confidential information
D. Special fire extinguishers with inert gas, such as Argon

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Physical security includes the protection of equipment through climate control (air conditioning, air humidity), the use of special fire extinguishers and the provision of clean' energy. Clean energy refers to the prevention of peaks and troughs (dirty energy) in the power supply and the fact that the power supply is filtered.

QUESTION 6
What physical security measure is necessary to control access to company information?

A. Air-conditioning
B. Username and password
C. The use of break-resistant glass and doors with the right locks, frames and hinges
D. Prohibiting the use of USB sticks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Physical security uses various types of sensors. The most common are:
- Passive infrared detection - these sensors are usually used indoors and detect temperature changes within a certain distance from the sensor;
- Cameras - these sensors record images which can be viewed at a later time. Certain smart software allows automatic checks to be carried out;
- Vibration detection - these sensors detect vibrations;
- Glass break sensors - these sensors detect when a window has been broken;
- Magnetic contacts - these sensors detect when a door or window is opened.

QUESTION 7
Why do organizations have an information security policy?

A. In order to demonstrate the operation of the Plan-Do-Check-Act cycle within an organization.
B. In order to ensure thatstaff do not break any laws.
C. In order to give direction to how information security is set up within an organization.
D. In order to ensure that everyone knows who is responsible for carrying out the backup procedures.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
9.2.1 Information security policy
By establishing a policy for the security of information, management provides direction and support to the organization. This policy must be written in accordance with the business requirements as well as the relevant legislation and regulations.

QUESTION 8
You work in the IT department of a medium-sized company. Confidential information has got 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 drives of laptops and USB sticks
D. Set up an access control policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
You work for a large organization. You notice that you have access to confidential information that you should not be able to access in your position. You report this security incident to the helpdesk. The incident cycle isinitiated. What are the stages of the security incident cycle?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The incident cycle has the following stages: threat, incident, damage and recovery.
Security measures are aimed at a certain moment in the incident cycle. The measures are intended to prevent incidents (preventive) or reduce the threats (reductive), detect incidents (detective), respond to incidents, stop threats (repressive) and to correct damage (corrective).
The measures are taken in order to ensure the availability, integrity and confidentiality of company information.

QUESTION 10
Your organization has an office with space for 25 workstations. These workstations are all fully equipped and in use. Due to a reorganization 10 extra workstations are added, 5 of which are used for a call centre 24 hours per day. Five workstations must always be available. What physical security measures must be taken in order to ensure this?

A. Obtain an extra office and set up 10 workstations. You would therefore have spare equipment that can be used to replace any non-functioning equipment.
B. Obtain an extra office and set up 10 workstations. Ensure that there are security personnel both in the evenings and at night, so that staff can work there safely and securely.
C. Obtain an extra office and connect all 10 new workstations to an emergency power supply and UPS (Uninterruptible Power Supply). Adjust the access control system to the working hours of the new staff. Inform the building security personnel that work will also be carried out in the evenings and at night.
D. Obtain an extra office and provide a UPS (Uninterruptible Power Supply) for the five most important workstations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Physical security includes the protection of equipment through climate control (air conditioning, air humidity), the use of special fire extinguishers and the provision of clean' energy. Clean energy refers to the prevention of peaks and troughs (dirty energy) in the power supply and the fact that the power supply is filtered.

QUESTION 11
Which of the following measures 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
D. Classifying a risk as acceptable because the cost of addressing the threat is higher than the value of the information at risk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Prevention makes it impossible for the threat to occur.
Examples in IT security are: disconnect Internet connections and internal network connections.
In physical security: closing doors to prevent people entering the building, though this countermeasure is not very practical. There are other preventive measures that are more practical. For example, placing sensitive information after office hours in a safe. Another example is video surveillance with stickers on the windows informing people they are being monitored.

QUESTION 12
What is a risk analysis used for?

A. A risk analysis is used to express the value of information for an organization in monetary terms.
B. A risk analysis is used to clarify to management their responsibilities.
C. A risk analysis is used in conjunction with security measures to reduce risks to an acceptable level.
D. A risk analysis is used to ensure that security measures are deployed in a cost-effective and timely fashion.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The purpose of carrying out a risk analysis is to clarify which threats are relevant to the operational processes and to identify the associated risks. The appropriate security level, along with the associated security measures, can then be determined.
A risk analysis is used to ensure that the security measures are deployed in a cost-effective and timely manner, and consequently provide an effective answer to the threats.

The purpose of risk management (not risk analysis) is to reduce risks to an acceptable level.

QUESTION 13
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. Determining the costs of threats
C. Establishing a balance between the costs of an incident and the costs of a security measure
D. Determining relevant vulnerabilities and threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A risk analysis has four main objectives:
- To identify assets and their value;
- To determine vulnerabilities and threats;
- To determine the risk that threats will become a reality and disrupt the operational process;
- To determine a balance between the costs of an incident and the costs of a security measure.

QUESTION 14
What is an example of a security incident?

A. The lighting in the department no longer works.
B. A member of staff loses a laptop.
C. You cannot set the correct fonts in your word processing software.
D. A file is saved under an incorrect name.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following measures is a corrective measure?

A. Incorporating an Intrusion Detection System (IDS) in the design of a computer centre
B. Installing a virus scanner in an information system
C. Making a backup of the data that has been created or altered that day
D. Restoring a backup of the correct database after a corrupt copy of the database was written over the original

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Corrective countermeasures are aimed at recovering from the damage caused by an incident

QUESTION 16
We can acquire and supply information in various ways. The value of the information depends on whether it is reliable. What are the reliability aspects of information?

A. Availability, Information Value and Confidentiality
B. Availability, Integrity and Confidentiality
C. Availability, Integrity and Completeness
D. Timeliness, Accuracy and Completeness

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A security program may have several large and small objectives, but the most important principles in all security programs are confidentiality (exclusivity), integrity and availability. These are referred to as the CIA triangle.

QUESTION 17
Your company has to ensure that it meets the requirements set down in personal data protection legislation. What is the first thing you should do?

A. Make the employees responsible for submitting their personal data.
B. Translate the personal data protection legislation into a privacy policy that is geared to the company and the contracts with the customers.
C. Appoint a person responsible for supporting managers in adhering to the policy.
D. Issue a ban on the provision of personal information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
What sort of security does a Public Key Infrastructure (PKI) offer?

A. It provides digital certificates which can be used to digitally sign documents. Such signatures irrefutably determine from whom a document was sent.
B. Having a PKI shows customers that a web-based business is secure.
C. By providing agreements, procedures and an organization structure, a PKI defines which person or which system belongs to which specific public key.
D. A PKI ensures that backups of company data are made on a regular basis.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
PKI is based on public key cryptography, and includes much more than just the cryptography. 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.

QUESTION 19
An employee in the administrative department of Smiths Consultants Inc. finds out that the expiry date of a contract with one of the clients is earlier than the start date. What type of measure could prevent this error?

A. Availability measure
B. Integrity measure
C. Organizational measure
D. Technical measure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Applications (software, computer programs) must work reliably, which means that they have consistent intended behaviour and results. A program that causes errors, allows data to be lost, or enables unauthorized persons to make changes or misuse information, could result in a significant risk for an organization. Application systems and applications that have been developed for the user should incorporate suitable protective measures. Such protective measures concern the validation of the data that is entered, the internal processing and the output data. This means that the information has to be entered in such a manner that the data can be checked to see whether it is correct.

QUESTION 20
What is the greatest risk for an organization if no information security policy has been defined?

A. If everyone works with the same account, it is impossible to find out who worked on what.
B. Information security activities are carried out by only a few people.
C. Too many measures are implemented.
D. It is not possible for an organization to implement information security in a consistent manner.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is the objective of classifying information?

A. Authorizing the use of an information system
B. Creating a label that indicates how confidential the information is
C. Defining different levels of sensitivity into which information may be arranged
D. Displaying on the document who is permitted access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Classification is used to define the different levels of sensitivity into which information may be structured;
Grading is the act of assigning the appropriate classification - such as secret, confidential or public - to specific information. This term is used often within the government;

QUESTION 22
What do employees need to know to report a security incident?

A. How to report an incident and to whom.
B. Whether the incident has occurred before and what was the resulting damage.
C. The measures that should have been taken to prevent the incident in the first place.
D. Who is responsible for the incident and whether it was intentional.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
The purpose of the incident management process is to ensure that incidents and weaknesses that are related to information systems are known so that appropriate measures can be taken in a timely manner.
Staff, temporary personnel and external users should all be made aware of the procedures for reporting the various types of incidents and weaknesses that can have an influence on the reliability of the information and the security of the business assets.
Staff and users should be required to report all incidents and weaknesses as quickly as possible to the service desk or a contact person.

QUESTION 23
You have just started working at a large organization. You have been asked to sign a code of conduct as well as a contract. What does the organization

wish to achieve with this?

A. A code of conduct helps to prevent the misuse of IT facilities.
B. A code of conduct is a legal obligation that organizations have to meet.
C. A code of conduct prevents a virus outbreak.
D. A code of conduct gives staff guidance on how to report suspected misuses of IT facilities.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
All personnel are responsible for information security. This responsibility must be made clear in the employment contract. The staff manual should contain a code of conduct and the sanctions that are imposed in the event of non-compliance and if incidents arise as a result.

QUESTION 24
Peter works at the company Midwest Insurance. His manager, Linda, asks him to send the terms and conditions for a life insurance policy to Rachel, a client. Who determines the value of the information in the insurance terms and conditions document?

A. The recipient, Rachel
B. The person who drafted the insurance terms and conditions
C. The manager, Linda
D. The sender, Peter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Information is knowledge that someone has acquired. While some people may consider a particular set of data uninteresting, others may be able to extract valuable information from it. The value of information is, therefore, determined by the value that the recipient attaches to it.

QUESTION 25
When we are at our desk, we want the information system and the necessary information to be available. We want to be able to work with the computer and access the network and our files.
What is the correct definition of availability?

A. The degree to which the system capacity is enough to allow all users to work with it
B. The degree to which the continuity of an organization is guaranteed
C. The degree to which an information system is available for the users

D. The total amount of time that an information system is accessible to the users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when needed. In addition this concept guarantees that the security services that the security practitioner requires are in working order.

QUESTION 26
What is an example of a non-human threat to the physical environment?

A. Fraudulent transaction
B. Corrupted file
C. Storm
D. Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
In most organizations, access to the computer or the network is granted only after the user has entered a correct username and password. This process consists of 3 steps: identification, authentication and authorization. What is the purpose of the second step, authentication?

A. In the second step, you make your identity known, which means you are given access to the system.
B. The authentication step checks the username against a list of users who have access to the system.
C. The system determines whether access may be granted by determining whether the token used is authentic.
D. During the authentication step, the system gives you the rights that you need, such as being able to read the data in the system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Granting access to authorized users involves a number of steps which include identification of the user, authentication of this user and authorizing the

user to access an asset. Identification is the first step in the process to granting access. In identification a person presents a token, for example an account number or username. The system then needs to determine whether the token is authentic. To determine the authenticity of, for example, a username, the system checks if the username exists within the system. If the username exists the user is requested to give a password. The systems tests if the password is registered with the given username. If both these tests are valid, a user is authenticated. In this example, authenticating the username is based on its existence in the system and a valid password. From this information it can be derived that a valid user is requesting access. Subsequently the system checks the resources to which access may be granted based on the permissions attached to authenticated user.

QUESTION 28
Which of these is not malicious software?

A. Phishing
B. Spyware
C. Virus
D. Worm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Phishing is a form of Internet fraud. Typically the victim will receive an email asking him or her to check or confirm an account with a bank or service provider. Sometimes instant messaging is used and even telephone contact has been tried. It is difficult to catch up with the perpetrators of phishing. Internet users have to remain particularly vigilant and must never respond to an email request to transfer money or submit personal (financial) information, such as bank account numbers, PIN codes or credit card details.

QUESTION 29
Some threats are caused directly by people, others have a natural cause. What is an example of an intentional human threat?

A. Lightning strike
B. Arson
C. Flood
D. Loss of a USB stick

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

What is the definition of the Annual Loss Expectancy?

A. The Annual Loss Expectancy is the amount of damage that can occur as a result of an incident during the year.
B. The Annual Loss Expectancy is the size of the damage claims resulting from not having carried out risk analyses effectively.
C. The Annual Loss Expectancy is the average damage calculated by insurance companies for businesses in a country.
D. The Annual Loss Expectancy is the minimum amount for which an organization must insure itself.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
SLE stands for single loss expectancy, and ALE for annualized loss expectancy.
The SLE is an amount that is assigned to a single event that represents the company's potential loss if a specific threat were to take place.
The annualized rate of occurrence (ARO) is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe.

QUESTION 31
What is the most important reason for applying segregation of duties?

A. Segregation of duties makes it clear who is responsible for what.
B. Segregation of duties ensures that, when a person is absent, it can be investigated whether he or she has been committing fraud.
C. Tasks and responsibilities must be separated in order to minimize the opportunities for business assets to be misused or changed, whether the change be unauthorized or unintentional.
D. Segregation of duties makes it easier for a person who is ready with his or her part of the work to take time off or to take over the work of another person.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Tasks and responsibilities must be segregated in order to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets
In the segregation of duties, a review is conducted as to whether a person carries out decision¬making, executive or control tasks. It is also determined whether the person needs access to information. Unnecessary access increases the risk of information being intentionally or unintentionally used, altered or destroyed.

QUESTION 32
A non-human threat for computer systems is a flood. In which situation is a flood always a relevant threat?

A. If the risk analysis has not been carried out.
B. When computer systems are kept in a cellar below ground level.
C. When the computer systems are not insured.
D. When the organization is located near a river.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Why is compliance important for the reliability of the information?

A. Compliance is another word for reliability. So, if a company indicates that it is compliant, it means that the information is managed properly.
B. By meeting the legislative requirements and the regulations of both the government and internal management, an organization shows that it manages its information in a sound manner.
C. When an organization employs a standard such as the ISO/IEC 27002 and uses it everywhere, it is compliant and therefore it guarantees the reliability of its information.
D. When an organization is compliant, it meets the requirements of privacy legislation and, in doing so, protects the reliability of its information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Compliance can also be described as tractability, obligingness, pliability, tolerance and dutifulness. What it boils down to is that an organization must observe its own internal regulations as well as the laws of the country and the requirements of local legislation and regulations.

QUESTION 34
You are the owner of the courier company SpeeDelivery. On the basis of your risk analysis you have decided to take a number of measures. You have daily backups made of the server, keep the server room locked and install an intrusion alarm system and a sprinkler system. Which of these measures is a detective measure?

A. Backup tape
B. Intrusion alarm
C. Sprinkler installation
D. Access restriction to special rooms

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Detective countermeasures are aimed at detecting incidents.

QUESTION 35
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Difference between data and information.
It is essential to understand the difference between data and information. Data can be processed by information technology, but it becomes information once it has acquired a certain meaning.

QUESTION 36
Which type of malware builds a network of contaminated computers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Storm Worm is patient, and therefore difficult to detect and analyze. It works like a colony of ants, whereby there is no central command and control server, but instead a network connection between thousands of infected PCs is set up. As a result, the infected machines do not affect the botnet. What's more, Storm Worm does not cause any damage or load to the host, so that the hosts do not know that they are infected.

QUESTION 37
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Your company is in the news as a result of an unfortunate action by one of your employees. The phones are ringing off the hook with customers wanting to cancel their contracts. What do we call this type of damage?

A. Direct damage
B. Indirect damage

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Damage resulting from the occurrence of the above threats can be classified into two groups:
- direct damage;
- indirect damage.
An example of direct damage is theft. Theft has direct consequences on the business. Another example damage caused by the water from fire extinguishers,
Indirect damage is consequential loss that can occur. An example of indirect damage is being unable to meet a contract due to the IT infrastructure being destroyed by fire, or loss of goodwill by unintentional failure to fulfill contractual obligations

QUESTION 39
An airline company employee notices that she has access to one of the company's applications that she has not used before. Is this an information security incident?

A. Yes
B. No

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Under which condition is an employer permitted to check if Internet and email 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.
D. The employer is in no way permitted to check the use of IT services by employees.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
In many organizations, there is now a code of conduct stipulating the rights and duties of the employer and of the employees in this area. It is, for example, often permissable to use the telephone and Internet for private means as long as the work does not suffer as a consequence. Downloading music, films and software and visiting sexually oriented sites are usually explicitly prohibited. The use of email should also be subject to conditions. The employer has the right to monitor the use to which their systems are put. This may be done in the form of random checks or in a highly targeted manner when there is a strong suspicion of misuse by certain employees. This might be on the condition, however, that the employees are aware of the fact that these monitoring measures may be carried out. Conditions regarding such monitoring depend on the local legislation.

QUESTION 41
You have a small office in an industrial area. You would like to analyze the risks your company faces. The office is in a pretty remote location; therefore, the possibility of arson is not entirely out of the question. What is the relationship between the threat of fire and the risk of fire?

A. The risk of fire is the threat of fire multiplied by the chance that the fire may occur and the consequences thereof.
B. The threat of fire is the risk of fire multiplied by the chance that the fire may occur and the consequences thereof.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact.

QUESTION 42
You work for a flexible employer who doesnt mind if you work from home or on the road. You regularly take copies of documents with you on a USB

memory stick that is not secure. What are the consequences for the reliability of the information if you leave your USB memory stick behind on the train?

A. The integrity of the data on the USB memory stick is no longer guaranteed.
B. The availability of the data on the USB memory stick is no longer guaranteed.
C. The confidentiality of the data on the USB memory stick is no longer guaranteed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
What is the best way to comply with legislation and regulations for personal data protection?

A. Performing a threat analysis
B. Maintaining an incident register
C. Performing a vulnerability analysis
D. Appointing the responsibility to someone

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
An example of direct damage is theft. Theft has direct consequences on the business. Another example damage caused by the water from fire extinguishers,
Indirect damage is consequential loss that can occur. An example of indirect damage is being unable to meet a contract due to the IT infrastructure being destroyed by fire, or loss of goodwill by unintentional failure to fulfill contractual obligations.

QUESTION 45
There is a network printer in the hallway of the company where you work. Many employees dont pick up their printouts immediately and leave them in 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Difference between data and information.
It is essential to understand the difference between data and information. Data can be processed by information technology, but it becomes information once it has acquired a certain meaning.

QUESTION 47
What is a human threat to the reliability of the information on your company website?

A. One of your employees commits an error in the price of a product on your website.
B. The computer hosting your website is overloaded and crashes. Your website is offline.
C. Because of a lack of maintenance, a fire hydrant springs a leak and floods the premises. Your employees cannot come into the office and therefore can not keep the information on the website up to date.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Unintentional human threat. People can also cause damage unintentionally. For example, accidentally pressing the delete button and carelessly confirming this with OK. You could also insert a USB stick that has a virus into a machine and spread the virus throughout the network. Alternatively, in panic, you may use a powder extinguisher to put out a small fire and as a result destroy a server. These are typical human responses whereby good security measures are inappropriately applied or subverted.

QUESTION 48
Midwest Insurance grades the monthly report of all claimed losses per insured as confidential. What is accomplished if all other reports from this insurance office are also assigned the appropriate grading?

A. The costs for automating are easier to charge to the responsible departments.
B. A determination can be made as to which report should be printed first and which one can wait a little longer.
C. Everyone can easiliy see how sensitive the reports' contents are by consulting the grading label.
D. Reports can be developed more easily and with fewer errors.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Logging in to a computer system is an access-granting process consisting of three steps:
identification, authentication and authorization. What occurs during the first step of this process:
identification?

A. The first step consists of checking if the user is using the correct certificate.
B. The first step consists of checking if the user appears on the list of authorized users.
C. The first step consists of comparing the password with the registered password.
D. The first step consists of granting access to the information to which the user is authorized.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Granting access to authorized users involves a number of steps which include identification of the user, authentication of this user and authorizing the user to access an asset. Identification is the first step in the process to granting access. In identification a person presents a token, for example an account number or username. The system then needs to determine whether the token is authentic. To determine the authenticity of, for example, a username, the system checks if the username exists within the system. If the username exists the user is requested to give a password. The systems tests if the password is registered with the given username. If both these tests are valid, a user is authenticated. In this example, authenticating the username is based on its existence in the system and a valid password. From this information it can be derived that a valid user is requesting access. Subsequently the system checks the resources to which access may be granted based on the permissions attached to authenticated user.

QUESTION 50
In the organization where you work, information of a very sensitive nature is processed. Management is legally obliged to implement the highest-level security measures. What is this kind of risk strategy called?

A. Risk bearing
B. Risk avoiding
C. Risk neutral

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Risk bearing, means that certain risks are accepted. This could be because the costs of the security measures exceed the possible damage. But it could also be that the management decides to do nothing even if the costs are not higher than the possible damage. The measures that a risk bearing organization takes in the area of information security are usually of a repressive nature.
Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. The majority of measures taken in the area of information security by a risk neutral organization are a combination of preventive, detective and repressive measures.
Risk avoidance means that measures are taken so that the threat is neutralized to such an extent that it no longer leads to an incident. Consider, for example, the software patches for an operating system. By patching the OS immediately after the patches are available, you are preventing your system against known technical problems or security issues. Many of the countermeasures within this strategy have a preventive character.

QUESTION 51
The act of taking organizational security measures is inextricably linked with all other measures that have to be taken. 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
The information security policy is the main document. The information security policy includes policy documents, procedures and guidelines that are aimed at a certain aspect of information security and which provide detailed expectations. These documents are an important part of the Information Security Management System (ISMS).

QUESTION 52
You are the owner of SpeeDelivery courier service. Because of your companys growth you have to think about information security. You know that you have to start creating a policy. Why is it so important to have an information security policy as a starting point?

A. The information security policy gives direction to the information security efforts.
B. The information security policy supplies instructions for the daily practice of information security.
C. The information security policy establishes which devices will be protected.
D. The information security policy establishes who is responsible for which area of information security.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
By establishing a policy for the security of information, management provides direction and support to the organization.

QUESTION 53
What is a repressive measure in the case of a fire?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
When the network monitoring activities of the security officer give an indication that something irregular has happened, action has to be taken. When

something actually does go wrong - i.e. when an incident occurs - the thing to do is to minimize the consequences. There is, for example, no point in having fire extinguishers if someone doesn't take the initiative to use them in case of a fire. Repressive measures, such as extinguishing a fire, are aimed at minimizing any damage that may be caused.

QUESTION 54
The consultants at Smith Consultants Inc. work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair. What is the companys risk if they operate in this manner?

A. If the private key becomes known all laptops must be supplied with new keys.
B. If the Public Key Infrastructure (PKI) becomes known all laptops must be supplied with new keys.
C. If the public key becomes known all laptops must be supplied with new keys.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
An asymmetrical system solves the vulnerability involved in sharing a secret key. The characteristic of an asymmetrical system is that different keys are used for encrypting and for decrypting.
Using this method, the private key is responsible for the encryption and only the public key of this key pair can decrypt the message. What makes this system so special is that the public key can be known to the whole world, as long as the private key is kept secret.

QUESTION 55
You are the owner of a growing company, SpeeDelivery, which provides courier services. You decide that it is time to draw up a risk analysis for your information system. This includes an inventory of the threats and risks. What is the relation between a threat, risk and risk analysis?

A. A risk analysis identifies threats from the known risks.
B. A risk analysis is used to clarify which threats are relevant and what risks they involve.
C. A risk analysis is used to remove the risk of a threat.
D. Risk analyses help to find a balance between threats and risks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A risk analysis has four main objectives:
1. To identify assets and their value;
2. To determine vulnerabilities and threats;
3. To determine the risk that threats will become a reality and disrupt the operational process;
4. To determine a balance between the costs of an incident and the costs of a security measure.

QUESTION 56
You apply for a position in another company and get the job. Along with your contract, you are asked to sign a code of conduct. What is a code of conduct?

A. A code of conduct specifies how employees are expected to conduct themselves and is the same for all companies.
B. A code of conduct is a standard part of a labor contract.
C. A code of conduct differs from company to company and specifies, among other things, the rules of behavior with regard to the usage of information systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
All personnel are responsible for information security. This responsibility must be made clear in the employment contract. The staff manual should contain a code of conduct and the sanctions that are imposed in the event of non-compliance and if incidents arise as a result. The code of conduct may state, for example, that private emails are not permitted.

QUESTION 57
My user profile specifies which network drives I can read and write to. What is the name of the type of logical access management where in my access and rights are determined centrally?

A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Public Key Infrastructure (PKI)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
With Discretionary Access Control, a data owner and individual users are able to define what access will be allowed to their data regardless of policy, at their own discretion. An example of this is giving others access to one's own home directory.
With Mandatory Access Control, permissions are derived from a policy. Owners and users can only permit access to others within the limits of these policy statements. Usually such a policy is centrally managed.

QUESTION 58
Some security measures are optional. Other security measures must always be implemented.
Which measure(s) must always be implemented?

A. Clear Desk Policy
B. Physical security measures
C. Logical access security measures
D. Measures required by laws and regulations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Midwest Insurance controls access to its offices with a passkey system. We call this a preventive measure. What are some other measures?

A. Detective, repressive and corrective measures
B. Partial, adaptive and corrective measures
C. Repressive, adaptive and corrective measures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Categories of countermeasures
1. Preventive countermeasures are aimed at preventing incidents;
2. Reductive countermeasures are aimed at reducing the likelihood that a threat will occur;
3. Detective countermeasures are aimed at detecting incidents;
4. Repressive countermeasures are aimed at limiting an incident;
5. Corrective countermeasures are aimed at recovering from the damage caused by an incident.
6. Acceptance of risk is a possibility too.

QUESTION 60
You are the owner of the SpeeDelivery courier service. Last year you had a firewall installed. You now discover that no maintenance has been performed since the installation. What is the biggest risk because of this?

A. The risk that hackers can do as they wish on the network without detection
B. The risk that fire may break out in the server room
C. The risk of a virus outbreak
D. The risk of undesired e-mails

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A couple of years ago you started your company which has now grown from 1 to 20 employees. Your companys information is worth more and more and gone are the days when you could keep it all in hand 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Another method of risk analysis is qualitative, and here numbers and monetary values are not assigned to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities, and rank the seriousness of the threats and the validity of the possible countermeasures.

QUESTION 62
Susan sends an email to Paul. Who determines the meaning and the value of information in this email?

A. Paul, the recipient of the information.
B. Paul and Susan, the sender and the recipient of the information.
C. Susan, the sender of the information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Information is knowledge that someone has acquired. While some people may consider a particular set of data uninteresting, others may be able to extract valuable information from it. The value of information is, therefore, determined by the value that the recipient attaches to it.

QUESTION 63
Which measure assures that valuable information is not left out available for the taking?

A. Clear desk policy
B. Infra-red detection
C. Access passes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Examples of confidentiality measures are:
- Employees take measures to ensure that information does not find its way to those people who do not need it. They ensure, for example, that no confidential documents are lying on their desk while they are away (clear desk policy).

QUESTION 64
What is an example of a good physical security measure?

A. All employees and visitors carry an access pass.
B. Printers that are defective or have been replaced are immediately removed and given away as garbage for recycling.
C. Maintenance staff can be given quick and unimpeded access to the server area in the event of disaster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You read in the newspapers that the ex-employee of a large company systematically deleted files out of revenge on his manager. Recovering these files caused great losses in time and money.
What is this kind of threat called?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Intentional human threat.
People can intentionally cause damage to information systems for various reasons. We usually think of outsiders such as a hacker who has something against a company and wishes to break into it and cause it damage.
However, what about a company employee who destroys company data after being dismissed, or who, not getting the promotion he or she wanted, takes revenge by destroying data or selling it to the competition.

QUESTION 66
Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A. ISO/IEC 27001:2005
B. Intellectual Property Rights
C. ISO/IEC 27002:2005
D. Personal data protection legislation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The protection of data and privacy falls under personal data protection legislation and guidelines. In addition, contractual stipulations with a customer may also play a part. Every organization should have a policy for the protection of personal data and this policy should be known to everybody who processes personal data.

QUESTION 67
You are the first to arrive at work in the morning and notice that the CD ROM on which you saved contracts yesterday has disappeared. You were the last to leave yesterday. When should you report this information security incident?

A. This incident should be reported immediately.
B. You should first investigate this incident yourself and try to limit the damage.
C. You should wait a few days before reporting this incident. The CD ROM can still reappear and, in that case, you will have made a fuss for nothing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reporting weaknesses in the security
When staff, temporary personnel and external users of information systems and services notice that there are (suspected) weaknesses in the system or services, it is important that they report those weaknesses as soon as possible. Only then can incidents be avoided.
When an information security incident is discovered, it is often not immediately clear whether the incident will lead to legal action. There is also the danger of critical evidence being destroyed, either intentionally or unintentionally, before the seriousness of the situation is realized. It is therefore

important to firstly report the incident and then ask for advice on the action to take. It is possible that a lawyer or the police need to be involved at an early stage and that evidence will need to be collected.

QUESTION 68
A Dutch company requests to be listed on the American Stock Exchange. Which legislation within the scope of information security is relevant in this case?

A. Public Records Act
B. Dutch Tax Law
C. Sarbanes-Oxley Act
D. Security regulations for the Dutch government

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
There is legislation for tax matters, for privacy and for how business is conducted. There is local legislation, international legislation and regulations such as the Sarbanes-Oxley Act which stipulates that each foreign corporation that is listed on the New York Stock Exchange must demonstrate that it conforms with American legislation and regulations.

QUESTION 69
You own a small company in a remote industrial area. Lately, the alarm regularly goes off in the middle of the night. It takes quite a bit of time to respond to it and it seems to be a false alarm every time. You decide to set up a hidden camera. What is such a measure called?

A. Detective measure
B. Preventive measure
C. Repressive measure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Detective countermeasures are aimed at detecting incidents.

QUESTION 70
At Midwest Insurance, all information is classified. What is the goal of this 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Classification is used to define the different levels of sensitivity into which information may be structured;
Grading is the act of assigning the appropriate classification - such as secret, confidential or public - to specific information. This term is used often within the government;

QUESTION 71
Which one of the threats listed below 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 off because of overheating.
C. A confidential document is left in the printer.
D. Hackers can freely enter the computer network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Physical security includes the protection of equipment through climate control (air conditioning, air humidity), the use of special fire extinguishers and the provision of clean' energy. Clean energy refers to the prevention of peaks and troughs (dirty energy) in the power supply and the fact that the power supply is filtered.

QUESTION 72
What is the best description of a risk analysis?

A. A risk analysis is a method of mapping risks without looking at company processes.
B. A risk analysis helps to estimate the risks and develop the appropriate security measures.
C. A risk analysis calculates the exact financial consequences of damages.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A risk analysis has four main objectives:

1. To identify assets and their value;
2. To determine vulnerabilities and threats;
3. To determine the risk that threats will become a reality and disrupt the operational process;
4. To determine a balance between the costs of an incident and the costs of a security measure.

QUESTION 73
What is the goal of an organization's security policy?

A. To provide direction and support to information security
B. To define all threats to and measures for ensuring information security
C. To document all incidentsthat threaten the reliability of information
D. To document all procedures required to maintain information security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
By establishing a policy for the security of information, management provides direction and support to the organization.

QUESTION 74
The Information Security Manager (ISM) at Smith Consultants Inc. introduces the following measures to assure information security:
- The security requirements for the network are specified.
- A test environment is set up for the purpose of testing reports coming from the database.
- The various employee functions are assigned corresponding access rights.
- RFID access passes are introduced for the building.
Which one of these measures is not a technical measure?

A. The specification of requirements for the network
B. Setting up a test environment
C. Introducing a logical access policy
D. Introducing RFID access passes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Physical security.
Electronic access management.
Many organizations use pass systems with wireless RFID passes. These are currently the most widely used systems, but are the subject of much

discussion as they can be ‘tapped’, copied and mimicked.

QUESTION 75
A company moves into a new building. A few weeks after the move, a visitor appears unannounced in the office of the director. An investigation shows that visitors passes grant the same access as the passes of the companys staff. Which kind of security measure could have prevented this?

A. A physical security measure
B. An organizational security measure
C. A technical security measure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
You have an office that designs corporate logos. You have been working on a draft for a large client. Just as you are going to press the <save> button, the screen goes blank. The hard disk is damaged and cannot be repaired. You find an early version of the design in your mail folder and you reproduce the draft for the customer. What is such a measure called?

A. Corrective measure
B. Preventive measure
C. Reductive measure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Preventive countermeasures are aimed at preventing incidents;
Reductive countermeasures are aimed at reducing the likelihood that a threat will occur;
Corrective countermeasures are aimed at recovering from the damage caused by an incident.

QUESTION 77
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 avoiding

C. Risk neutral

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Risk bearing, means that certain risks are accepted. This could be because the costs of the security measures exceed the possible damage. But it could also be that the management decides to do nothing even if the costs are not higher than the possible damage. The measures that a risk bearing organization takes in the area of information security are usually of a repressive nature.
Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. The majority of measures taken in the area of information security by a risk neutral organization are a combination of preventive, detective and repressive measures.
Risk avoidance means that measures are taken so that the threat is neutralized to such an extent that it no longer leads to an incident.

QUESTION 78
Three characteristics determine the reliability of information. Which characteristics are these?

A. Availability, Integrity and Correctness
B. Availability, Integrity and Confidentiality
C. Availability,Nonrepudiation and Confidentiality

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A security program may have several large and small objectives, but the most important principles in all security programs are confidentiality (exclusivity), integrity and availability. These are referred to as the CIA triangle.

QUESTION 79
What action is an unintentional human threat?

A. Arson
B. Theft of a laptop
C. Social engineering
D. Incorrect use of fire extinguishing equipment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: