Total Questions: 50
Latest Version: 6.0

Question: 1

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

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

Answer: A

Question: 2

What is the most important reason for applying the 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 readywith his or her part of the work to take time off or to take over the work of another person.

Answer: C

Question: 3

Companies use 27002 for compliance for which of the following reasons:

A. A structured program that helps with security and compliance
B. Explicit requirements for all regulations
C. Compliance with ISO 27002 is sufficient to comply with all regulations

Answer: A

Question: 4

Of the following, which is the best organization or set of organizations to contribute to compliance?

A. IT only
B. IT,business management, HR and legal
C. IT and management
D. IT and legal

Answer: B

Question: 5

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

Answer: C

Question: 6

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

A. It provides digital certificates that can be used to digitally signdocuments. 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.

Answer: D

Question: 7

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

Answer: D

Question: 8

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. Thefirst 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.

Answer: B

Question: 9

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
D. Risk passing

Answer: C

Question: 10

What does the Information Security Policy describe?

A. how the InfoSec-objectives will be reached
B. which InfoSec-controls have been selected and taken
C. what the implementation-planning of the information security management system is

D. which Information Security-procedures are selected

Answer: A

Question: 11

Why is compliance important forthe 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 theregulations 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 thereforeit 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.

Answer: B

Question: 12

In the context ofcontact with special interest groups, any information-sharing agreements should identify requirements for the protection of _________ information.

A. Availability
B. Confidential
C. Authentic
D. Authorization

Answer: B

Question: 13

Select risk control activities for domain "10. Encryption" of ISO / 27002: 2013 (Choose two)

A. Work in safe areas
B. Cryptographic Controls Use Policy
C. Physical security perimeter
D. Key management

Answer: B,D

Question: 14

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.

Answer: B

Question: 15

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.

Answer: B

Question: 16

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

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

Answer: C

Question: 17

Physical labels and ________ are two common forms of labeling which are mentioned in ISO 27002.

A. metadata

B. teradata
C. bridge

Answer: A

Question: 18

You have juststarted 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 alegal 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.

Answer: A

Question: 19

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

Answer: A

Question: 20

Which of these control objectives are NOT in the domain "12.OPERATIONAL SAFETY"?

A. Protection against malicious code
B. Redundancies
C. Test data
D. Technical vulnerability management

Answer: B

Question: 21

An employee in the administrative department of Smiths Consultants Inc. finds out that the expiry date of a contract with one of theclients 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

Answer: D

Question: 22

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

A. If the riskanalysis 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.

Answer: B

Question: 23

One of the ways Internet of Things (IoT) devices can communicate with each other (or `the outside world') is using a so-called short-range radio protocol. Which kind of short-range radio protocol makes it possible to use your phone as a credit card?

A. Near Field Communication (NFC)
B. Bluetooth
C. Radio Frequency Identification (RFID)
D. The 4G protocol

Answer: A

Question: 24

How many domains does ISO / IEC 27002: 2013 have?

A. 140
B. 14
C. 110
D. 114

Answer: B

Question: 25

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 company's staff. Which kind of security measure could have prevented this?

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

Answer: A

Question: 26

Who is accountable to classify information assets?

A. the CEO
B. the CISO
C. the Information Security Team
D. theasset owner

Answer: D

Question: 27

Which of the following measures is a correctivemeasure?

A. Incorporating an Intrusion Detection System (IDS) in the design of a computer center
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

Answer: D

Question: 28

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

Answer: B

Question: 29

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 ofconduct 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.

Answer: C

Question: 30

The identified owner of an asset is always an individual

A. True
B. False

Answer: B

Question: 31

Select the controls that correspond to thedomain "9. ACCESS CONTROL" of ISO / 27002
(Choose three)

A. Restriction of access to information
B. Return of assets
C. Management of access rights with special privileges
D. Withdrawal or adaptation of access rights

Answer: A,B,D

Question: 32

Responsibilities for information security in projects should be defined and allocated to:

A. the project manager
B. specified roles defined in the used project management method of the organization
C. the InfoSec officer
D. the owner of the involved asset

Answer: B

Question: 33

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 thecompany 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

Answer: C

Question: 34

True or False: Organizations allowing teleworking activities, the physical security of the building and the local environment of the teleworking site should be considered

A. True
B. False

Answer: A

Question: 35

It is allowed that employees and contractors are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing")

A. True
B. False

Answer: A

Question: 36

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

Answer: D

Question: 37

Which of these reliability aspects is "completeness" a part of?

A. Availability
B. Exclusivity
C. Integrity
D. Confidentiality

Answer: C

Question: 38

ISO 27002 provides guidance in the following area

A. PCI environment scoping

B. Information handling recommendations
C. Framework for an overall security andcompliance program
D. Detailed lists of required policies and procedures

Answer: C

Question: 39

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.

Answer: A

Question: 40

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 replacedare 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.

Answer: A

Question: 41

What is the greatest risk for an organization ifno 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 areimplemented.
D. It is not possible for an organization to implement information security in a consistent manner.

Answer: D

Question: 42

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 firstand which ones can wait a little longer.
C. Everyone can easily see how sensitive the reports' contents are by consulting the grading label.
D. Reports can be developed more easily and with fewer errors.

Answer: C

Question: 43

What is the ISO / IEC 27002 standard?

A. It is a guide of good practices that describes the controlobjectives and recommended controls regarding information security.
B. It is a guide that focuses on the critical aspects necessary for the successful design and implementation of an ISMS in accordance with ISO / IEC 27001

C. It is a guide for the development and use of applicable metrics and measurement techniques to determine the effectiveness of an ISMS and the controls or groups of controls implemented according to ISO / IEC 27001.

Answer: A

Question: 44

You are a consultant and areregularly hired by the Ministry of Defense to perform analysis. Since the assignments are irregular, you outsource the administration of your business to temporary workers. You don't want the temporary workers to have access to your reports. Which reliability aspect of the information in your reports must you protect?

A. Availability
B. Integrity
C. Confidentiality

Answer: C

Question: 45

Prior to employment, _________ as well as terms & conditions of employment are included as controls in ISO 27002 to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A. screening
B. authorizing
C. controlling
D. flexing

Answer: A

Question: 46

What are the data protection principles set out in the GDPR?

A. Purpose limitation, proportionality, availability, data minimisation
B. Purpose limitation, proportionality, data minimisation, transparency
C. Target group, proportionality, transparency, data minimisation
D. Purpose limitation, pudicity, transparency, data minimisation

Answer: B

Question: 47

What should be used to protect data on removable media ifdata confidentiality or integrity are important considerations?

A. backup on another removable medium
B. cryptographic techniques
C. a password
D. logging

Answer: B

Question: 48

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 ofinformation

Answer: A

Question: 49

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 inventoryof 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 riskanalysis is used to remove the risk of a threat.
D. Risk analyses help to find a balance between threats and risks.

Answer: B

Question: 50

What is the objective of classifying information?

A. Authorizing the use of an information system
B. Creating alabel 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

Answer: C