EX0-105.examcollection.premium.exam.128q

Number: EX0-105
Passing Score: 800
Time Limit: 120 min
File Version: 6.0

EX0-105

Information Security Foundation based on ISO/IEC 27002

Version 6.0

Sections

1. Volume A
2. Volume B
3. Volume C

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: Volume A
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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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 that staff 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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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 is initiated. 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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

QUESTION 28
Which of these is not malicious software?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

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: Volume A
Explanation

Explanation/Reference:

QUESTION 38
You are a consultant and are regularly hired by the Ministry of Defense to perform analyses.
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 39
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: Volume A
Explanation

Explanation/Reference:

QUESTION 40
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: Volume A
Explanation

Explanation/Reference:

QUESTION 41
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: Volume B
Explanation

Explanation/Reference:

QUESTION 42
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: Volume B
Explanation

Explanation/Reference:

QUESTION 43
You work for a flexible employer who doesn't 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: Volume B
Explanation

Explanation/Reference:

QUESTION 44
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: Volume B
Explanation

Explanation/Reference:

QUESTION 45
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: Volume B
Explanation

Explanation/Reference:

QUESTION 46
There is a network printer in the hallway of the company where you work. Many employees don't pick up their printouts immediately and leave them 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: Volume B
Explanation

Explanation/Reference:

QUESTION 47
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: Volume B
Explanation

Explanation/Reference:

QUESTION 48
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: Volume B
Explanation

Explanation/Reference:

QUESTION 49
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: Volume B
Explanation

Explanation/Reference:

QUESTION 50
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: Volume B
Explanation

Explanation/Reference:

QUESTION 51
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: Volume B
Explanation

Explanation/Reference:

QUESTION 52
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: Volume B
Explanation

Explanation/Reference:

QUESTION 53
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: Volume B
Explanation

Explanation/Reference:

QUESTION 54
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: Volume B
Explanation

Explanation/Reference:

QUESTION 55
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 company's 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: Volume B
Explanation

Explanation/Reference:

QUESTION 56
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: Volume B
Explanation

Explanation/Reference:

QUESTION 57
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: Volume B
Explanation

Explanation/Reference:

QUESTION 58

My user profile specifies which network drives I can read and write to. What is the name of the type of logical access management wherein 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: Volume B
Explanation

Explanation/Reference:

QUESTION 59
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: Volume B
Explanation

Explanation/Reference:

QUESTION 60
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: Volume B

Explanation

Explanation/Reference:

QUESTION 61
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: Volume B
Explanation

Explanation/Reference:

QUESTION 62
A couple of years ago you started your company which has now grown from 1 to 20 employees.
Your company's information is worth more and more and gone are the days when you could keep 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: Volume B
Explanation

Explanation/Reference:

QUESTION 63
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: Volume B
Explanation

Explanation/Reference:

QUESTION 64
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: Volume B
Explanation

Explanation/Reference:

QUESTION 65
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: Volume B
Explanation

Explanation/Reference:

QUESTION 66
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: Volume B
Explanation

Explanation/Reference:

QUESTION 67
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: Volume B
Explanation

Explanation/Reference:

QUESTION 68
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: Volume B

Explanation

Explanation/Reference:

QUESTION 69
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: Volume B
Explanation

Explanation/Reference:

QUESTION 70
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: Volume B
Explanation

Explanation/Reference:

QUESTION 71
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: Volume B
Explanation

Explanation/Reference:

QUESTION 72
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: Volume B
Explanation

Explanation/Reference:

QUESTION 73
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: Volume B
Explanation

Explanation/Reference:

QUESTION 74
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 incidents that threaten the reliability of information
D. To document all procedures required to maintain information security

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 75
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: Volume B
Explanation

Explanation/Reference:

QUESTION 76
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: Volume B
Explanation

Explanation/Reference:

QUESTION 77
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: Volume B
Explanation

Explanation/Reference:

QUESTION 78
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: Volume B
Explanation

Explanation/Reference:

QUESTION 79
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: Volume B
Explanation

Explanation/Reference:

QUESTION 80
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: Volume B
Explanation

Explanation/Reference:

QUESTION 81
To which category of security measures does a smoke alarm belong?

A. Corrective
B. Detective
C. Preventive
D. Repressive

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 82
Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 83
Which regulation is only applicable for United States public companies (e.g. listed on the New York Stock Exchange)?

A. BS ISO 22301:2012
B. ISO/IEC 27001
C. Payment Card Industry compliance
D. Sarbanes-Oxley act

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 84
A marketing employee accidentally e-mails a spreadsheet with all the company¡¯s clients, their personal and commercial data, to the wrong email address.
Who determines the value of the information in the spreadsheet?

A. Each party determines the value of the information independently
B. Privacy legislation determines the penalty and thus the value
C. The recipient, who can use it for identity theft

D. The sender, who uses it for accounting purposes

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 85
Lightning strikes the data center and the power surge destroys several servers. What type of threat is this?

A. Electrical threat
B. Non-human threat
C. Sporadic threat
D. Unintentional threat

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 86
What is the purpose of authentication?

A. To make your identity known, which means you are given access to the system
B. To check the username against a list of users who have access to the system
C. To determine whether access may be granted by determining whether the token used is authentic
D. To give you the rights that you need, such as being able to read the data in the system

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 87
Your company is concerned about the effect of global warming on sea levels and asks you to make preparations that prevents downtime of the billing

process.

What will you create?

A. Business Continuity Plan
B. Disaster Recovery Plan

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 88
What is the most common risk strategy besides Risk bearing and Risk neutral?

A. Risk acceptance
B. Risk avoidance
C. Risk insurance
D. Risk transference

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 89
A Dutch company is processing information from Dutch civilians; this implies applicability of some Dutch regulations regarding the privacy of these civilians. The company is mandated to implement security measures.

Which measure helps the company best in proving compliance with applicable regulations?

A. Handing over the Non disclosure agreements (NDAs) that are signed by all employees.
B. Handing over the results of a security audit.
C. Installing a firewall to limit the access to the server.
D. The execution of a penetration test on the server processing the sensitive information.

Correct Answer: B

Section: Volume C
Explanation

Explanation/Reference:

QUESTION 90
Which security measure is not an organizational level security measure?

A. Carrying out background investigations on new personnel
B. Implementing Role Based Access Control
C. Setting up a security awareness program
D. Setting up an information security policy document

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 91
Which legislation regulates the storage and destruction of archive documents?

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

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 92
Which threat can materialize as a result of the absence of physical security?

A. A USB stick with confidential information is lost by an employee.

B. A worm infects several servers due to insufficient port filtering.
C. Software stops working because the license has expired.
D. Systems malfunction due to spikes in the power supply.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 93
Someone sends an e-mail. The sender wants the recipient to be able to verify who wrote and sent the email.

What does the sender attach to the email?

A. A digital signature
B. A PKI certificate
C. Her private key
D. Her public key

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 94
What is the purpose for an organization to have an information security policy?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 95
Physical security must protect a company for anyone to easily access the company assets. This is illustrated by thinking in terms of series of protection rings.

Which protection ring deals with the asset that is to be protected?

A. Building
B. Object
C. Outer ring
D. Working space

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 96
During a risk analysis a system administrator mentions that due to the lack of communication between Human recourses management (HRM) and system administrators, employees can still access the company server from home even if they are no longer employed by the company.

Which characteristic of a risk is missing here?

A. Business impact
B. Security control
C. Threat agent
D. Vulnerability

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 97
There are three types of human threats: Intentional human threats, Unintentional human threats and a third human threat.

What is the third type of human threat?

A. Acts of stupidity
B. Social engineering
C. Technical human threats

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 98
Midwest Insurance controls access to its offices with a passkey system. What kind of security measure is this?

A. Corrective
B. Detective
C. Preventive
D. Repressive

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 99
You own a store, and money keeps disappearing from the cash register. You want to put an end to this by means of a detective measure.

What is an example of a detective measure?

A. Close the store and hire a detective.
B. Post a warning sign on the register.
C. Set up a hidden camera.

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:

QUESTION 100
What is the main reliability aspect of information besides Confidentiality and Integrity?

A. Accounting
B. Authenticity
C. Authorization
D. Availability

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 101
An information security incident has several stages which together are known as the incident cycle. At different stages within this cycle different kinds of security measures are applied.
At which stage of the incident cycle is the Intrusion detection system (IDS) measure aimed?

A. At the stage Threat
B. Between the stages Threat and Incident
C. At the stage Incident
D. Between the stages Incident and Damage

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 102
What is accomplished if reports are 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 easily 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: Volume C
Explanation

Explanation/Reference:

QUESTION 103
Of which concept is ‘measures taken to safeguard an information system from attacks’ the definition?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 104
What is the physical equivalent of the logical information security measure Intrusion Detection System (IDS)?

A. Cameras
B. Cooling
C. Fire extinguishers
D. UPS

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 105
An employee is about to lose his job and decides to delete as many documents as possible from the network storage server.

In which main threat category does this threat belong?

A. Disgruntled employee
B. Intentional human threat
C. Social engineering

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 106
What are the two main types of damage, resulting from incidents?

A. Direct and indirect damage
B. Financial and emotional damage
C. Visible and invisible damage

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 107
The term ‘big data’ is commonly used. However data itself has less (or no) value for an organization.
Which process adds value to the data and turns data into ‘information’?

A. Analysis
B. Archiving
C. Back-up
D. Duplication

Correct Answer: A

Section: Volume C
Explanation

Explanation/Reference:

QUESTION 108
An employee detects abnormal behavior of her desktop computer.

After reporting to the system administrator and a first investigation, the system administrators decide to get some help from the Computer emergency response Team (CERT).

Which type of escalation is described above?

A. Functional escalation
B. Hierarchical escalation
C. Privilege escalation
D. Vertical escalation

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 109
Two friends want to exchange a confidential document. It is important that eavesdroppers cannot see this information. Furthermore the receiver should be able to validate the sender and that the information is not altered during transport. Both friends have a public/private key combination.

Which key is used, prior to transmission, to ensure the authenticity of the document?

A. Public key of the sender
B. Public key of the recipient
C. Private key of the sender
D. Private key of the recipient

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 110
After a thorough risk analysis and the identification of appropriate security controls, the management team decides that for one specific threat the impact should be covered by insurance.

Which kind of risk treatment control is described here?

A. Accept
B. Avoid
C. Reduce
D. Transfer

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 111
Within a company several employees work mostly outside the perimeter of the company. These employees have laptops on which the necessary (confidential) information is stored.
Which technical security measure protects the information from unwanted disclosure in case the employee loses the laptop?

A. Anti-theft cable chain
B. Awareness presentations for employees
C. Classification of information
D. Disk encryption

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 112
Which approach does/did the United States take with regard to privacy legislation?

A. Create legislation as it is needed
B. Proactively create legislation on upcoming technologies
C. Rely purely on self-regulation
D. Translate the convention on human rights into privacy laws

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 113
Why is sensitive information graded?

A. To determine how the information should be processed
B. To determine the applicable back-up scheme
C. To improve awareness of employees
D. To permit the recipient to archive received information

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 114
Your organization has an office with space for twenty five (25) workstations. These workstations are all fully equipped and in use. Due to a reorganization ten (10) extra workstations are added, five (5) of which are used for a call center 24 hours per day. Five (5) 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 ten (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 ten (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 ten (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: Volume C
Explanation

Explanation/Reference:

QUESTION 115
Which legislation makes it easier to deal with offences perpetrated through advanced information technology?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 116
An Incident Management process has several purposes.

Which is not a purpose of the Incident Management process?

A. Learn from weaknesses so they can be fixed and future incidents are prevented.
B. Make sure that all employees and staff know the procedure for reporting incidents.
C. Reprimand the person who is responsible for causing the incident.
D. Solve the incident appropriately and as quickly as possible.

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 117
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 is initiated.

Which stage of the incident cycle follows the incident stage?

A. Threat
B. Damage
C. Recovery

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 118
Which type of malware is a program that collects information of the computer user and sends it to another party?

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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 119
What is an organizational security measure?

A. Create procedures for screening new personnel
B. Implement access control on doors to secure areas
C. Install antivirus software on all systems

D. Switch to a newer operating system throughout the company

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 120
A hacker gains access to a webserver and deletes a file on the server containing credit card numbers.

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

A. Availability
B. Confidentiality
C. Integrity

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 121
There are three types of “human threats”.

The threat that a user accidentally deletes a document belongs to which category?

A. Acts of stupidity
B. Intentional human threats
C. Social engineering
D. Unintentional human threats

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 122
What is a risk analysis used for?

A. to express the value of information for an organization in monetary terms
B. to clarify to management their responsibilities
C. to make everyone in the organization aware of all risks
D. to ensure that security measures are deployed in a cost-effective and timely fashion

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 123
What is not a criteria in the review process where it is determined whether segregation of duties is applicable for an employee?

A. In which decision making processes the person in question is involved.
B. In which control processes the person in question is involved.
C. At which locations the person in question is active.

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 124
What is the purpose of a Disaster Recovery Plan (DRP)?

A. to identify the vulnerability underlying a disaster
B. to limit the consequences in case a disaster occurs C. to reduce the possibility of a disaster to occur
C. to restore the situation back to how this was before the disaster

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 125
The incident cycle has four stages. Which stage follows the Threat stage?

A. Damage
B. Incident
C. Recovery

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 126
Two friends want to exchange a confidential document by e-mail. They decide to use cryptography to protect the confidentiality of the document. To be able to encrypt alid decrypt the document they first exchange the key that is both used for encryption and decryption by phone.

What type of encryption system is used by the two friends?

A. Asymmetrical system
B. Public Key Infrastructure (PKI)
C. Symmetrical system

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 127
What is not a category for security measures?

A. Corrective measures
B. Investigative measures
C. Preventive measures

D. Reductive measures

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 128
What is 'a potential cause of an unwanted incident, which may result in harm to a system or organization' called?

A. Exposure
B. Risk
C. Threat
D. Vulnerability

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference: