Exin

Exam EX0-105

Information Security Foundation based on ISO/IEC 27002

Version: 8.0

[Total Questions: 128]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	40
Topic 2: Volume B	40
Topic 3: Volume C	48

Topic 1, Volume A

Question No : 1 - (Topic 1)

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.

Answer: A

Question No : 2 - (Topic 1)

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

Answer: C

Question No : 3 - (Topic 1)

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

Answer: B

Question No : 4 - (Topic 1)

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

Answer: D

Question No : 5 - (Topic 1)

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

Answer: C

Question No : 6 - (Topic 1)

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.

Answer: D

Question No : 7 - (Topic 1)

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 No : 8 - (Topic 1)

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

Answer: D

Question No : 9 - (Topic 1)

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

Answer: B

Question No : 10 - (Topic 1)

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

Answer: B

Question No : 11 - (Topic 1)

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.

Answer: C

Question No : 12 - (Topic 1)

Which of these is not malicious software?

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

Answer: A

Question No : 13 - (Topic 1)

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

Answer: C

Question No : 14 - (Topic 1)

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.

Answer: C

Question No : 15 - (Topic 1)

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.

Answer: C

Question No : 16 - (Topic 1)

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 No : 17 - (Topic 1)

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 No : 18 - (Topic 1)

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

Answer: C

Question No : 19 - (Topic 1)

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

Answer: C

Question No : 20 - (Topic 1)

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

Answer: B