

ISFS.exam.44q

Number: ISFS

Passing Score: 800

Time Limit: 120 min



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

ISFS

Information Security Foundation based on ISO/IEC 27002

Exam A

QUESTION 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?



<https://vceplus.com/>

- 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:

QUESTION 2

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:

QUESTION 3

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:

QUESTION 4

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:

QUESTION 5

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:

QUESTION 6

What is an example of a security incident?



<https://vceplus.com/>

- 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 7

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:

QUESTION 8

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:

QUESTION 9

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 10

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:

QUESTION 11

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?



<https://vceplus.com/>

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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 13

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:

QUESTION 14

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:

QUESTION 15

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:

QUESTION 16

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:

QUESTION 17

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:

QUESTION 18

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:

QUESTION 19

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



<https://vceplus.com/>

- 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 20

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:

QUESTION 21

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:

QUESTION 22

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:

QUESTION 23

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:

QUESTION 24

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 25

You are a consultant and are regularly 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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?



<https://vceplus.com/>

- 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:

QUESTION 27

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: (none)

Explanation

Explanation/Reference:

QUESTION 28

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 29

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:

QUESTION 30

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: (none)

Explanation

Explanation/Reference:

QUESTION 31

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:

QUESTION 32

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 cannot keep the information on the website up to date.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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 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: (none)

Explanation

Explanation/Reference:

QUESTION 34

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:

QUESTION 35

You are the owner of a growing company, SpeedDelivery, 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:

QUESTION 36

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?



<https://vceplus.com/>

- 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:

QUESTION 37

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: (none)

Explanation

Explanation/Reference:

QUESTION 38

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 39

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:

QUESTION 40

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 41

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: (none)

Explanation

Explanation/Reference:

QUESTION 42

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:

QUESTION 43

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:

QUESTION 44

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:



<https://vceplus.com/>