Question #1 *Topic 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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *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

Suggested Answer: *B*

defconx 1 year, 2 months ago

correto! o custo das ameaças NÃO é um dos 4 principais objetivos de uma análise de risco.
1.Identificar os bens e os seus valores;
2.Determinar as vulnerabilidades e ameaças;
3.Determinar quais as ameaças se tornarão um risco e que podem interromper o processo operacional;
4.Indicar um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança parte da análise de risco é uma análise custo / benefício.

upvoted 1 times

fangeel 1 year, 6 months ago

correct! cost of threats is NOT one of the 4 main objectives of a risk analysis

upvoted 2 times

Question #14 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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.

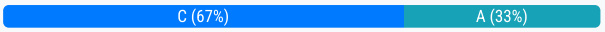
B. Having a PKI shows customers that a web-based business is secure.

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.

Suggested Answer: *C*

Community vote distribution



crazycoder 9 months, 1 week ago

Selected Answer: C

The correct answer is C: It is written word by word in a book for this exam—Foundation of Information Security, 4th revised edition by Jule Hinzbergen.

upvoted 1 times

b274b54 10 months ago

Selected Answer: C

I have been reading the Wikipedia page on what is PKI and answer C also makes sense. I hope someone else can clarify this question please

upvoted 1 times

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: A

I should be A.

upvoted 1 times

tinoez 1 year, 5 months ago

Should this not be answer A?
It provides digital certificates which can be used to digitally sign documents. Such signatures irrefutably
determine from whom a document was sent.

upvoted 1 times

Question #19 *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

Suggested Answer: *D*

Community vote distribution

B (100%)

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: B

The issue described—where the expiry date of a contract is earlier than the start date—indicates a problem with data integrity. Data integrity measures aim to ensure the accuracy, consistency, and reliability of information. In this case, a control such as input validation or automated checks could have prevented the error.

How other options compare:
A. Availability measure: Availability measures ensure that information is accessible when needed. This does not address the accuracy of the contract data.
C. Organizational measure: Organizational measures involve policies, procedures, and training but may not directly address errors in data entry or logic.
D. Technical measure: While technical measures (e.g., automated tools) might implement the integrity controls, the focus here is on the nature of the error, which is related to data integrity.

upvoted 1 times

ruilopesss 3 years, 8 months ago

Could be option B too?

upvoted 1 times

soniazk 4 years ago

C'est plutôt la réponse B

upvoted 1 times

ruilopesss 3 years, 8 months ago

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

upvoted 1 times

NoventiqInternationalPeruSAC 11 months, 1 week ago

In the question they didn´t metion nothing aboyt a system. The "employee" just found that information so they need to prevent the "Integrity measure" answer should be B.

upvoted 1 times

Question #20 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: D

Based on ISO/IEC 27001, the organization wishes to achieve several objectives by asking you to sign a code of conduct and a contract. The primary goal is to provide staff with guidance on how to report suspected misuses of IT facilities. This ensures that employees are aware of the proper procedures for reporting any security incidents or breaches, which is crucial for maintaining the organization's information security management system (ISMS) and protecting sensitive data.

Therefore, the correct answer is:

D. A code of conduct gives staff guidance on how to report suspected misuses of IT facilities.

upvoted 1 times

Question #24 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

eKizengue 8 months, 2 weeks ago

Selected Answer: C

In an organization, the value of information is typically determined by the person responsible for it, often a manager or an information owner. In this scenario, Linda, as Peter's manager, is likely responsible for the document and its classification, sensitivity, and importance. I just don't see way the rigth answer should be "A"

upvoted 1 times

b274b54 10 months ago

Selected Answer: A

Can someone please clarify why the answer should be A? I dont understand any of this

upvoted 1 times

defconx 1 year, 2 months ago

quem recebe/destinado a informação que determina este valor, "informação é poder" se voce souber utiliza-lo.

upvoted 1 times

eKizengue 8 months, 2 weeks ago

Mas.... Em uma organização, o valor da informação é geralmente determinado pela pessoa responsável por ela, frequentemente um gerente ou um proprietário da informação.... certo ?

upvoted 1 times

fangeel 1 year, 6 months ago

Yes - it's the recipient!

upvoted 1 times

ruilopesss 2 years, 2 months ago

that question dont have any interest to be here.

upvoted 1 times

soniazk 2 years, 6 months ago

la question n'est pas claire

upvoted 1 times

Question #25 *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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Which of these is not malicious software?

A. Phishing

B. Spyware

C. Virus

D. Worm

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *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.

Suggested Answer: *C*

king777 1 year, 3 months ago

It's is separation of duties not segregation of duties, so guys don't be confused!

upvoted 1 times

Question #32 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which type of malware builds a network of contaminated computers?

A. Logic Bomb

B. Storm Worm or Botnet

C. Trojan

D. Virus

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *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 dont 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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

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

A. Yes

B. No

Suggested Answer: *B*

fangeel 1 year ago

It is not yet an incident, therefor No

upvoted 1 times

Sohail30 1 year, 2 months ago

It should be YES.

Because she can misuse the application, which she is not authorized for.

upvoted 1 times

soniazk 2 years ago

i think that it is yes

upvoted 2 times

king777 1 year, 3 months ago

same bro agrees with you.

upvoted 1 times

Question #1 *Topic 2*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

You work for a flexible employer who doesnt mind if you work from home or on the road. You regularly take copies of documents with you on a USB memory stick that is not secure. What are the consequences for the reliability of the information if you leave your USB memory stick behind on the train?

A. The integrity of the data on the USB memory stick is no longer guaranteed.

B. The availability of the data on the USB memory stick is no longer guaranteed.

C. The confidentiality of the data on the USB memory stick is no longer guaranteed.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

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

Suggested Answer: *D*

king777 1 year, 3 months ago

For example, Privacy Officer who can handle SPI PII PHI.

upvoted 2 times

Question #5 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

There is a network printer in the hallway of the company where you work. Many employees dont pick up their printouts immediately and leave them in the printer.
What are the consequences of this to the reliability of the information?

A. The integrity of the information is no longer guaranteed.

B. The availability of the information is no longer guaranteed.

C. The confidentiality of the information is no longer guaranteed.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 2*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 2*

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

A. If the private key becomes known all laptops must be supplied with new keys.

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

C. If the public key becomes known all laptops must be supplied with new keys.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 2*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 2*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 2*

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)

Suggested Answer: *B*

Community vote distribution

B (100%)

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: B

The type of logical access management wherein your access and rights are determined centrally is Mandatory Access Control (MAC). This system is managed centrally by a single security authority, as opposed to Discretionary Access Control (DAC), where the owner of the object can grant others privileges within the object

upvoted 1 times

fangeel 3 years ago

B correct!

upvoted 1 times

jaystar 3 years, 5 months ago

RESPONSE I A

upvoted 1 times

Question #19 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 2*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: A

measures besides preventive measures include detective, repressive, and corrective measures. Detective measures are designed to identify and detect security incidents, repressive measures aim to stop or mitigate the impact of an incident, and corrective measures are implemented to restore systems and processes to their normal state after an incident.

upvoted 1 times

Question #21 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 2*

A couple of years ago you started your company which has now grown from 1 to 20 employees.
Your companys information is worth more and more and gone are the days when you could keep it all in hand yourself. You are aware that you have to take measures, but what should they be?
You hire a consultant who advises you to start with a qualitative risk analysis. What is a qualitative risk analysis?

A. This analysis follows a precise statistical probability calculation in order to calculate exact loss caused by damage.

B. This analysis is based on scenarios and situations and produces a subjective view of the possible threats.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 2*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

NoventiqInternationalPeruSAC 11 months, 1 week ago

Selected Answer: A

the meaning and value of information in an email are determined by the recipient of the information. This is because the recipient interprets the information based on their context, understanding, and needs.

upvoted 1 times

Question #24 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!