EX0-105.exam.71q

EX0-105

Information Security Foundation based on ISO/IEC 27002

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

Exam A

QUESTION 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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
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

QUESTION 57
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 58
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 59
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 60
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 61
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 62
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 63
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 64
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 65
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 66
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

QUESTION 67
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 68
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 69
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 70
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 71
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: