INFORMATION SECURITY
FOUNDATION

Sample Exam

SECO INSTITUTE

Context

Information Security Foundation is the first level of the SECO Institute's Certified Information Security Officer certification track.

Successful completion of the Foundation course provides candidates with sufficient knowledge to continue with the *Information Security Practitioner* course.

Target audience

The course is intended for those who aspire to protect systems and networks against information security threats and raise cybersecurity awareness across their organisation.

Certification exam

Candidates can take their exams at an accredited exam centre or book an exam directly with the SECO-Institute.

Attending a course is not a prerequisite for taking a certification exam.

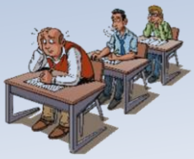
Exam details

- Computer-based
- 40 multiple-choice questions
- Time allotted: 60 minutes
- Pass mark: 60% (60 points out of 100 points)
- Open book/notes: not permitted
- Electronic equipment: not permitted

Rules to be observed by candidates: The SECO-Institute's Examination Rules and Regulations

(https://www.seco-institute.org/html/filesystem/storeFolder/10/General-Terms-and-Conditions-for-participation-in-SECO-Institute-exams-2017-11.pdf)

Questions



Question 1

You want to establish a well-structured information security process. Which reference framework can best help you to achieve your goal?

A. Section 404 of the Sarbanes-Oxley Act
B. IT Service Management
C. Your organisation’s corporate strategy
D. An Information Security Management System (ISMS)

Question 2

You are outsourcing a process. Which mechanism best enables you to have proper control over the security of the outsourced process?

A. A set of best practices
B. A normative standard
C. Security clauses in the outsourcing contract
D. A code of conduct

Question 3

You want to implement an effective Information Management System that fits your organisation’s needs. What should you do first?

A. Determine the scope of the ISMS
B. Enhance management commitment
C. Establish information security objectives
D. Understand the organisation’s goals

Question 4

What is the main driver for a modern company to invest in information security?

A. Information is increasingly becoming organisations’ most valuable asset
B. Governments are implementing stricter information security laws
C. Customers are expecting companies to invest more in information security
D. Contracts and agreements often include information security clauses

Question 5

An information security audit is performed on a medium-size enterprise. The auditor concludes that the board of directors did not make any effort to ensure that asset owners and the information security department keep informed of information security issues. What is this an example of?

A. Lack of due care
B. Lack of due diligence
C. Lack of accountability
D. Lack of communication

Question 6

You are planning to outsource a process to an external service provider. You know that you will need to include information security clauses in your supplier agreement, but you have no idea what to include in those clauses. Now, you need to decide what requirements you should set for your supplier. What should you do first?

A. Carry out risk assessments to determine the security implications of outsourcing the process
B. Contract a third party to perform a background check on your potential supplier
C. Review ISO 27002 and select the controls that may apply to the outsourced activities
D. Decide what encryption methods you want your supplier to use

Question 7

A social engineer gains access to your colleague's username and password through a phishing mail. Which security property has been compromised?

A. Availability
B. Confidentiality
C. Integrity
D. Authenticity

Question 8

Susie claims that she was harassed by her colleague, Pete. She talks to a counsellor about her situation. Consequently, the counsellor notifies Susie's manager. The manager decides to take disciplinary action against Pete. As proof, he presents Pete with a copy of e-mails exchanged between Susie and the counsellor. Later on, Susie decides to withdraw the allegation. She says she never sent those e-mails to the counsellor. Which security principle is involved in this dispute?

A. Authenticity
B. Integrity
C. Authentication
D. Non-repudiation

Question 9

Which term refers to an event that has a disruptive effect on an organisation's information provision?

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

Question 10

What is the main goal of risk management?

A. To assess the threats IT resources are exposed to
B. To determine the damage that may be caused by security incidents
C. To ensure that all risks remain at an acceptable level
D. To determine the likelihood that a risk will occur

Question 11

Your colleagues regularly leave important documents in the printer tray. Which reliability aspect is compromised through this practice?

A. Confidentiality
B. Integrity
C. Authenticity
D. Availability

Question 12

Your colleague is trying to figure out what consequences your company would face if the web server were hacked. He asks you and the asset owner to select the most appropriate impact category from a pre-defined list. What is your colleague doing?

A. He is performing a quantitative risk analysis
B. He is performing a cost-benefit analysis
C. He is performing a qualitative risk analysis
D. He is performing a loss expectancy analysis

Question 13

An organisation stores its offline backup media in the same secured zone as the server. What risk is the organisation running?

A. Responsibility for the backup is not clearly assigned
B. After a fire, the information system cannot be recovered
C. After a server crash, it would take much time to make the system operational again
D. A power failure could compromise both the server and the backup media

Question 14

Which situation best illustrates the importance of 'the human element' in information security?

A. The use of a memory stick results in a malware infection
B. There is too much dust in the server room
C. The server room is hit by lightning
D. New laws impose stricter requirements on handling personal data

Question 15

You receive a phone call. The caller claims that he works for a large tech company, which has been hired by your organisation to improve security. He asks for your username and password in order to run a security scan on your PC. What type of threat is this?

A. Social engineering
B. Logic bomb
C. Worm
D. Malware

Question 16

Which type of malware builds a network of compromised computers?

A. Worm
B. Trojan
C. Spyware
D. Botnet

Question 17

Which is an example of indirect damage caused by fire?

A. Water from the sprinkler system damages the floor.
B. Computer and network equipment burn down.
C. The backup tapes melt in the fire.
D. The smoke discolours the walls.

Question 18

You have carried out a risk analysis. Now, you would like to determine your risk strategy. You decide to take sufficient measures to safeguard the continuity of your organisation, but you only do what is strictly necessary to keep your organisation functioning. What risk attitude does this approach reflect?

A. Risk-seeking
B. Risk-neutral
C. Risk-averse
D. Risk-tolerant

Question 19

What is the goal of a strategic information security policy?

A. To provide details that concretise the information security plan
B. To provide insight into threats and their potential impact
C. To provide management direction and support for information security
D. To document the outcomes of risk analyses and the selection of mitigation measures

Question 20

A security officer finds a virus-infected workstation. The infection was caused by a targeted phishing mail which contained a Word document with a malicious macro in it. What would be the best way to avoid similar incidents in the future?

A. Installing ‘proofing tools’
B. Updating the firewall
C. Adopting a new risk strategy
D. Starting an awareness campaign

Question 21

A manager discovers that his staff regularly use the corporate email system to send personal messages. What should the manager do to reduce this phenomenon?

A. Implement a sanctions policy
B. Implement privacy rules
C. Set up a monitoring system
D. Introduce a code of conduct

Question 22

After an office fire, all employees are moved to a new permanent location. What type of security measure is this?

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

Question 23

A large organisation's help desk receives a phone call from an employee. The employee says that she has accidentally deleted several important files from her computer. She requests the help desk to e-mail her the backup copies of the files. How should the help desk proceed?

A. Ask the caller to provide her username and e-mail address
B. Verify caller ID, full name and corporate e-mail address
C. Contact a member of the support staff
D. Send the files to the e-mail address as requested

Question 24

During a routine check, a potentially compromised network device is found. The device is immediately isolated from the network. What type of security measure is this?

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

Question 25

What is the main goal of information classification?

A. To facilitate information analysis and corporate decision-making
B. To identify the required level of protection and appropriate security measures
C. To identify information that should be covered in the organisation's telework policy
D. To identify privacy and data protection risks

Question 26

Who has ultimate responsibility for changing server configurations?

A. The asset owner
B. The system administrator
C. The change manager
D. The security manager

Question 27

A company experiences an information security incident. Nobody knows whether the affected system should be isolated, because the company has no policies or procedures that would describe who has authority to make such a decision. What would you do to solve this issue and prevent similar ones in the future?

A. Authorise the incident response team to make the final decision in similar cases
B. Implement a procedure that requires the incident response team to obtain the asset owner's approval
C. Compile a list of security measures approved by management and authorise the incident response team to take those measures
D. Authorise the incident manager to make the final decision in similar cases

Question 28

Management approves a new information security policy and publishes it on the intranet. After some time, it becomes clear that an employee is not abiding by the policy. When the employee is asked to explain himself, he claims that he did not know about the policy. What should management do to avoid similar problems in the future?

A. Managers should actively communicate policy changes to all staff
B. Managers should explicitly state that all staff must follow policy changes
C. Managers should publish new policies on multiple platforms, not just the intranet
D. Managers should require employees to formally acknowledge receipt of new policies

Question 29

A computer room is protected by a biometric entry system. Only administrators are registered in the system, which means no one else can access the computer room. Ideally, what additional measure should the organisation implement to ensure the effectiveness of this control?

A. External service technicians should also be registered in the system as administrators
B. The organisation should maintain the physical access control logs in a separate system
C. The organisation should communicate to all staff that only administrators can access the computer room
D. The organisation should draw up a procedure describing how the list of authorised individuals is maintained

Question 30

An organisation implements a classic physical security zoning model. The model consists of 4 protection rings: public, internal, sensitive and secret. Ideally, in which ring should the organisation place HR employees' workstations?

A. Internal
B. Public
C. Sensitive
D. Secret

Question 31

You work in an organisation's IT department. Your management has long neglected information security. Now as data breaches are becoming more frequent, the managers are looking for ways to increase computer security. You are asked to propose effective security measures. What should you do first to ensure the effective protection of your organisation's information assets?

A. Suggest that management designate a person responsible for information security
B. Encrypt all sensitive information and implement two-factor authentication
C. Draw up a telework policy and a 'bring your own device' policy
D. Implement an access control and an incident management procedure

Question 32

Marcel Bicsma wants to send a secure e-mail to his brother Vincent. Marcel encrypts the e-mail and digitally signs it before sending it to Vincent. What does Vincent need to verify that the e-mail truly comes from Marcel?

A. Marcel's public key
B. Marcel's private key
C. Vincent's public key
D. Vincent's private key

Question 33

Who has ultimate responsibility for allocating information security roles and responsibilities?

A. Senior management
B. The Chief Information Security Officer
C. The Data Protection Officer
D. The Chief Information Officer

Question 34

Which statement about access control is FALSE?

A. Access control policies should address both physical and logical access control
B. Access control policies should only apply to the organisation's employees
C. Access control policies should contain rules on removing user access rights
D. Access control policies should contain rules on reviewing user access rights

Question 35

What role does biometrics play in granting access to an information system?

A. Identification
B. Authentication
C. Authorisation
D. Accounting

Question 36

Why should organisations regularly test their Disaster Recovery Plan (DRP)?

A. Without testing, the organisation cannot assess whether its security measures and incident procedures work in practice
B. Without testing, the organisation cannot demonstrate that its DRP is suitable for the organisation's operational processes
C. Without testing, the organisation cannot ensure that off-site backups are available when needed
D. Without testing, the organisation cannot update its DRP every year as required by ISO 27001

Question 37

Segregation of duties is important because:

A. It helps to prevent fraud and error
B. It helps to reduce personnel's workload
C. It helps to reduce operational costs
D. It eliminates all information security risks

Question 38

How does malware get on your computer?

A. You click on suspicious e-mail attachments and links
B. You visit a compromised website
C. You use a USB drive you picked up from a public location
D. All of the above

Question 39

Which is a good definition of 'reliability'?

A. The extent to which it can be guaranteed that information is true and safe to use
B. The extent to which information is authentic and correct
C. The extent to which the confidentiality, integrity and availability of information can be guaranteed
D. The extent to which it is possible to verify that information cannot be misused by malicious agents

Question 40

You store highly confidential information on a server. The server is in a physically secure room. Now, you want to ensure the security of the data stored on the server. Which measure should you take?

A. Applying full disk encryption
B. Using a firewall with strict rules
C. Installing a host integrity monitoring system
D. Installing data leak prevention software

Answers

Question 1

The correct answer is D.

An Information Security Management System addresses all aspects of information security (people, processes and technology), and thereby enables you to build a system which takes into account all IT and non-IT-related risks to the security of information.

Section 404 of the Sarbanes-Oxley Act requires publicly traded companies to establish, document and maintain internal controls and procedures for financial reporting. Compliance with Section 404 requires the implementation of information security measures (e.g. effective access control), but Section 404 does not address all aspects of information security.

IT Service Management refers to the design, delivery, operation and control of information technology services. It only covers IT-related areas.

Your organisation's corporate strategy plays a role in making strategic decisions about information security. Aligning corporate strategy with information security policies and objectives is crucial, but it is only a component of effective information security.

Module 1: Information Security Management System (ISO/IEC 27001) & Code of Practice for Information Security Controls (ISO/IEC 27002)

Question 2

The correct answer is B.

Normative standards cover a variety of areas and contain uniform requirements. Compliance with the requirements is assessed by an objective, independent party (an auditor).

Best practices are less likely to cover all your needs. A set of best practices may not address as many areas as a standard. Compliance with best practices is also less measurable than compliance with a normative standard.

Most contracts do not cover operational detail. Therefore, most security clauses only address a limited number of relevant areas.

A code of conduct only addresses people's behaviour.

Module 1: Information Security Management System (ISO/IEC 27001) & Code of Practice for Information Security Controls (ISO/IEC 27002)

Question 3

The correct answer is D.

The scope of the ISMS is determined based on the organisation's goals and the requirements of interested parties relevant to information security (e.g. the needs of customers who expect their information to be protected). To determine the scope of the ISMS, you should fully understand the business needs the ISMS should cover. Enhancing management commitment and establishing information security objectives follow after you have determined the ISMS scope.

Module 1: Information Security Management System (ISO/IEC 27001) & Code of Practice for Information Security Controls (ISO/IEC 27002)

Question 4

The correct answer is A.

More and more business reports confirm that modern organisations attribute more value to their intangible assets than to their tangible assets, with information being the prime intangible asset. With the digital economy, information has become an important production factor. This is why modern organisations increasingly invest in information security, even beyond legal obligations, customer expectations and liabilities.

Module 2: Information and Security

Question 5

The correct answer is B.

In information security, 'due diligence' refers to an organisation's responsibility to identify the potential risks that may threaten the organisation's information. If the asset owners and the information security department do not have the means to keep informed of information security issues, risks may remain undiscovered, which means the organisation is not practicing due diligence.

In information security, 'due care' means an organisation's responsibility to take appropriate measures to reduce information security risks to an acceptable level. In our scenario, the problem centres around being aware of information security risks, not taking measures to reduce the risks.

'Accountability' means that every action can be traced back to an individual. Being unaware of information security risks does not necessarily imply lack of accountability. Similarly, being unaware of information security risks does not necessarily imply lack of communication.

Module 2: Information and Security

Question 6

The correct answer is A.

First, you need to identify and evaluate the risks you will face if you outsource the process. Based on the risks, you can decide what you will require of your supplier and what actions you will take to ensure that your supplier meets your requirements.

Module 4 Approach and Organisation, Section: Internal Information Security Organisation

Question 7

The correct answer is B.

You do not know what the social engineer has done with your colleague's credentials. What you do know is that the social engineer has obtained information he or she should not have. Therefore, you conclude that confidentiality has been definitely compromised. Depending on what the attacker does next (change information, delete information or block access to information), integrity and availability may also be compromised.

Module 2: Information and Security

Question 8

The correct answer is D.

Non-repudiation is a legal concept. It assures that a statement's author cannot successfully deny their authorship. Non-repudiation techniques, such as e-mail tracking, allow you to prove to third parties what was communicated to the recipient, and sometimes even when the communication took place.

Authenticity is a technical concept. It refers to verifying that a message came from the said sender. Authenticity is usually verified through authentication. Authenticity and non-repudiation are closely related. Non-repudiation can only be achieved if the true identity of the originating party can be confirmed.

Integrity is the degree to which the information is complete, up to date and without errors. In our scenario, the question is not whether the e-mails are up to date and without errors, but whether Susie was the author of the e-mails.

Authentication is the process of verifying the identity of a person, process or device. A common example is entering a username and password when logging in to a website.

Module 2: Information and Security

Question 9

The correct answer is D.

Incident is an unexpected event which has an impact on the organisation's operations.

A vulnerability is a weakness in an object that could potentially allow an attacker to compromise the object. If the object is used in a particular environment, the vulnerability gives rise to a threat to that environment (the vulnerability becomes relevant). When the threat manifests itself (becomes reality), it poses a risk to the security of the particular environment, and results in a negative impact on the organisation's operations.

Module 3: Threats and Risks

Question 10

The correct answer is C.

Risk management aims to identify potential threat sources, assess the resulting risks, and identify appropriate measures to reduce the risks to an acceptable level. Information security risk management should cover all risks that have to do with the security of information, not only IT-related risks. Estimating potential damage and determining the likelihood of occurrence are important components of risk analysis, but they are not the main goals of risk management.

Module 3: Threats and Risks

Question 11

The correct answer is A.

If documents are left in the printer tray, confidentiality cannot be upheld. Unauthorised parties may gain access to the information the documents contain. Integrity is not likely to be affected, as printed documents cannot be changed easily. Authenticity is irrelevant in this context. Just because a document was left in the printer tray, the information does not become inauthentic. Finally, availability is not likely to be affected. Even if the print disappears, the information still exists in a digital form.

Module 2: Information and Security

Question 12

The correct answer is C.

In qualitative risk analysis, risks are rated in comparison to other risks. Impact categories are usually classified as ‘very high’, ‘high’, ‘medium’, and ‘low’. In quantitative risk analysis, risk values are calculated based on quantifiable parameters that are measured and derived, or based on statistics. A cost-benefit analysis is not aimed at evaluating risks. It assesses the value of an asset and the costs of securing that asset. Loss expectancy is the monetary value expected from the occurrence of a risk on an asset.

Module 3: Threats and Risks

Question 13

The correct answer is B.

If the backup and the server are kept in the same secured zone, a fire could destroy both. An important security measure is to store backups in a different physical location (preferably off-site) to ensure that the backups are not exposed to the same risks as the originals. Storing backups in the same secure zone as the server does not necessarily mean that responsibilities have not been properly assigned. A server crash will not affect offline backup media, which are not connected to the server. As the backup media are offline, they would not be affected by a power outage.

Module 2: Information and Security

Question 14

The correct answer is A.

‘The human element’ refers to problems that occur due to lack of awareness or due to (un)intentional behaviour that exposes the information assets to threats. Malware infection through the use of a found memory stick is a typical example of incidents caused by lack of awareness and careless behaviour. Answers B and C may indicate insufficient attention to the physical aspects of information security, which may result in compromising the availability of information. Answer D refers to what is expected of those who handle personal data, but is not necessarily linked to awareness or behaviour that may lead to the manifestation of threats.

Module 3: Threats and Risks

Question 15

The correct answer is A.

Social engineering is the use of deception to manipulate individuals into sharing confidential or personal information or into performing actions that may compromise security. A logic bomb is a set of instructions incorporated into a program. Malware is software that was designed to disrupt or gain access to a computer system. A worm is a small computer program that purposefully replicates itself.

Module 5: Security Measures

Question 16

The correct answer is A.

A worm is a small computer program capable of spreading itself through a network for malicious purposes. The result of a worm infection may be a botnet, a network of malware-infected computers that are remote-controlled by a command server. Trojan and Spyware do not necessarily build networks of infected devices.

Module 5: Security Measures

Question 17

The correct answer is A.

Damage caused by the sprinkler system is not a direct result of the fire, whereas the other damages are.

Module 3: Threats and Risks

Question 18

The correct answer is A.

Risk-seeking organisations only mitigate the risks that must be mitigated to keep the organisation functioning. They accept all the remaining risks, which might still be significant. Risk-neutral organisations strive to find a good balance between the potential loss and the costs of risk mitigation or incident resolution. Risk-averse organisations (such as banks or government institutions) strive to mitigate risks as much as possible, because their operations warrant a minimisation of the residual risks. In all three risk strategies, it is important to balance the costs of the mitigation measures against the potential loss that may result from the risk.

Module 3: Threats and Risks

Question 19

The correct answer is C.

A strategic information security policy is a high-level document, which sets the strategic direction, scope, and tone for the organisation's information security efforts. A strategic information security policy does not describe details and does not document threats, potential impact or risk analysis outcomes.

Module 1: Information Security Management System (ISO/IEC 27001) & Code of Practice for Information Security Controls (ISO/IEC 27002)

Module 4: Approach and Organisation

Question 20

The correct answer is D.

The best way to avoid falling victim to phishing is to raise information security awareness and train staff on how to identify phishing scams. Adopting a new risk strategy would not prevent employees from clicking on malicious links and e-mails. Firewalls are an important means of protection, but they filter based on the source and the destination address. Unlike intrusion prevention systems or antivirus/malware filters, firewalls do not filter based on the contents of a message. Proofing tools are used to check spelling and grammar. Such tools cannot distinguish a malicious macro from a legitimate one.

Module 4: Approach and Organisation

Question 21

The correct answer is D.

A code of conduct describes acceptable employee behaviours. An information security code of conduct may cover confidentiality and appropriate use of the organisation's equipment and facilities. For example, a code of conduct may state that private use of the organisation's assets is permitted only during lunch breaks, or not at all. A code of conduct may include sanctions, but it has been proven that sanctions alone do not effectively change employee behaviour. For employees to change their behaviour, they need to know what is expected of them and why. Privacy rules protect employees' personal data, but they do not limit the use of the organisation's assets. Setting up a monitoring system requires careful consideration, as it is likely to result in privacy issues.

Module 4: Approach and Organisation

Question 22

The correct answer is C.

Corrective measures are aimed at recovering from the damage caused by a security incident. Relocating employees after a fire is an attempt to recover operations after the damage has occurred. Repressive measures aim to limit the potential consequences of a security incident. Such measures are put into effect before the incident occurs. Preventive measures are taken to keep incidents from arising. Detective measures are taken in order to detect incidents.

Module 5: Security Measures

Question 23

The correct answer is B.

This might be a social engineering attempt. The help desk must make sure that they do not send the documents to an unauthorised party. They may contact the employee at a previously documented phone number to confirm her identity, but they cannot exclude the possibility that meanwhile an attacker has gained access to the employee's phone. All information given by the caller should be considered untrustworthy, as it may have been collected through illicit means. It is wise to verify the caller's identity and only send the files to a corporate e-mail address. If highly confidential documents are concerned, the help desk may decide not to send the files at all.

Module 5: Security Measures

Question 24

The correct answer is C.

Repressive measures limit the consequences of a potential security incident. By isolating the potentially compromised device, we may prevent malware from spreading and affecting other devices connected to the same network. Corrective measures are used to recover from the damage caused by a security incident. A corrective measure would be, for example, reinstalling the affected device. Detective measures would be any measures that made it possible to discover that the device had been compromised. Preventive measures would be any measures aimed at preventing incidents that may affect the device.

Module 5: Security Measures

Question 25

The correct answer is B.

To ensure the appropriate protection of information, we should classify information in terms of its security needs and importance to the organisation. Classifying and labelling information (assigning a confidentiality level to each category) allows us to define how much protection is needed and assign security priorities accordingly.

Module 5: Security Measures

Question 26

The correct answer is A.

Effective information security requires the designation of asset owners. Asset owners have ultimate responsibility for their assets, including the proper protection of the assets. Asset owners may delegate the implementation of specific controls to another party, such as a system administrator, but ultimate responsibility for the asset cannot be transferred to another party.

Change managers have a supervisory function. They oversee the transition or transformation of an organisation's technology or processes, but they do not bear responsibility for specific assets or processes. Security managers are responsible for the overall quality of the security management process. They develop and implement security policies and procedures and they may advise asset or process owners on security, but they are not responsible for specific assets or processes.

Module 4: Approach and Organisation

Question 27

The correct answer is A.

During an incident, you may not have time to discuss what to do. Depending on the type of the incident, it might be critical to take decisive action at the shortest notice. Obtaining the asset owner's approval takes time, and you can never be sure that the asset owner will be available when you need them. A pre-compiled list is not an effective solution, because it is impossible to foresee all potential scenarios. Finally, an incident manager is not necessarily a security specialist, and may not be able to make the right decision. Therefore, the best option is to authorise the incident management team to make decisions on the spot, provided that there is no procedure in place. Post-mortem evaluations and reports enable the incident management team to improve the effectiveness of the team and the existing procedures.

Module 4: Approach and Organisation

Question 28

The correct answer is A.

Active communication of policies (and policy changes) is crucial to ensure that all employees understand the rules they must follow. Active communication may include publishing the policy on the intranet and other platforms, conducting personal interviews, and organising trainings. Merely publishing the policy and requiring employees to acknowledge their receipt/understanding of the policy would not result in true understanding and compliance.

Module 4: Approach and Organisation

Question 29

The correct answer is D.

Effective access control requires two things: a means to limit access to the authorised individuals (i.e. the biometric entry system), and a means to administer the list of authorisations. To ensure that access is granted on an ‘as-needed’ basis, there must be a procedure that defines how access is granted, maintained and revoked. The lists should be audited regularly to ensure the proper maintenance of authorisations. Logging access is useful, but it does not prevent the wrong people from gaining access to the asset if the list of authorisations is not properly maintained. You may or may not decide to register external service technicians as administrators. If you decide not to grant access to external technicians, you can still have them enter under the supervision of an administrator.

Module 5: Security Measures

Question 30

The correct answer is C.

HR workstations should be placed in the ‘sensitive’ ring. Access to this ring is role-based, which means access is granted to all employees who need it in order to perform their jobs. The public ring is available to everyone, including external parties. Placing the workstations in the public ring would not provide sufficient protection. The internal ring is accessible to all employees. Placing the workstations in the internal ring would result in employees having unnecessary access to the workstations, which is a significant security risk. The secret ring is only accessible on a strict ‘as-needed’ basis. Placing the workstations in the secret ring would be an unnecessarily rigid measure, which would likely have a negative impact on operational effectiveness.

Module 5: Security Measures

Question 31

The correct answer is A.

Before drawing up policies, implementing procedures, or adopting security measures, you need to allocate information security roles and responsibilities. For effective information security, all information security responsibilities should be clearly defined, explicitly assigned, and acknowledged by management.

Module 4: Approach and Organisation

Question 32

The correct answer is A.

Marcel uses his private key to create the digital signature, and Vincent uses Marcel's public key to decrypt the signature and verify that the e-mail came from Marcel. As long as Vincent can reasonably assume that no one else but Marcel has access to Marcel's private key, Vincent has proof that is was indeed Marcel who signed the e-mail. The fact that the message was also encrypted is not relevant to the verification of the signature.

Module 5: Security Measures

Question 33

The correct answer is A.

According to ISO 27001, management should demonstrate its support and commitment to information security by implementing and maintaining an information security policy. The information security policy should contain a clear description of information security roles and responsibilities, including the responsibilities of users, staff members, managers, senior management and third-party service providers.

Module 4: Approach and Organisation

Question 34

The correct answer is B.

Access control is aimed at preventing unauthorised access to an organisation's assets, including information systems. Access control can only be effective if it covers the organisation's employees and all external party users who should have access to the organisation's assets. For effective access control, it is essential to implement procedures describing how authorisation lists will be kept accurate and up to date.

Module 5: Security Measures

Question 35

The correct answer is B.

Access to an information system is granted in three steps: identification, authentication and authorisation. In the identification phase, the user claims an identity, for example by presenting a username. The authentication process verifies the claimed identity through the use of a password, a token or biometric data, such as a fingerprint. The authorisation process determines what tasks the individual (the verified identity) may perform. Accounting refers to tracking and recording the activities undertaken by the individual while active in the system.

Module 5: Security Measures

Question 36

The correct answer is A.

Without testing (preferably through simulations and exercises), the organisation cannot determine whether its security measures are appropriate and effective. Organisations have no obligation to ‘demonstrate their DRP’s suitability’ or ‘update their DRP every year’, thus these are not relevant reasons for testing. Testing whether off-site backups can be used to restore data in the event of a disaster may be part of a DRP, but a DRP’s scope is much wider than that.

Module 5: Security Measures

Question 37

The correct answer is A.

The main reason to segregate conflicting areas of responsibility (for example, the acquisition of goods and record keeping) is to prevent fraud and error. If different individuals are responsible for sub-processes within the same process, they would have to cooperate to commit fraud. Segregation of duties may reduce workload, but it does not reduce operational costs or eliminate all information security risks.

Module 5: Security Measures

Question 38

The correct answer is D.

Clicking on suspicious e-mail attachments, visiting a compromised website or using a found USB drive can all lead to installing malware on your computer.

Module 5: Security Measures

Question 39

The correct answer is C.

Reliability refers to the extent to which the confidentiality, integrity and availability of information can be guaranteed.

Module 2: Information and Security

Question 40

The correct answer is D.

Full disk encryption on a system that is always on and that is connected to a network will not help protect the data, as the encryption will be completely transparent to the running processes. A firewall or IDS might help filter traffic to or from untrusted sources, but you should also consider the possibility that no malware is used to exfiltrate the data. More importantly, you should consider the possibility that the data is exfiltrated by one of your own employees.

Module 3: Threats and Risks

Hoewel de Security Academy zich heeft ingespannen dit te voorkomen kan niet worden uitgesloten dat dit document desondanks toch onvolkomenheden bevat. Een ieder die zijn acties baseert op de inhoud van dit document doet dit dientengevolge op eigen risico en is zich ervan bewust dat de Security Academy niet aansprakelijk kan worden gesteld voor eventuele schade die uit dergelijke acties voortvloeit.

De auteurs van dit document hebben hun best gedaan eventuele rechthebbenden, anders dan de Security Academy, te achterhalen. Mocht u een rechthebbende zijn, vertegenwoordigen of kennen en van mening zijn dat dit document ten onrechte gebruik maakt van auteursrechtelijk beschermd materiaal, neemt u dan alstublieft contact op met de Security Academy.