Sample Exam

Edition 202506

Copyright © EXIN Holding B.V. 2025. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Content

Introduction

This is the EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 30 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct, unless otherwise stated.

The maximum number of points that can be obtained for this exam is 30. Each correct answer is worth 1 point. You need 20 points or more to pass the exam.

The time allowed for this exam is 90 minutes.

Good luck!

Sample exam

1 / 30
Which is a **key** element of security strategy development?

A) Description of how the services are being supported
B) Policy that does not conflict with the law of the organization's country
C) Relevant control objectives
D) Return on Investment (ROI)

2 / 30
An organization has several suppliers which contribute to the delivery and support of end-to-end services.

Which capability should the organization invest in **primarily** to minimize the information security issues originating from its suppliers?

A) Audits
B) Governance
C) Risk management
D) Training

3 / 30
The security manager is responsible for defining the security controls for a company. The company is selecting a supplier to host the web-facing ordering system.

What is the **most** important aspect the security manager should look for?

A) A standard for due care
B) A standard for due diligence
C) Benchmarking
D) Best security practices

4 / 30
Security controls are defined based on the security classification of a data element.

Who is responsible for the security classification of a data element?

A) The board of directors, that runs the company
B) The data custodian, who manages the use of the data
C) The process owner, who governs the process
D) The system owner, who safeguards the information system

5 / 30
A risk manager is asked to perform a complete risk assessment for a company.

What is the **best** method to identify **most** of the threats to the company?

A) Have a brainstorm with representatives of all stakeholders
B) Interview top management
C) Send a checklist for threat identification to all staff involved in information security

6 / 30
Information security management is currently being implemented in a company that sells books. The project leader for the information security project understands that the risk identification process requires her to list organizational assets arranged in order of importance and she is working with the financial manager to develop this list. The weight of importance is based on the following criteria: impact on revenue (30%), impact on profitability (40%) and impact on public image (30%).

The financial manager has come up with four important information assets:
- Supplier orders (outbound)
- Customer order via SSL (inbound)
- Supplier fulfillment advice (inbound)
- Customer service request via e-mail (inbound)

What asset ranks the highest based on the impact criteria?

A) Supplier orders (outbound)
B) Customer order via SSL (inbound)
C) Supplier fulfillment advice (inbound)
D) Customer service request via e-mail (inbound)

7 / 30
An operations manager wants some advice about opening a second data center as a hot standby location.

What would the information security officer (ISO) advise the operations manager to do?

A) Ensure that network and power supply are made redundant and from different providers
B) Ensure that physical access is only granted to specific operators
C) Ensure that the company will not be a victim of the Patriot Act legislation
D) Ensure that the location has a different physical risk profile than the primary location

8 / 30
A large transportation company has adopted the standard for information security and needs to set up controls for its software development department, which they will outsource. An external consultant has been appointed to ensure that security controls consistent with the code of practice will be implemented over the complete supply chain for software development in the new outsourced situation.

What control should be put in place to guarantee availability of the source code should one of the partners in the supply chain go out of business?

A) Acceptance testing
B) Effective documentation
C) Escrow arrangements
D) Licensing agreements

9 / 30
The scope of risk management is not limited to the organizational processes alone. It should also be embedded in the project management methodology. An information security risk assessment, for example, should be conducted at an early stage of each project. When implementing project risk management, it is necessary to consider the scope of this project.

What should be included in the scope of project risk management for standard projects?

A) It is necessary to prepare for the maximum risk level and therefore implement important sub-processes like risk identification, quantification, response development and response control.
B) It is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project, because a project organization is only a small part of the organization.
C) It should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.

10 / 30
Which strategy is **best** to implement when a risk assessment points out that a specific vulnerability can be exploited?

A) Implementation of a risk management framework
B) Implementation of an information security control
C) Implementation of anti-virus software

11 / 30
An organization has convinced its senior leadership of the need for a formal approach to risk management. Senior leadership has raised concerns over the costs of the proposed risk controls.

Which statement should be included in the business case for the implementation of risk controls?

A) Controls are the primary means of improving the organization's risk profile.
B) Controls determine the organization's risk mitigation options.
C) Controls help the organization to identify its most critical assets.
D) Controls will provide the organization with information about asset vulnerabilities.

12 / 30
An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization's risk appetite.

When has the risk assessment program accomplished its **primary** goal?

A) Once the controls are implemented
B) Once the transference of the risk is complete
C) When decision makers have been informed of uncontrolled risks, and it is decided to leave the risks in place
D) When the risk analysis has been completed, and the results are documented in the risk report

13 / 30
The maintenance of an information security program requires a continuous process. This requires inputs from the many different factors that will influence its success.

Which is an input influence that would require the process to change?

A) Policy
B) Risk assessment
C) Security plan

14 / 30
The information security officer (ISO) for a global company has just received a management review of the information security policy.

What should this output include?

A) Feedback from interested parties
B) Improvement of control objectives and controls
C) Status of preventive and corrective actions

15 / 30
An organization is implementing information security incident handling. It already has a mechanism for personnel to report observed or suspected information security events, but these are not handled well once they are reported.

The organization has put relevant processes, roles, and responsibilities in place. It is now moving on to implement other activities needed for information security incident handling.

What is **not** an activity to implement information security incident handling?

A) Agree on how to prevent information security incidents by using knowledge gained from incidents to strengthen and improve information security controls
B) Define and communicate procedures on information security incident response that should be carried out by competent staff
C) Devise a categorization and prioritization scheme that can be used to categorize information security events as information security incidents
D) Implement procedures to collect and preserve evidence related to information security events for use in any necessary disciplinary or legal actions
E) Set up rules to control physical and logical access to information and other associated assets to prevent information security incidents

16 / 30
The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

A) The business continuity plan
B) The disaster recovery plan
C) The incident response plan
D) The risk treatment plan

17 / 30
Whose responsibility is it to coordinate an organization's security awareness program?

A) Everyone in the organization
B) Information security management
C) The IT department
D) The secretary of the CIO

18 / 30
Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer (ISO) wants to know the mindset of the employees towards information security controls.

How does the ISO get an impression quickly?

A) By checking the internet data stream
B) By determining if there are viruses on the network
C) By walking around the office after normal business hours

19 / 30
The business continuity manager asks for input for the contingency plan.

Which should be the business continuity manager's **first** activity?

A) Define the scope
B) Identify critical business functions
C) Test the plan

20 / 30
A security architect argues with the internal fire prevention team about the statement in the information security policy that doors to confidential areas should always be locked at all times. The emergency response team wants access to those areas in case of fire.

What is the **best** solution to this dilemma?

A) The doors should stay closed in case of fire to prevent access to confidential areas.
B) The doors will automatically open in case of fire.
C) The security architect will be informed when there is a fire.

21 / 30
What is the **main** advantage of using an open design of the security architecture?

A) Open designs are easy to set up.
B) Open designs are tested a lot.
C) Open designs have a lot of extra features.

22 / 30
What is a characteristic of security architecture?

A) Security architecture completely defines implementation rules.
B) Security architecture follows strategy.
C) Security architecture is secondary.

23 / 30
Why is it important to define which security services will be provided?

A) To better align the information security requirements and the customer service
B) To determine the information security strategy of an organization
C) To ensure an organization is compliant with the requirements of ISO/IEC 27001
D) To understand the scope of the information security management system (ISMS)

24 / 30
Which security item is designed to see harmful traffic and ensure the intrusion is prevented and blocked?

A) Firewall
B) Intrusion prevention system (IPS)
C) Virtual private network (VPN)

25 / 30
The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business e-mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD), and organized an awareness training regarding BYOD.

What other control should the security manager propose to prevent data loss in case of theft or loss of the personal device?

A) Do not grant the wish until stable integration of business functions on private devices is possible
B) Encrypt the local storage and network connections
C) Implement strong authentication using tokens with one-time passwords
D) Install anti-malware and a firewall to prevent infection

26 / 30
Why are the security elements in the IT infrastructure important?

A) To enable business continuity of the IT infrastructure
B) To manage information security incidents which impact the IT infrastructure
C) To prevent unauthorized physical access to the IT infrastructure
D) To protect the information assets which are on the IT infrastructure

27 / 30
Zoning is a security control to separate physical areas with different security levels. Zones with higher security levels can be secured by more controls. The security manager of a hotel is responsible for security and is considering different zones for the hotel.

What business functions should be combined into one security zone?

A) Boardroom and general office space
B) Fitness area and storage facility
C) Hotel rooms and public bar
D) Public restaurant and lobby

28 / 30
A security manager for a large company has the task to achieve physical protection for corporate data stores.

Through which control can physical protection be achieved?

A) Having visitors sign in and out of the corporate datacenter
B) Install a firewall to prevent access to the network infrastructure
C) Using key cards as access control for employees needing access
D) Writing a policy stating who may have access to the company

29 / 30
Knowing that physical security controls are a very important part of an information security program, the information security team is asked to design and then implement a security perimeter for a department that is setting up some new data systems.

According to ISO/IEC 27001, which is the **most** important guideline that needs to be considered when establishing this perimeter?

A) A two-person support model
B) Installing cameras and alarms
C) Strength of the perimeter in line with the data's value
D) System logging and monitoring

30 / 30
The human resource manager for an organization asked what she could do as a quick win in the area of employment and hiring to help strengthen the organization’s data security program according to ISO/IEC 27001.

What should the advice be?

A) Do background checks
B) Implement security policy
C) Place revolving gates at the entrance

Answer key

1 / 30
Which is a **key** element of security strategy development?

A) Description of how the services are being supported
B) Policy that does not conflict with the law of the organization's country
C) Relevant control objectives
D) Return on Investment (ROI)

A) Incorrect. This answer does not pertain to defining an overall security strategy and is more focused on the service level agreement (SLA).
B) Incorrect. This answer does not pertain to defining an overall security strategy and is more related to policy development.
C) Correct. Having relevant control objectives is a key element to the development of security strategy. (Literature: A, Slide 013)
D) Incorrect. This answer does not pertain to defining an overall security strategy and is more related to financial forecasting and budgeting.

2 / 30
An organization has several suppliers which contribute to the delivery and support of end-to-end services.

Which capability should the organization invest in **primarily** to minimize the information security issues originating from its suppliers?

A) Audits
B) Governance
C) Risk management
D) Training

A) Incorrect. Audits are essential to ensure that agreed activities are being performed, but it would be better to invest in governance capabilities to ensure that there are policies which direct the behavior of all parties involved in the service provision.
B) Correct. Governance is the overlying capability which directs an organization’s policies and processes, including the suppliers’ involvement. Governance handles the evaluation, direction and monitoring of the organization in topics like information security. Governance works on developing policies, receiving monitoring information, evaluating this information based on the policies of the organization, and providing direction to management to make changes where necessary. (Literature: A, Slide 018)
C) Incorrect. Risk management has a number of activities which would be useful in this scenario, but strengthening the organization’s governance capabilities will increase the likelihood of stronger overall control of the activities of all parties involved in service provision.
D) Incorrect. It is important to invest in training, but a robust governance capability will help the organization to develop policies which direct the behavior of all parties involved in service provision.

3 / 30
The security manager is responsible for defining the security controls for a company. The company is selecting a supplier to host the web-facing ordering system.

What is the **most** important aspect the security manager should look for?

A) A standard for due care
B) A standard for due diligence
C) Benchmarking
D) Best security practices

A) Incorrect. A standard for due care symbolizes a minimum level of security.
B) Incorrect. Due diligence means that the supplier meets a standard requirement. This is not necessarily the standard.
C) Incorrect. Benchmarking is a technique used to compare organizations with similar business, maturity and markets.
D) Correct. Best security practices are the best in class for a given industry or line of work. This is what the security manager will be looking for in a supplier. (Literature: A, Slide 024)

4 / 30
Security controls are defined based on the security classification of a data element.

Who is responsible for the security classification of a data element?

A) The board of directors, that runs the company
B) The data custodian, who manages the use of the data
C) The process owner, who governs the process
D) The system owner, who safeguards the information system

A) Incorrect. The board is overall accountable for any business process, but the responsibility for exercising all duties is delegated.
B) Incorrect. A custodian is responsible for defining and managing the requirements towards any data element as far as it concerns compliancy to laws and regulations, but also for the use of data by different parties and processes in the form of data contracts.
C) Correct. Any data element is an object of control of a business process. The process owner is the only person who can identify if a data element is critical within the organization. (Literature: A, Slide 045)
D) Incorrect. The system owner is responsible for implementing the controls as required by the defined confidentiality, integrity, availability (CIA) classification.

5 / 30
A risk manager is asked to perform a complete risk assessment for a company.

What is the **best** method to identify **most** of the threats to the company?

A) Have a brainstorm with representatives of all stakeholders
B) Interview top management
C) Send a checklist for threat identification to all staff involved in information security

A) Correct. A brainstorm with all stakeholders makes sure that all perspectives are represented. (Literature: A, Slide 030)
B) Incorrect. Top management can oversee a lot of threats but not all of them. There is a better way to identify more threats.
C) Incorrect. Staff involved in information security cannot see all the threats. There is a better way to identify more threats.

6 / 30
Information security management is currently being implemented in a company that sells books. The project leader for the information security project understands that the risk identification process requires her to list organizational assets arranged in order of importance and she is working with the financial manager to develop this list. The weight of importance is based on the following criteria: impact on revenue (30%), impact on profitability (40%) and impact on public image (30%).

The financial manager has come up with four important information assets:
- Supplier orders (outbound)
- Customer order via SSL (inbound)
- Supplier fulfillment advice (inbound)
- Customer service request via e-mail (inbound)

What asset ranks the highest based on the impact criteria?

A) Supplier orders (outbound)
B) Customer order via SSL (inbound)
C) Supplier fulfillment advice (inbound)
D) Customer service request via e-mail (inbound)

A) Incorrect. When supplier orders cannot be sent out, it will have a high impact on the possibility to create revenue and make profit. However, it will cause customer orders to be delayed. Some customers may move their purchase to a competitor. This will also impact on profitability and public image. Normally, revenue and profit will still be realized.
B) Correct. When a customer is not able to order online, they will immediately order from another source. The impact on revenue, profitability and public image will be maximal. (Literature: A, Slide 037)
C) Incorrect. When supplier delivery on call orders cannot be sent out, it will have a high impact on the possibility to create revenue and make profit. Besides, it will cause customer orders to be delayed. Some customers may move their purchase to a competitor. This will also impact on profitability and public image. Eventually, revenue and profit will be realized.
D) Incorrect. When customer service requests cannot be fulfilled, it will have a high impact on public image. The impact on revenue and profitability will be significantly lower than compared to elements of the logistics process failing.

7 / 30
An operations manager wants some advice about opening a second data center as a hot standby location.

What would the information security officer (ISO) advise the operations manager to do?

A) Ensure that network and power supply are made redundant and from different providers
B) Ensure that physical access is only granted to specific operators
C) Ensure that the company will not be a victim of the Patriot Act legislation
D) Ensure that the location has a different physical risk profile than the primary location

A) Incorrect. This is only part of the risk profile.
B) Incorrect. This is a general security control.
C) Incorrect. This is not a physical security risk. It is a legislation problem.
D) Correct. Since it is a backup location, it is wise to make sure that it has a different risk profile. (Literature: A, Slide 050)

8 / 30
A large transportation company has adopted the standard for information security and needs to set up controls for its software development department, which they will outsource. An external consultant has been appointed to ensure that security controls consistent with the code of practice will be implemented over the complete supply chain for software development in the new outsourced situation.

What control should be put in place to guarantee availability of the source code should one of the partners in the supply chain go out of business?

A) Acceptance testing
B) Effective documentation
C) Escrow arrangements
D) Licensing agreements

A) Incorrect. Acceptance testing is a mechanism to ensure that the deliverables of the development process meet the quality criteria of the customer. The customer gets no access to the source code.
B) Incorrect. Effective documentation is a general requirement for all controls. Source code is not part of documentation that is accessible to the customer.
C) Correct. Escrow arrangements will ensure that software source code is stored at a neutral site. The source code is accessible to the customer when certain criteria are met, for example if the supplier goes into receivership. (Literature: A, Slide 050)
D) Incorrect. Licensing agreements only ensure code ownership and intellectual property rights. They cannot guarantee access to the source code for the customer should the supplier go out of business.

9 / 30
The scope of risk management is not limited to the organizational processes alone. It should also be embedded in the project management methodology. An information security risk assessment, for example, should be conducted at an early stage of each project. When implementing project risk management, it is necessary to consider the scope of this project.

What should be included in the scope of project risk management for standard projects?

A) It is necessary to prepare for the maximum risk level and therefore implement important sub-processes like risk identification, quantification, response development and response control.
B) It is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project, because a project organization is only a small part of the organization.
C) It should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.

A) Incorrect. Implementation of all possible sub-processes is only applicable to high-risk project scenarios like security projects or in mission critical environments. Only in those environments it should be the generic approach.
B) Correct. Generally, this scope should be sufficient for most projects. That said, it is necessary to allow for larger and more critical projects, so there should also be a process to escalate to more detailed risk management processes for larger/more comprehensive enterprise projects. Therefore, it is necessary to implement a generic scope like is done for the organization as a whole. (Literature: A, Slide 047)
C) Incorrect. Project risk management is very similar to normal risk management. The generic scope should therefore be similar. On many occasions only a simple approach will be necessary, identifying and rating only those threats specifically facing the project.

10 / 30
Which strategy is **best** to implement when a risk assessment points out that a specific vulnerability can be exploited?

A) Implementation of a risk management framework
B) Implementation of an information security control
C) Implementation of anti-virus software

A) Incorrect. A risk management framework is a risk methodology and not a strategy.
B) Correct. Controls must be implemented in order to minimize the organizational risks. (Literature: A, Slide 033)
C) Incorrect. Although anti-virus software helps organizations to be protected against viruses and malwares, this is not the solution for all the risks.

11 / 30
An organization has convinced its senior leadership of the need for a formal approach to risk management. Senior leadership has raised concerns over the costs of the proposed risk controls.

Which statement should be included in the business case for the implementation of risk controls?

A) Controls are the primary means of improving the organization's risk profile.
B) Controls determine the organization's risk mitigation options.
C) Controls help the organization to identify its most critical assets.
D) Controls will provide the organization with information about asset vulnerabilities.

A) Correct. Information security can primarily be improved by implementing controls. (Literature: A, Slide 050 and 051)
B) Incorrect. This is a benefit of risk assessment, not implementing controls.
C) Incorrect. This is a benefit of risk assessment, not implementing controls.
D) Incorrect. This is a benefit of identifying threats, not implementing controls.

12 / 30
An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization's risk appetite.

When has the risk assessment program accomplished its **primary** goal?

A) Once the controls are implemented
B) Once the transference of the risk is complete
C) When decision makers have been informed of uncontrolled risks, and it is decided to leave the risks in place
D) When the risk analysis has been completed, and the results are documented in the risk report

A) Incorrect. If there is no ongoing monitoring of the controls, they will deteriorate over time and the risk will exceed the organizational risk appetite.
B) Incorrect. Risk transference is only one of the methods used to control risks. This question is asking about the entirety of the control structure.
C) Correct. It is important that information security professionals ensure that the remaining risks are maintained within the bounds of the organization's risk appetite. (Literature: A, Slide 030)
D) Incorrect. When the risk analysis is completed, the real risk management work is just starting.

13 / 30
The maintenance of an information security program requires a continuous process. This requires inputs from the many different factors that will influence its success.

Which is an input influence that would require the process to change?

A) Policy
B) Risk assessment
C) Security plan

A) Incorrect. Policy is an output of the program. It is not an input.
B) Correct. Risk assessment is a change in input which requires adaption of the process. (Literature: A, Slide 033)
C) Incorrect. The security plan is an output of the program. It is not an input.

14 / 30
The information security officer (ISO) for a global company has just received a management review of the information security policy.

What should this output include?

A) Feedback from interested parties
B) Improvement of control objectives and controls
C) Status of preventive and corrective actions

A) Incorrect. This is input to a management review of the information security policy.
B) Correct. This should be included in the output. (Literature: A, Slide 060)
C) Incorrect. This is input to a management review of the information security policy.

15 / 30
An organization is implementing information security incident handling. It already has a mechanism for personnel to report observed or suspected information security events, but these are not handled well once they are reported.

The organization has put relevant processes, roles, and responsibilities in place. It is now moving on to implement other activities needed for information security incident handling.

What is **not** an activity to implement information security incident handling?

A) Agree on how to prevent information security incidents by using knowledge gained from incidents to strengthen and improve information security controls
B) Define and communicate procedures on information security incident response that should be carried out by competent staff
C) Devise a categorization and prioritization scheme that can be used to categorize information security events as information security incidents
D) Implement procedures to collect and preserve evidence related to information security events for use in any necessary disciplinary or legal actions
E) Set up rules to control physical and logical access to information and other associated assets to prevent information security incidents

A) Incorrect. This is part of implementing information security incident handling.
B) Incorrect. This is part of implementing information security incident handling.
C) Incorrect. This is part of implementing information security incident handling.
D) Incorrect. This is part of implementing information security incident handling.
E) Correct. Implementing access control can support the prevention of incidents but is not part of implementing information security incident handling. (Literature: A, Slides 085 and 094)

16 / 30
The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

A) The business continuity plan
B) The disaster recovery plan
C) The incident response plan
D) The risk treatment plan

A) Incorrect. The business continuity plan is deployed after the disaster is determined to affect business operation. Its goal is to ensure long-term organization of appropriate measures to guarantee the continuity of business processes.
B) Correct. The disaster recovery plan covers short-term recovery and is executed immediately after the incident is labeled a disaster. (Literature: A, Slide 081)
C) Incorrect. The time frame for the incident response plan is immediate/real-time. It is executed when a security incident unfolds.
D) Incorrect. The risk treatment plan is a type of information security improvement plan. Improvement plans are usually executed on an annual basis.

17 / 30
Whose responsibility is it to coordinate an organization's security awareness program?

A) Everyone in the organization
B) Information security management
C) The IT department
D) The secretary of the CIO

A) Incorrect. While everyone in the organization is responsible for organizational security, they are not responsible for coordinating the organization's security awareness program.
B) Correct. Information security management is responsible for coordinating the security awareness campaign. (Literature: A, Slide 095)
C) Incorrect. While the IT department needs to promote and be aware of security issues and concerns, they are not responsible for coordinating the organization's security awareness campaign.
D) Incorrect. The secretary of the CIO may be responsible for promoting and championing awareness but is not directly responsible for coordinating the organization's security awareness program.

18 / 30
Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer (ISO) wants to know the mindset of the employees towards information security controls.

How does the ISO get an impression quickly?

A) By checking the internet data stream
B) By determining if there are viruses on the network
C) By walking around the office after normal business hours

A) Incorrect. This only gives information about how the internet is being used, not about the general mindset of employees.
B) Incorrect. This is a technical measure and gives no information about the mindset of the employees.
C) Correct. When the ISO walks around the office after normal business hours, it is possible to see how employees handle sensitive information. (Literature: A, Slide 095)

19 / 30
The business continuity manager asks for input for the contingency plan.

Which should be the business continuity manager's **first** activity?

A) Define the scope
B) Identify critical business functions
C) Test the plan

A) Incorrect. Scope is a pillar of project management and not a cornerstone for contingency planning as the scope is driven by the results of the business impact analysis (BIA).
B) Correct. The main thing that must be completed in order to have a contingency plan is for the business to define their critical business functions and systems and document these. (Literature: A, Slide 080)
C) Incorrect. Testing of the contingency plan is extremely important and needs to take place at least annually, however it is not the first activity.

20 / 30
A security architect argues with the internal fire prevention team about the statement in the information security policy that doors to confidential areas should always be locked at all times. The emergency response team wants access to those areas in case of fire.

What is the **best** solution to this dilemma?

A) The doors should stay closed in case of fire to prevent access to confidential areas.
B) The doors will automatically open in case of fire.
C) The security architect will be informed when there is a fire.

A) Incorrect. Safety comes before security.
B) Correct. Safety comes before security. (Literature: A, Slide 091)
C) Incorrect. Although it is good to be informed, the emergency response team cannot wait until the security architect has arrived at the scene.

21 / 30
What is the **main** advantage of using an open design of the security architecture?

A) Open designs are easy to set up.
B) Open designs are tested a lot.
C) Open designs have a lot of extra features.

A) Incorrect. Open designs are not set up easier than secret designs.
B) Correct. Open designs are tested extensively, and moreover secret designs never stay secret. (Literature: A, Slide 114)
C) Incorrect. Open designs do not necessarily have more features than secret designs.

22 / 30
What is a characteristic of security architecture?

A) Security architecture completely defines implementation rules.
B) Security architecture follows strategy.
C) Security architecture is secondary.

A) Incorrect. Security architecture is higher-level design than this and does not completely define the implementation rules.
B) Correct. Security architecture follows information security strategy. (Literature: A, Slide 112)
C) Incorrect. Security architecture is strategic and therefore not secondary.

23 / 30
Why is it important to define which security services will be provided?

A) To better align the information security requirements and the customer service
B) To determine the information security strategy of an organization
C) To ensure an organization is compliant with the requirements of ISO/IEC 27001
D) To understand the scope of the information security management system (ISMS)

A) Correct. The definition of which security services will be provided, and in which architecture, must be defined to better align the information security requirements and the service for the customers. (Literature: A, Slide 113)
B) Incorrect. The information security strategy is determined before the information security architecture, which includes security services, is defined.
C) Incorrect. This is not a requirement of ISO/IEC 27001.
D) Incorrect. The scope of the ISMS should be understood before the security services are defined.

24 / 30
Which security item is designed to see harmful traffic and ensure the intrusion is prevented and blocked?

A) Firewall
B) Intrusion prevention system (IPS)
C) Virtual private network (VPN)

A) Incorrect. This is a security tool but does not collect large amounts of network traffic.
B) Correct. An IPS resembles an intrusion detection system (IDS) but is placed in-line and can actively prevent/block intrusions that are detected. (Literature: A, Slide 108)
C) Incorrect. This is a network infrastructure access device.

25 / 30
The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business e-mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD), and organized an awareness training regarding BYOD.

What other control should the security manager propose to prevent data loss in case of theft or loss of the personal device?

A) Do not grant the wish until stable integration of business functions on private devices is possible
B) Encrypt the local storage and network connections
C) Implement strong authentication using tokens with one-time passwords
D) Install anti-malware and a firewall to prevent infection

A) Incorrect. It may be wise, but the CEO cannot be overlooked.
B) Correct. In case of loss or theft at least corporate data are safe. (Literature: A, Slide 061)
C) Incorrect. This only allows secure login to the corporate network.
D) Incorrect. In case of theft or loss the data are still accessible to third parties.

26 / 30
Why are the security elements in the IT infrastructure important?

A) To enable business continuity of the IT infrastructure
B) To manage information security incidents which impact the IT infrastructure
C) To prevent unauthorized physical access to the IT infrastructure
D) To protect the information assets which are on the IT infrastructure

A) Incorrect. Enabling business continuity of the IT infrastructure is important, but the purpose of this security element is to protect the information assets.
B) Incorrect. Managing information security incidents which impact the IT infrastructure is important, but the purpose of this security element is to protect the information assets.
C) Incorrect. Preventing unauthorized physical access to the IT infrastructure is important, but the purpose of this security element is to protect the information assets.
D) Correct. All information security elements are there to protect the information. Most information resides in IT infrastructure which needs to be protected. (Literature: A, Slide 018)

27 / 30
Zoning is a security control to separate physical areas with different security levels. Zones with higher security levels can be secured by more controls. The security manager of a hotel is responsible for security and is considering different zones for the hotel.

What business functions should be combined into one security zone?

A) Boardroom and general office space
B) Fitness area and storage facility
C) Hotel rooms and public bar
D) Public restaurant and lobby

A) Incorrect. The boardroom could contain valuable strategic and thus confidential information that may not be accessible to regular personnel.
B) Incorrect. The storage facility should be available for (some) staff only, whereas the fitness area is accessible for all guests and staff.
C) Incorrect. The hotel rooms and bar must be separated. The public bar can be used by everyone, and the hotel rooms are only for paying guests.
D) Correct. Both these locations can be used by anybody. (Literature: A, Slide 091)

28 / 30
A security manager for a large company has the task to achieve physical protection for corporate data stores.

Through which control can physical protection be achieved?

A) Having visitors sign in and out of the corporate datacenter
B) Install a firewall to prevent access to the network infrastructure
C) Using key cards as access control for employees needing access
D) Writing a policy stating who may have access to the company

A) Incorrect. This does not directly provide a physical barrier or physical protection. It is a good passive/detective control and audit point.
B) Incorrect. This is not a physical protection control. It is a logical protection control.
C) Correct. Key cards are a good form of physical access control especially when combined with some sort of camera or facial recognition procedure to verify the identity of someone entering the data center. (Literature: A, Slide 090)
D) Incorrect. This is an organizational control.

29 / 30
Knowing that physical security controls are a very important part of an information security program, the information security team is asked to design and then implement a security perimeter for a department that is setting up some new data systems.

According to ISO/IEC 27001, which is the **most** important guideline that needs to be considered when establishing this perimeter?

A) A two-person support model
B) Installing cameras and alarms
C) Strength of the perimeter in line with the data's value
D) System logging and monitoring

A) Incorrect. This is a good physical control, but it is not the most important control, and it is not a guideline.
B) Incorrect. This is a good physical control, but it is not the most important control, and it is not a guideline.
C) Correct. Every decision an information security team makes should be data centric and the decisions should be based on the classification of the data involved. (Literature: A, Slide 087)
D) Incorrect. This is a good control, but it is not the most important control, and it is not a perimeter control.

30 / 30
The human resource manager for an organization asked what she could do as a quick win in the area of employment and hiring to help strengthen the organization's data security program according to ISO/IEC 27001.

What should the advice be?

A) Do background checks
B) Implement security policy
C) Place revolving gates at the entrance

A) Correct. One best practice is to conduct background checks on prospective employees. This simple step greatly strengthens the overall security of organizational data. (Literature: A, Slide 094 and 097)
B) Incorrect. This is a good idea but is not a quick win. It would be a long-term strategy.
C) Incorrect. This is a physical control and does not help in the area of employment and hiring.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	C	**16**	B
2	B	**17**	B
3	D	**18**	C
4	C	**19**	B
5	A	**20**	B
6	B	**21**	B
7	D	**22**	B
8	C	**23**	A
9	B	**24**	B
10	B	**25**	B
11	A	**26**	D
12	C	**27**	D
13	B	**28**	C
14	B	**29**	C
15	E	**30**	A

Contact EXIN

www.exin.com