EXIN Information Security Management ISO/IEC 27001 PROFESSIONAL

Certified by EXIN

Sample Exam

Edition 202006

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.

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 should not conflict with the law of the country it is being implemented in
C) Relevant control objectives
D) Return on Investment (ROI)

2 / 30
One of the challenges of the IT security manager for a rather conservative organization is to teach IT management that in order to provide an effective information security program for the organization a change in thought as to what IT security is and what it encompasses is necessary.

What is the IT security manager trying to teach management?

A) By focusing on the protection of the IT infrastructure and not getting sidetracked, it can ensure that proper focus is given where it is most critical.
B) Information security increasingly requires attention from more than just IT as not only the technology matters but also public acceptance of the use of technology.
C) Information security needs to operate within the bounds of the organizational IT group and limit their interaction with other organizational groups.

3 / 30
One of the business managers is really concerned that any sort of IT security program is going to be too intrusive for the business to continue to thrive and be innovative.

Which statement **best** describes what should be told to the manager?

A) Information security exists to serve the interests of the organization and only the level of security that is appropriate for the value of the information is implemented.
B) Information security is a means to safeguard information and mitigate all the data risks within the organization.
C) While information security can be a bit intrusive it is for the best of the organization and all corporate information needs to be locked down tight or dire consequences can be faced.

4 / 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 should be the **most** important aspect the security manager looks for?

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

5 / 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

6 / 30
Which risk assessment approach uses categories instead of actual numbers to determine risks?

A) Evaluative
B) Qualitative
C) Quantitative

7 / 30
Information security management is currently being implemented in the company “Internet Booksellers”. The project leader for the information security project understands that the risk identification process requires him to list organizational assets arranged in order of importance and he 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)

8 / 30
What needs to be decided prior to considering the treatment of risks?

A) How to apply appropriate controls to reduce the risks
B) Operational requirements and constraints
C) Requirements and constraints of national and international legislation and regulations
D) Quantifying risks

9 / 30
A large transportation company has adopted the standard for information security (ISO/IEC 27001:2013) and needs to set up controls for its software development department which they will outsource. An external consultant has been appointed to make sure 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

10 / 30
The security manager for a company has just been tasked with leading the organization's first ever risk assessment effort. The security manager is in the process of implementing controls to mitigate the identified risks. She has taken into account the organizational feasibility and the political feasibility using the organizational objectives and applicable legislation and regulations.

Which item also needs to be accounted for when taking into account the operational feasibility?

A) Risk mitigation
B) Operational constraints
C) Prioritization of risks
D) Transfer of risks

11 / 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) Because a project organization is only a small part of the organization, it is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project.
B) It is should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.
C) 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.

12 / 30
What is the popular name of the ISO/IEC 15408 about security architecture models?

A) Graham-Denning model
B) Rainbow series – the "orange book"
C) Common criteria

13 / 30
An operations manager wants some advice about opening a second datacenter as a hot standby location.

What would the information security officer advise her to do?

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

14 / 30
A security team has just finished an organizational risk assessment and is now discussing controls to mitigate the risks. As part of that effort, programs and technical controls have been considered.

What is the third category of access controls that needs to be considered?

A) Costs
B) Policies
C) Transferences

15 / 30
After doing a risk assessment and establishing a proper set of controls that comply with an organization's risk appetite, a consultant's job is just about complete. The consultant understands that the reality is that no set of controls can achieve complete security.

What needs to be completed in order to strengthen security even more?

A) An internal audit needs to take place in order to provide assurance that the right risk decisions have been made.
B) Management action should be implemented to monitor, evaluate and improve the effectiveness of the security policies and controls to support the organization's aims.
C) The business units must continue to perform risk self-assessments annually.
D) Transference of the residual risks must take place.

16 / 30
The information security officer of the company has just been notified of a pending management review of the information security policy.

What is an input to this management review?

A) Improvement of control objectives and controls
B) Improvement of the management approach to information security
C) Resource needs

17 / 30
The information security officer 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

18 / 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

19 / 30
A large part of an information security team's responsibility is to monitor and detect incidents.

What is the **strongest** indicator of an incident?

A) Activities at unexpected times
B) Activities by dormant accounts
C) Notification from Intrusion Detection System (IDS)
D) The presence of new accounts

20 / 30
Whose responsibility is it to coordinate an organization's security awareness campaign?

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

21 / 30
Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer wants to know the mindset of the employees towards information security controls.

How does she get an impression quickly?

A) She checks the internet data stream.
B) She checks to determine if there are viruses on the network.
C) She walks about the office after normal business hours.

22 / 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.

23 / 30
Which security item is designed to take large collections of network-related traffic that can indicate a denial-of-service attack?

A) Firewall
B) Host-Based Intrusion Detection and Prevention System (Host-Based IDPS)
C) Network-Based Intrusion Detection and Prevention System (Network-Based IDPS)
D) Virtual Private Network (VPN)

24 / 30
The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD).

What controls (besides an awareness training) should the security manager propose to prevent data loss in case of theft or loss of the personal device?

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

25 / 30
Which statement about security architecture is **most** correct?

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

26 / 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 combination of 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

27 / 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) Cameras and alarms must be installed
C) System logging and monitoring
D) The strength of the perimeter should depend on the classification of the data being protected

28 / 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

29 / 30
The business continuity manager asks for input for the contingency plan.

Which should be his **first** activity?

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

30 / 30
One key component to integrate into an organization's information security program is a robust business continuity program. In support of this, a security consultant has been asked to list out the key information security requirements for such a program.

What is his **first** concern in business continuity management from an information security point of view?

A) Ensuring the safety of personnel and the protection of information processing facilities
B) Identifying events that can cause interruptions to the organization's finances, followed by a risk assessment
C) Linking the different risk aspects together into a holistic plan to be endorsed by management to implement the strategy
D) Identifying the consequences of disasters, system down time, security failures, loss of service and inclusive risks to ensure that business systems are available

Answer Key

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

A) Description of how the services are being supported
B) Policy should not conflict with the law of the country it is being implemented in
C) Relevant control objectives
D) Return on Investment (ROI)

A) Incorrect. This answer does not pertain to defining overall security strategy and is more focused on the Service Level Agreement (SLA).
B) Incorrect. This answer does not pertain to defining overall security strategy and is more a part of policy development.
C) Correct. Having relevant control objectives is a key element to the development of security strategy. (Literature: A, Slide 059)
D) Incorrect. This answer does not pertain to defining overall security strategy and is more a part of financial forecasting and budgeting.

2 / 30
One of the challenges of the IT security manager for a rather conservative organization is to teach IT management that in order to provide an effective information security program for the organization a change in thought as to what IT security is and what it encompasses is necessary.

What is the IT security manager trying to teach management?

A) By focusing on the protection of the IT infrastructure and not getting sidetracked, it can ensure that proper focus is given where it is most critical.
B) Information security increasingly requires attention from more than just IT as not only the technology matters but also public acceptance of the use of technology.
C) Information security needs to operate within the bounds of the organizational IT group and limit their interaction with other organizational groups.

A) Incorrect. This is a very small subset of an information security program. It does not educate IT management that it takes an extended view to run and manage an effective information security program. Information security increasingly requires attention from more than just IT.
B) Correct. Security requires more than just the attention of IT within an organization. (Literature: A, Slide 015)
C) Incorrect. This does not teach IT-management that it takes an extended view to run and manage an effective information security program. Information security increasingly requires attention from more than just IT.

3 / 30
One of the business managers is really concerned that any sort of IT security program is going to be too intrusive for the business to continue to thrive and be innovative.

Which statement **best** describes what should be told to the manager?

A) Information security exists to serve the interests of the organization and only the level of security that is appropriate for the value of the information is implemented.
B) Information security is a means to safeguard information and mitigate all the data risks within the organization.
C) While information security can be a bit intrusive it is for the best of the organization and all corporate information needs to be locked down tight or dire consequences can be faced.

A) Correct. Choices are made regarding which data to protect and which level of protection that data needs. (Literature: A, Slide 015)
B) Incorrect. This answer states that all risks will be mitigated. Only subsets of corporate data truly need to be protected.
C) Incorrect. This answer states that all organizational data needs to be protected, which is not true.

4 / 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 should be the **most** important aspect the security manager looks 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/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 015)

5 / 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 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 042)
D) Incorrect. The system owner is responsible for implementing the controls as required by the defined CIA (confidentiality, integrity, availability) classification.

6 / 30
Which risk assessment approach uses categories instead of actual numbers to determine risks?

A) Evaluative
B) Qualitative
C) Quantitative

A) Incorrect. This is not a standard risk methodology or approach.
B) Correct. Qualitative is a well-accepted risk methodology that does not use pure numbers and relies somewhat on the experience of the security professional. (Literature: A, Slide 041)
C) Incorrect. Quantitative is the risk methodology that uses actual numbers.

7 / 30

Information security management is currently being implemented in the company “Internet Booksellers”. The project leader for the information security project understands that the risk identification process requires him to list organizational assets arranged in order of importance and he 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, he/she will immediately order from another source. The impact on revenue, profitability and public image will be maximal. (Literature: A, Slide 029)
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. 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. Eventually revenue and profit will be realized.
D) Incorrect. When customer service request 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.

8 / 30
What needs to be decided prior to considering the treatment of risks?

A) How to apply appropriate controls to reduce the risks
B) Operational requirements and constraints
C) Requirements and constraints of national and international legislation and regulations
D) Quantifying risks

A) Incorrect. This is one of the four possible options for treatment of risks and is not something that needs to be decided prior to considering the treatment of risks.
B) Incorrect. This is one of the five items that need to be taken into account when designing controls and is not in the same ISO table as the correct answer.
C) Incorrect. This is one of the five items that need to be taken into account when designing controls and is not in the same ISO table as the correct answer.
D) Correct. If these criteria are in place, risks that are within the bounds of the organization's work appetite can be ignored. Thereby it is not necessary to spend time focusing on items that are not considered a risk by the organization or by regulation. (Literature: A, Slide 030 and Slide 041)

9 / 30
A large transportation company has adopted the standard for information security (ISO/IEC 27001:2013) and needs to set up controls for its software development department which they will outsource. An external consultant has been appointed to make sure 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 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 043)
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.

10 / 30
The security manager for a company has just been tasked with leading the organization's first ever risk assessment effort. The security manager is in the process of implementing controls to mitigate the identified risks. She has taken into account the organizational feasibility and the political feasibility using the organizational objectives and applicable legislation and regulations.

Which item also needs to be accounted for when taking into account the operational feasibility?

A) Risk mitigation
B) Operational constraints
C) Prioritization of risks
D) Transfer of risks

A) Incorrect. Risk mitigation is the objective of what needs to be accomplished with controls but is not one of the items that needs to be taken into account when implementing the designed controls.
B) Correct. Organizational objectives, operational constraints and applicable legislation and regulation need to be accounted for when implementing risk controls. (Literature: A, Slide 032)
C) Incorrect. The step of the prioritization of risks takes place prior to the design and implementation of controls.
D) Incorrect. The transfer of risk is a control to be implemented. It is not something that needs to be taken into account when implementing a control.

11 / 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) Because a project organization is only a small part of the organization, it is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project.
B) It is should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.
C) 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.

A) 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 a 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 046)
B) Incorrect. Project risk management is very similar to normal risk management. The generic scope should therefore be similar. On many occasions a simple approach will only be necessary, identifying and rating only those threats specifically facing the project.
C) 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.

12 / 30
What is the popular name of the ISO/IEC 15408 about security architecture models?

A) Graham-Denning model
B) Rainbow series – the “orange book”
C) Common criteria

A) Incorrect. The Graham-Denning access control model describes eight primitive protection rights. This is a good model, but not the methodology meant here.
B) Incorrect. The “orange book” is considered the cornerstone of the Rainbow series. The Trusted Computer System Evaluation Criteria (TCSEC) is a DoD (Department of Defense) standard that defines the criteria for assessing the access controls in a computer system. This standard is part of a larger series of standards collectively referred to as the Rainbow series.
C) Correct. The common criteria for information technology security evaluation (often called the common criteria or CC) is the international standard ISO/IEC 15408 for computer security certification. (Literature: A, Slide 125)

13 / 30
An operations manager wants some advice about opening a second datacenter as a hot standby location.

What would the information security officer advise her to do?

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

A) Correct. Since it is a backup location, it would be wise to make sure that is has a different risk profile. (Literature: A, Slide 043)
B) Incorrect. This is only part of the risk profile.
C) Incorrect. This is a general security control.
D) Incorrect. This is not a physical security risk. It is a legislation problem.

14 / 30
A security team has just finished an organizational risk assessment and is now discussing controls to mitigate the risks. As part of that effort, programs and technical controls have been considered.

What is the third category of access controls that needs to be considered?

A) Costs
B) Policies
C) Transferences

A) Incorrect. The three categories of access controls are technical controls, programs and policies.
B) Correct. The three categories of access controls are technical controls, programs and policies. (Literature: A, Slide 099)
C) Incorrect. The three categories of access controls are technical controls, programs and policies.

15 / 30
After doing a risk assessment and establishing a proper set of controls that comply with an organization's risk appetite, a consultant's job is just about complete. The consultant understands that the reality is that no set of controls can achieve complete security.

What needs to be completed in order to strengthen security even more?

A) An internal audit needs to take place in order to provide assurance that the right risk decisions have been made.
B) Management action should be implemented to monitor, evaluate and improve the effectiveness of the security policies and controls to support the organization's aims.
C) The business units must continue to perform risk self-assessments annually.
D) Transference of the residual risks must take place.

A) Incorrect. An audit is not a mandatory step to make sure that correct risk decisions were made. While an audit can be done if there is a lack of confidence in the person(s) deciding on the mitigating controls.
B) Correct. This is a basic step in many best practice methodologies (for example Plan Do Check Act) that must be completed in order to assure that systemic improvement and ongoing evaluation is a critical item in maintaining adequate policies and controls. (Literature: A, Slide 057 and Slide 060)
C) Incorrect. Self-assessments are a good idea but are only as good as the people doing the assessment.
D) Incorrect. This is a control and the question states that the controls have already been established.

16 / 30
The information security officer of the company has just been notified of a pending management review of the information security policy.

What is an input to this management review?

A) Improvement of control objectives and controls
B) Improvement of the management approach to information security
C) Resource needs

A) Incorrect. This is output from the management review.
B) Incorrect. This is output from the management review.
C) Correct. This is input to the management review. (Literature: A, Slide 057)

17 / 30
The information security officer 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 057)
C) Incorrect. This is input to a management review of the information security policy.

18 / 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 030)
C) Incorrect. The security plan is an output of the program. It is not an input.

19 / 30
A large part of an information security team's responsibility is to monitor and detect incidents.

What is the **strongest** indicator of an incident?

A) Activities at unexpected times
B) Activities by dormant accounts
C) Notification from Intrusion Detection System (IDS)
D) The presence of new accounts

A) Incorrect. This is associated with probable indicators, not definite ones.
B) Correct. If any of these dormant accounts start activities, an incident is quite certain to have occurred. (Literature: A, Slide 126)
C) Incorrect. This is associated with probable indicators, not definite ones.
D) Incorrect. This is associated with probable indicators, not definite ones.

20 / 30
Whose responsibility is it to coordinate an organization's security awareness campaign?

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 085)
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. He/she may be responsible for promoting and championing awareness but is not directly responsible for coordinating the organization's security awareness program.

21 / 30
Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer wants to know the mindset of the employees towards information security controls.

How does she get an impression quickly?

A) She checks the internet data stream.
B) She checks to determine if there are viruses on the network.
C) She walks about 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 she walks about the office after normal business hours, she will see how employees handle sensitive information. (Literature: A, Slide 085)

22 / 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 124)
C) Incorrect. Open designs do not necessarily have more features than secret designs.

23 / 30
Which security item is designed to take large collections of network-related traffic that can indicate a denial-of-service attack?

A) Firewall
B) Host-Based Intrusion Detection and Prevention System (Host-Based IDPS)
C) Network-Based Intrusion Detection and Prevention System (Network-Based IDPS)
D) Virtual Private Network (VPN)

A) Incorrect. This is a security tool but does not collect large amounts of network traffic.
B) Incorrect. This focuses on host-based data traffic collection and not network-based.
C) Correct. The Network-Based IDPS is used to gather and collect data flows across an organization's network in order to see if abnormal events are indicative of an active attack such as a denial-of-service would be. (Literature: A, Slide 116)
D) Incorrect. This is a network infrastructure access device.

24 / 30
The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD).

What controls (besides an awareness training) should the security manager propose to prevent data loss in case of theft or loss of the personal device?

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

A) Correct. In case of loss or theft at least corporate data are safe. (Literature: A, Slide 099 and Slide 120)
B) Incorrect. This only allows secure login to the corporate network.
C) Incorrect. It may be wise, but the CEO cannot be overlooked.
D) Incorrect. In case of theft or loss the data are still accessible to third parties.

25 / 30
Which statement about security architecture is **most** correct?

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

A) Correct. Security architecture follows information security strategy. (Literature: A, Slide 123)
B) Incorrect. Security architecture is strategic and therefore not secondary.
C) Incorrect. Security architecture is higher-level design than this and does not completely define the implementation rules.

26 / 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 combination of 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 080)

27 / 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) Cameras and alarms must be installed
C) System logging and monitoring
D) The strength of the perimeter should depend on the classification of the data being protected

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) Incorrect. This is a good control, but it is not the most important control and it is not a perimeter control.
D) 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 082)

28 / 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 063 and Slide 084)
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.

29 / 30
The business continuity manager asks for input for the contingency plan.

Which should be his **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 074)
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.

30 / 30
One key component to integrate into an organization's information security program is a robust business continuity program. In support of this, a security consultant has been asked to list out the key information security requirements for such a program.

What is his **first** concern in business continuity management from an information security point of view?

A) Ensuring the safety of personnel and the protection of information processing facilities
B) Identifying events that can cause interruptions to the organization's finances, followed by a risk assessment
C) Linking the different risk aspects together into a holistic plan to be endorsed by management to implement the strategy
D) Identifying the consequences of disasters, system down time, security failures, loss of service and inclusive risks to ensure that business systems are available

A) Correct. This is a key element of business continuity management from an information security point of view. (Literature: A, Slide 089)
B) Incorrect. This is part of business continuity and risk assessment: identifying events (or sequence of events) that can cause interruptions to the organizations business processes.
C) Incorrect. This is part of business continuity and risk assessment which should be carried out with full involvement from owners of business resources and processes.
D) Incorrect. This is part of business continuity and risk assessment: identifying events (or sequence of events) that can cause interruptions to the organizations business processes.

Evaluation

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

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

Contact EXIN

www.exin.com