

**Information Security Management Advanced**  
**based on ISO/IEC 27002**  
**edition July 2010**

**content**

2	introduction
3	sample exam
13	answer key
31	evaluation

## **Introduction**

This is the sample exam Information Security Management Advanced based on ISO/IEC 27002.

This sample exam consists of 30 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for this exam is 30. Each correct answer is worth one point. If you obtain 20 points or more you will pass.

The time allowed for this exam is 90 minutes.

No rights may be derived from this information.

Good luck!

Copyright © 2010 EXIN

All rights reserved. No part of this publication may be published, reproduced, copied or stored in a data processing system or circulated in any form by print, photo print, microfilm or any other means without written permission by EXIN.

## Exam

### 1 of 30

The CIO of a Fortune 500 company has asked you, an external information security consultant, what she should do to start up an information protection program in her company.

What do you advise the CIO as the first step in starting an information protection program?

- A.** Create an information protection policy as this is the key item for beginning an information protection program.
- B.** Establish security standards, procedures and guidelines in parallel with the protection policy.
- C.** Have a risk assessment conducted in order to baseline the risks that their infrastructure is facing. Mitigation steps can then be put in place.

### 2 of 30

An information security colleague of yours was given the task of writing the scope section of her organization's information security policy. She is not sure what type of data should be included and has asked for your help.

What kind of information is needed for defining the information security policy scope?

- A.** The characteristics of the business, the organization, its location, assets and technology covered by the policy.
- B.** The consequences to employees for non-compliance with the information security policy.
- C.** The identification of who is responsible for activities and tasks. The who in this case is always identified by job title/role and never by name?

### 3 of 30

A senior management representative of a Fortune 500 company has asked that you help the organization establish an Information Security Management System (ISMS) and he is worried about management responsibilities.

What is one of the first key responsibilities of the management?

- A.** Creating the business impact analysis report and having it approved by the board of directors.
- B.** Formulating, reviewing and approving the information security policy.
- C.** Having the details of the progress of the risk treatment plan in order to support it.
- D.** Reviewing reports on the state of information security throughout the organization.

**4 of 30**

Which condition should be met before a global information security policy can be established?

- A. All employees must sign a proper confidentiality agreement.
- B. The comments and observations issued by the top management must have been processed.
- C. The organization should comply with all legal requirements.

**5 of 30**

The Chief Information Security Officer (CISO) has asked you to create the organization's information security policy.

What are the topics you typically have to include?

- A. Definition of information security, its objectives and methodology
- B. Definition of information security, its objectives and scope
- C. Definition of information security, its objectives, methodology and planning
- D. Objectives and scope

**6 of 30**

While you are eating in the company cafeteria a senior management representative from marketing stops by your table and tells you that she just received the information security policy. She expresses confusion because just two weeks ago she received a copy of the information protection program. The manager wants to know what the difference is between the two documents.

What is your answer?

- A. The information protection program is a document that provides a roadmap the organization will use to protect its information. The information security policy document contains the policies that staff and employees will follow in order to support the goal of information security.
- B. The information protection program is a supportive appendix of the information security policy and is used to support the policies.
- C. The information security policy document contains the laws of the organization and her staff need to follow the policies in the document. The information protection program supports the information security policy document by having the standards of due care required to enforce the policies.
- D. The information security policy document contains the rules and regulations that her department needs to follow and the information protection program contains instructions on how to follow the policies.

**7 of 30**

The Chief Information Officer (CIO) for your organization has asked you to provide him with an executive summary outlining the basic components of a plan to implement an Information Security Management System.

What are the first tasks that you will indicate?

- A.** A definition for protecting the confidentiality, integrity and availability of data, information security procedures, business continuity plan and the risk mitigation strategies.
- B.** Identification and assessment of risks, definition of responsibilities, designing and implementation of security controls.
- C.** The information security charter, the work breakdown structure necessary for doing information security work and the risk mitigation and acceptance process.
- D.** Topic, thesis, organizational relationships and the list of key stakeholders.

**8 of 30**

The Chief Information Security Officer (CISO) has asked you to create metrics that will measure the information security controls that aren't perceived as going well.

Which controls would you create metrics for?

- A.** Access control, e-mail practices and virus management
- B.** Business unit responsibilities
- C.** Common threats
- D.** Risk treatment plan compliance

**9 of 30**

You are the Information Security Manager (ISM) of an IT Service Provider. One of your colleagues is working on an IT Service Management project. The management of Business Relationships is being implemented at the moment. She asks you if there are any requirements in ISO/IEC 27002 she should take into account, considering the organization wants to comply to this standard in the near future.

To which requirement in the standard will you refer her?

- A.** Business Continuity requirements
- B.** The requirement to address security in third party agreements
- C.** The requirement to manage information security incidents

**10 of 30**

Policies are the cornerstone of effective information security management. The various information security policies provide direction to employees on what is expected of them and how their actions will be perceived.

What is required in order for policies to be effective and to monitor their effectiveness?

- A.** Baseline metrics that can be used to show that the information security policy has created a systematic improvement across the organizational units.
- B.** Management support and ongoing supportive metrics which show the effectiveness of controls that enforce them.
- C.** Rules of enforcement and management commitment to force employees to comply with the information security policy.
- D.** Senior management support and a clear alignment and understanding among the organization's employees on how to follow the policies.

**11 of 30**

You have been asked to design an executive summary for the Board of Directors that outlines what the goals of an information security incident management program would be.

What are the primary objectives of information security incident management?

- A.** Contain the event, track the event from start to finish, clearly document the event, collect evidence.
- B.** Report and track incidents through the service desk, establish incident response responsibilities and procedures, establish incident response escalation points, collect evidence and conduct follow-up interviews.
- C.** Report security events quickly, contain the event, clearly document the event, collect evidence and conduct follow up interviews.
- D.** Report security events quickly, report weaknesses found in systems and services, establish incident response responsibilities and procedures, historical incident learning, evidence collection.

**12 of 30**

The company security service performs a clear desk round after business hours. They find a data CD on a desk.

What is/are the correct action(s)?

- A.** They leave a note behind on the desk.
- B.** They place the CD in an envelope and take it along with them.
- C.** They register the security incident into an incident-management system.
- D.** All of the above.

**13 of 30**

As part of the organization's Business Continuity Planning (BCP), a Business Impact Analysis (BIA) was completed. The Chief Information Officer (CIO) has handed you the results of the BIA and asked that you use these results to create an organizational recovery strategy for the assets listed in the BIA.

What are the four areas to consider for a recovery plan?

- A. Location, resources, money and scope of the recovery operations
- B. People, communications, computing equipment and facilities
- C. People, recovery types (hot, cold, warm), communications and facilities
- D. People, resources, computing equipment and facilities

**14 of 30**

An HR manager of a company wants to write a policy for illustrating the standard behavior required of all staff.

How is this policy usually called?

- A. Employee Disciplinary Code
- B. Records Management
- C. Standards of Conduct
- D. Workplace security standards

**15 of 30**

In the company where you work as Information Security Manager (ISM), the division directors are accountable and have their own support services at their disposal. You have posted an Information Security Coordinator in each division. One of them reports in a coordination discussion that their division director has decided to institute a more severe access policy.

What does this lead to?

- A. This leads to reporting this to top management with the request to reverse the decision.
- B. This leads to revision of the information security plan for the division in question.
- C. This leads to revision of the information security policy.
- D. This leads to revision of the risk analysis of the division in question.

**16 of 30**

Who determines the security classification of information?

- A. The custodian of the information
- B. The owner of the information
- C. The user of the information

**17 of 30**

It is advisable to have a number of security classification levels in your organization for the classification of information (assets).

What is the primary reason for identifying different classes of data?

- A. We are able to design information security controls that rely on layered defensive measures to protect all the classes of data.
- B. We can design information security controls that are dedicated for each of the different levels.
- C. We can focus our limited money and people resources on protecting the data and systems that need to be protected.
- D. We can make it easier for employees to know which data they are allowed to access during the course of doing their jobs.

**18 of 30**

As the Chief Information Security officer (CISO) you know that important organizational information should be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual and business requirements. The system of storage and handling for this organizational information should ensure clear identification of records and of their retention periods.

To meet these control objectives, which steps should you implement?

- A. an information incident management program, a security awareness program and a comprehensive identity management methodology
- B. guidelines for retention, storage, handling and disposal of information, an inventory of sources of key information and appropriate controls
- C. implement a data protection and privacy policy, encrypt all regulated data in transit and storage and provide annual training to the custodians of the information
- D. using appropriate audit tools, obeying copyright laws and ensuring that any related cryptographic keying materials are stored to enable decryption of the records for the length of time they are retained

**19 of 30**

Risk assessment is the process that allows business managers to balance operational and economic costs of security controls and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise.

When should a risk assessment be conducted?

- A.** It should be repeated periodically to address any change that might influence the risk assessment results.
- B.** When an organization wants to take control of its own destiny by ensuring that only those controls that are actually needed will be implemented.
- C.** When management wants to eliminate the risk associated with implementing a service or product.
- D.** When senior management has to prove to internal or external auditors that they are showing due diligence.

**20 of 30**

Which method for risk analysis provides the best basis for the measures that must be taken?

- A.** qualitative risk analysis
- B.** quantitative risk analysis
- C.** it makes no difference

**21 of 30**

An Information Security Officer (ISO) working for you has come to you after he conducted a threat identification and determined the impact of a threat on a system that is being implemented. Your ISO asked for your opinion on the security controls he is recommending to the project team.

What is the basic reason for the identification of recommended controls?

- A.** To clearly document the results in a standard format and issue a report to the board of directors or Chief Information Officer (CIO).
- B.** To ensure that the entire enterprise is mitigating or minimizing the risks associated with the implementation of a new service or product regardless of the cost associated with establishing adequate controls and safeguards.
- C.** To identify controls eliminating or reducing the risk to an acceptable level.
- D.** To protect the information and to make sure that outstanding vulnerabilities don't exist on deployed assets.

**22 of 30**

For the formulation of the list with the security measures to be introduced, a member of the management team proposes using the ISO/IEC 27002 as the basis for the security requirements.

What is your reaction?

- A.** You indicate that if the organization uses the ISO/IEC 27001 standard instead, the organization will also be able to be certified.
- B.** You indicate that the ISO/IEC 27002 standard in this case had better not be used because this standard does not contain the initiating of security measures.
- C.** You indicate that this standard should be used wisely, because the requirements in the ISO/IEC 27002 easily can lead to an extensive range of measures.

**23 of 30**

Your manager is a little bit confused about standards and guidelines. She has understood that the Information Security Management System (ISMS) can be certified against an ISO standard, but she doesn't know which one, ISO has published too many standards!

What is your answer?

- A.** ISO/IEC 15308-1:2005
- B.** ISO/IEC 17799:2005
- C.** ISO/IEC 27001:2005
- D.** ISO/IEC 27002:2005

**24 of 30**

You are the Information Security Manager (ISM) in your organization. You want to check if the controls that were implemented are adequate. You want to assess the controls against the complete ISO/IEC 27002 standard. The owner of one of the information systems expresses the opinion that the use of the ISO standard is an "overkill".

What is your reaction?

- A.** You understand the criticism and ask the owner to provide a tailor-made standard document.
- B.** You state that the standard is suitable, because the enterprise-wide analysis consists of more than one information system.
- C.** You state that you will investigate whether you can use only parts of the ISO standard.

**25 of 30**

What kind of legislation is in place to ensure that an enterprise maintains the confidentiality of personal information that it may hold?

- A.** A Computer Misuse Act
- B.** A Data Protection Act
- C.** A Freedom of Information Act

**26 of 30**

After having implemented technical and organizational controls, what security controls should an enterprise enforce before staff handle personal data?

- A.** It should ensure that all staff have access to personal data when required.
- B.** It should ensure that staff are aware of enterprise security controls.
- C.** It should introduce a new Tier 1 policy for personal data.
- D.** It should introduce biometric access control mechanisms.

**27 of 30**

The CIO has asked you, the Chief Information Security Officer (CISO), to help work on the security aspects of a 3rd party contract. She asks you to first investigate in ISO/IEC 27002 what should be included in the contract to make sure statutory requirements are met.

What is your finding?

- A.** Agreements can have considerable variance for different organizations and among different types of third parties. Care should be taken to include all identified risks and security requirements.
- B.** All employees, contractors and 3rd party users should return organizational assets in their possession when they terminate employment.
- C.** Background verification checks on all candidates for employment, contractors and 3rd party users should be carried out in accordance with relevant laws.
- D.** Security perimeters should be used to protect areas that contain information and information processing facilities used by the 3rd party vendor.

**28 of 30**

What should first be in place before allowing an external party access to enterprise wide information?

- A.** a security chapter in the Service Level Agreement (SLA)
- B.** background checks on the staff of the external party
- C.** full access control mechanisms
- D.** induction training for external parties

**29 of 30**

You are the Information Security Officer (ISO) in your organization and before performing a complete risk analysis you decide to conduct a walk-about.

Which information will you have learned during the walk-about?

- A.** The employees' mind-set towards information security controls.
- B.** Whether it is necessary to do a complete risk analysis or not.
- C.** Which physical controls will be necessary for implementation.
- D.** Who is responsible for which information.

**30 of 30**

You are one of the internal auditors in your organization. The audit plan has been determined and your team is setting up an audit program.

What is the correct order of the next steps that should be taken?

- A.** Determine the frequency of the audits, audit work programs, audit reports, storage requirements for the documentation collected during the audits, follow-up of the findings and development paths for the required audit expertise.
- B.** Execution of the audits by independent auditors, audit reports, correction of the findings, determination of the date for the next audit per analysis area and monitoring of the risk analysis and the changes thereupon.
- C.** Preparation of the audits, including follow-up of the remaining open audit findings, performance of the audits, prioritizing the recommendations, correcting the non-conformities, verification of the corrections.
- D.** The risk analysis, the audit work programs including objectives, the authorizations and responsibilities of the required (internal) auditors, audit findings and compliance thereof.

## Answer key

### 1 of 30

The CIO of a Fortune 500 company has asked you, an external information security consultant, what she should do to start up an information protection program in her company.

What do you advise the CIO as the first step in starting an information protection program?

- A.** Create an information protection policy as this is the key item for beginning an information protection program.
- B.** Establish security standards, procedures and guidelines in parallel with the protection policy.
- C.** Have a risk assessment conducted in order to baseline the risks that their infrastructure is facing. Mitigation steps can then be put in place.

A. Correct. Creation of an Information Protection policy is the first thing to do when starting an Information Protection program. See Information Security Fundamentals §1.5

B. Incorrect. Standards, procedures and guidelines are an important part of implementing an Information Protection program but they are subsequent to the creation of the information protection policy.

C. Incorrect. A risk assessment is important but it is not the first thing that should be done when implementing an Information Protection program.

### 2 of 30

An information security colleague of yours was given the task of writing the scope section of her organization's information security policy. She is not sure what type of data should be included and has asked for your help.

What kind of information is needed for defining the information security policy scope?

- A.** The characteristics of the business, the organization, its location, assets and technology covered by the policy.
- B.** The consequences to employees for non-compliance with the information security policy.
- C.** The identification of who is responsible for activities and tasks. The who in this case is always identified by job title/role and never by name.

A. Correct. The scope is described in §4.2.1.a of ISO/IEC 27001:2005 and §4.1 of ISO/IEC 27002:2005. See Information Security Fundamentals §4.10.1.2

B. Incorrect. The consequences for non-compliance are part of the compliance or consequences section of a policy.

C. Incorrect. The identification of who is responsible is in the responsibilities section of a policy.

**3 of 30**

A senior management representative of a Fortune 500 company has asked that you help the organization establish an Information Security Management System (ISMS) and he is worried about management responsibilities.

What is one of the first key responsibilities of the management?

- A.** Creating the business impact analysis report and having it approved by the board of directors.
- B.** Formulating, reviewing and approving the information security policy.
- C.** Having the details of the progress of the risk treatment plan in order to support it.
- D.** Reviewing reports on the state of information security throughout the organization.

A. Incorrect. The review and approval of a business impact analysis (BIA) is an important task but the management does not necessarily create the business impact analysis.

B. Correct. As per 6.1.1 in ISO/IEC 27002:2005. See Information Security Fundamentals §2

C. Incorrect. Management shouldn't have the details.

D. Incorrect. Reviewing reports on the state of information security is a key responsibility of the management but it is not an initial key responsibility.

**4 of 30**

Which condition should be met before a global information security policy can be established?

- A.** All employees must sign a proper confidentiality agreement.
- B.** The comments and observations issued by the top management must have been processed.
- C.** The organization should comply with all legal requirements.

A. Incorrect. Confidentiality agreements can only be drawn up when the policy has been established, asset classification is known and the employee handbook has been changed accordingly.

B. Correct. The top management must manage, support and enforce the policy in order to show due diligence. See Information Security Fundamentals §4.10

C. Incorrect. Compliance may form a part of information security plans.

**5 of 30**

The Chief Information Security Officer (CISO) has asked you to create the organization's information security policy.

What are the topics you typically have to include?

- A.** Definition of information security, its objectives and methodology
- B.** Definition of information security, its objectives and scope
- C.** Definition of information security, its objectives, methodology and planning
- D.** Objectives and scope

- A. Incorrect. Methodology is not required in a policy.
- B. Correct. As per §5.1.1 in ISO/IEC 27002:2005. See Information Security Fundamentals §3
- C. Incorrect. Methodology or planning is not required in a policy.
- D. Incorrect. This is incomplete.

While you are eating in the company cafeteria a senior management representative from marketing stops by your table and tells you that she just received the information security policy. She expresses confusion because just two weeks ago she received a copy of the information protection program. The manager wants to know what the difference is between the two documents.

What is your answer?

- A.** The information protection program is a document that provides a roadmap the organization will use to protect its information. The information security policy document contains the policies that staff and employees will follow in order to support the goal of information security.
- B.** The information protection program is a supportive appendix of the information security policy and is used to support the policies.
- C.** The information security policy document contains the laws of the organization and her staff need to follow the policies in the document. The information protection program supports the information security policy document by having the standards of due care required to enforce the policies.
- D.** The information security policy document contains the rules and regulations that her department needs to follow and the information protection program contains instructions on how to follow the policies.

- A. Correct. The information security policy document contains the policies that support the goals of the information security plan. See Information Security Fundamentals §1.5
- B. Incorrect. The information protection program does not support the information security policy, the policy supports the plan.
- C. Incorrect. Standards of due care are not used to enforce the policies cited in the information security policy document.
- D. Incorrect. The information protection program does not contain the instructions on how to follow the policies.

**7 of 30**

The Chief Information Officer (CIO) for your organization has asked you to provide him with an executive summary outlining the basic components of a plan to implement an Information Security Management System.

What are the first tasks that you will indicate?

- A.** A definition for protecting the confidentiality, integrity and availability of data, information security procedures, business continuity plan and the risk mitigation strategies.
- B.** Identification and assessment of risks, definition of responsibilities, designing and implementation of security controls.
- C.** The information security charter, the work breakdown structure necessary for doing information security work and the risk mitigation and acceptance process.
- D.** Topic, thesis, organizational relationships and the list of key stakeholders.

- A. Incorrect. Procedures are not part of the basic components of an Information Security plan and neither is the organizations business continuity plan.
- B. Correct. These are all the main critical components of an Information Security plan. See ISO/IEC 27002:2005
- C. Incorrect. These items cover information security project management and parts of information security risk management; they are not basic components of an information security plan.
- D. Incorrect. These items cover a breadth of Information security policies and standards but are not basic components of an information security plan.

**8 of 30**

The Chief Information Security Officer (CISO) has asked you to create metrics that will measure the information security controls that aren't perceived as going well.

Which controls would you create metrics for?

- A.** Access control, e-mail practices and virus management
- B.** Business unit responsibilities
- C.** Common threats
- D.** Risk treatment plan compliance

- A. Correct. Access control, e-mail practices and virus management are typical areas that information security groups struggle to show the benefits of. ISO/IEC 27001:2005 requires metrics for any control or group of controls. See Information Security Fundamentals §3 and §4
- B. Incorrect. Business unit responsibilities are not information security metrics.
- C. Incorrect. Common threats are not information security metrics.
- D. Incorrect. Risk treatment plan compliance can be measured but it is not a control for ISO/IEC 27002.

**9 of 30**

You are the Information Security Manager (ISM) of an IT Service Provider. One of your colleagues is working on an IT Service Management project. The management of Business Relationships is being implemented at the moment. She asks you if there are any requirements in ISO/IEC 27002 she should take into account, considering the organization wants to comply to this standard in the near future.

To which requirement in the standard will you refer her?

- A.** Business Continuity requirements
- B.** The requirement to address security in third party agreements
- C.** The requirement to manage information security incidents

- A. Incorrect. Business Continuity requirements are internal to the organization.
- B. Correct. Security should be addressed in third party agreements. See ISO/IEC 27002:2005 §6.2
- C. Incorrect. Management of information security incidents is internal to the organization

**10 of 30**

Policies are the cornerstone of effective information security management. The various information security policies provide direction to employees on what is expected of them and how their actions will be perceived.

What is required in order for policies to be effective and to monitor their effectiveness?

- A.** Baseline metrics that can be used to show that the information security policy has created a systematic improvement across the organizational units.
- B.** Management support and ongoing supportive metrics which show the effectiveness of controls that enforce them.
- C.** Rules of enforcement and management commitment to force employees to comply with the information security policy.
- D.** Senior management support and a clear alignment and understanding among the organization's employees on how to follow the policies.

- A. Incorrect. Baseline metrics are a starting point to judge where an organization is at a point in time but do not show systematic improvement.
- B. Correct. Management support of the information security policy is a critical component of effective policy compliance and that which is measured can be improved. See Information Security Fundamentals §3.1 - §4.4
- C. Incorrect. Rules of enforcement are not sufficient to insure that policies are effective.
- D. Incorrect. Employees' understanding of the policies is important but it is not enough to ensure that the policies will be effective.

You have been asked to design an executive summary for the Board of Directors that outlines what the goals of an information security incident management program would be.

What are the primary objectives of information security incident management?

- A.** Contain the event, track the event from start to finish, clearly document the event, collect evidence.
- B.** Report and track incidents through the service desk, establish incident response responsibilities and procedures, establish incident response escalation points, collect evidence and conduct follow-up interviews.
- C.** Report security events quickly, contain the event, clearly document the event, collect evidence and conduct follow up interviews.
- D.** Report security events quickly, report weaknesses found in systems and services, establish incident response responsibilities and procedures, historical incident learning, evidence collection.

A. Incorrect. Containing and tracking the event is important but they are not considered one of the primary goals in accordance with ISO/IEC 27002. These items are usually part of the procedure steps as noted when an organization establishes their incident response responsibilities and procedures.

B. Incorrect. Establishing incident response escalation points and conducting follow-up interviews are not considered primary goals in accordance with ISO/IEC 27002.

C. Incorrect. Containing and documenting the event is important and so are follow-up interviews but they are not considered one of the primary goals in accordance with ISO/IEC 27002. These items are usually part of the procedure steps as noted when an organization establishes their incident response responsibilities and procedures.

D. Correct. According to clause 13 of ISO/IEC 27002 these are the five primary objectives of Information Security Incident Management.

**12 of 30**

The company security service performs a clear desk round after business hours. They find a data CD on a desk.

What is/are the correct action(s)?

- A.** They leave a note behind on the desk.
- B.** They place the CD in an envelope and take it along with them.
- C.** They register the security incident into an incident-management system.
- D.** All of the above.

A. Incorrect. Leaving a note is not enough. The incident should also be registered in order to learn from it.

B. Incorrect. Taking the CD without informing the employee and registering the incident is not helpful.

C. Incorrect. Only registering the incident is not enough.

D. Correct. The employee should be informed, the CD is the proof of the incident and it should be registered so the organization can learn. See Information Security Fundamentals §1.2.1 and ISO/IEC 27002:2005 §6.2

**13 of 30**

As part of the organization's Business Continuity Planning (BCP), a Business Impact Analysis (BIA) was completed. The Chief Information Officer (CIO) has handed you the results of the BIA and asked that you use these results to create an organizational recovery strategy for the assets listed in the BIA.

What are the four areas to consider for a recovery plan?

- A.** Location, resources, money and scope of the recovery operations
- B.** People, communications, computing equipment and facilities
- C.** People, recovery types (hot, cold, warm), communications and facilities
- D.** People, resources, computing equipment and facilities

A. Incorrect. These are good things to keep in mind but resources and money are basically the same thing.

B. Correct. According to Peltier the four key considerations for BCP are people, communications, computing equipment and facilities. See Information Security Fundamentals §9.5.2

C. Incorrect. Recovery types and facilities are basically the same thing.

D. Incorrect. People and resources are basically the same thing.

**14 of 30**

An HR manager of a company wants to write a policy for illustrating the standard behavior required of all staff.

How is this policy usually called?

- A.** Employee Disciplinary Code
- B.** Records Management
- C.** Standards of Conduct
- D.** Workplace security standards

- A. Incorrect. Disciplinary measures are not written in a conduct policy.
- B. Incorrect. Records Management is not described in a conduct policy.
- C. Correct. In the standards of conduct the behavior required of all staff is written. See Information Security Fundamentals §4.2
- D. Incorrect. Workplace security standards are not written in a conduct policy.

**15 of 30**

In the company where you work as Information Security Manager (ISM), the division directors are accountable and have their own support services at their disposal. You have posted an Information Security Coordinator in each division. One of them reports in a coordination discussion that their division director has decided to institute a more severe access policy.

What does this lead to?

- A.** This leads to reporting this to top management with the request to reverse the decision.
- B.** This leads to revision of the information security plan for the division in question.
- C.** This leads to revision of the information security policy.
- D.** This leads to revision of the risk analysis of the division in question.

- A. Incorrect. The division manager is independent and may create his/her own interpretation of risk management, as long as it is not lower than the baseline of the whole company.
- B. Correct. Only one measure is revised. See Information Security Fundamentals §3.2
- C. Incorrect. The decision does not affect the policy. These kinds of interim deviations would be able to be taken into account in the next round of the Plan Do Check Act (PDCA) cycle.
- D. Incorrect. The risk analysis does not have to be revised.

**16 of 30**

Who determines the security classification of information?

- A.** The custodian of the information
- B.** The owner of the information
- C.** The user of the information

A. Incorrect. The custodian can be requested by the owner to protect the information according to the set rules.

B. Correct. The owner determines the classification of the information, because he or she is responsible for the adequate level of protection of the information. See Information Security Fundamentals Chapter 5

C. Incorrect. The user is not necessarily the owner of the information.

**17 of 30**

It is advisable to have a number of security classification levels in your organization for the classification of information (assets).

What is the primary reason for identifying different classes of data?

- A.** We are able to design information security controls that rely on layered defensive measures to protect all the classes of data.
- B.** We can design information security controls that are dedicated for each of the different levels.
- C.** We can focus our limited money and people resources on protecting the data and systems that need to be protected.
- D.** We can make it easier for employees to know which data they are allowed to access during the course of doing their jobs.

A. Incorrect. The reason for establishing data classes is to make it so that we don't have to protect all the organization's data.

B. Correct. Classification allows establishing pre-defined levels of protection. See Information Security Fundamentals §5.3

C. Incorrect. Even risk assessment allows defining controls aimed at protecting data and systems.

D. Incorrect. It is important that employees understand which data classes they can access but this is not a primary reason for the establishment of data classes.

As the Chief Information Security officer (CISO) you know that important organizational information should be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual and business requirements. The system of storage and handling for this organizational information should ensure clear identification of records and of their retention periods.

To meet these control objectives, which steps should you implement?

- A.** an information incident management program, a security awareness program and a comprehensive identity management methodology
- B.** guidelines for retention, storage, handling and disposal of information, an inventory of sources of key information and appropriate controls
- C.** implement a data protection and privacy policy, encrypt all regulated data in transit and storage and provide annual training to the custodians of the information
- D.** using appropriate audit tools, obeying copyright laws and ensuring that any related cryptographic keying materials are stored to enable decryption of the records for the length of time they are retained

A. Incorrect. These are all good ideas but pertain to the establishment of an information security program.

B. Correct. These are the steps that need to be taken in order for an organization to meet record safeguarding objectives for organizational information. See ISO/IEC 27002:2005 §15.1

C. Incorrect. These are all good ideas but pertain to data privacy and security awareness programs.

D. Incorrect. These are some of the steps for the safeguarding and protection of intellectual property.

**19 of 30**

Risk assessment is the process that allows business managers to balance operational and economic costs of security controls and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise.

When should a risk assessment be conducted?

- A.** It should be repeated periodically to address any change that might influence the risk assessment results.
- B.** When an organization wants to take control of its own destiny by ensuring that only those controls that are actually needed will be implemented.
- C.** When management wants to eliminate the risk associated with implementing a service or product.
- D.** When senior management has to prove to internal or external auditors that they are showing due diligence.

A. Correct. As per §0.4 of ISO/IEC 27002. See Information Security Fundamentals §8.2.2  
B. Incorrect. Taking control of ones own destiny is one of the reasons why a risk analysis should be conducted but does not answer the question of when a risk assessment should be conducted.  
C. Incorrect. The goal of risk assessment and risk analysis is to show if a proposed approach has an acceptable risk level for proceeding. In very rare cases all the risk associated with an approach can be eliminated.  
D. Incorrect. Showing due diligence is one of the reasons why a risk analysis should be conducted but does not answer the question of when a risk assessment should be conducted.

**20 of 30**

Which method for risk analysis provides the best basis for the measures that must be taken?

- A.** qualitative risk analysis
- B.** quantitative risk analysis
- C.** it makes no difference

A. Incorrect. The method for risk analysis is independent of the measures to be taken.  
B. Incorrect. The method for risk analysis is independent of the measures to be taken.  
C. Correct. The method for risk analysis is independent of the measures to be taken. See Information Security Fundamentals §8.4

**21 of 30**

An Information Security Officer (ISO) working for you has come to you after he conducted a threat identification and determined the impact of a threat on a system that is being implemented. Your ISO asked for your opinion on the security controls he is recommending to the project team.

What is the basic reason for the identification of recommended controls?

- A.** To clearly document the results in a standard format and issue a report to the board of directors or Chief Information Officer (CIO).
- B.** To ensure that the entire enterprise is mitigating or minimizing the risks associated with the implementation of a new service or product regardless of the cost associated with establishing adequate controls and safeguards.
- C.** To identify controls eliminating or reducing the risk to an acceptable level.
- D.** To protect the information and to make sure that outstanding vulnerabilities don't exist on deployed assets.

A. Incorrect. This is not the reason for identifying controls.

B. Incorrect. Controls must be monetarily compared in regards to what they are trying to protect. If the control costs more than the asset it is designed to protect it might not be smart to implement the control for that asset.

C. Correct. Identification of adequate controls and safeguards to eliminate or reduce risk in order to show due diligence is the basic principle of control management. See Information Security Fundamentals §8.4.5

D. Incorrect. Controls and safeguards might ensure that vulnerabilities don't exist on deployed assets but they are more focused on ensuring that an acceptable level of risk exists in regards to how vulnerable an asset is. An asset can be vulnerable and have vulnerabilities but still be within an acceptable range of risk.

**22 of 30**

For the formulation of the list with the security measures to be introduced, a member of the management team proposes using the ISO/IEC 27002 as the basis for the security requirements.

What is your reaction?

- A.** You indicate that if the organization uses the ISO/IEC 27001 standard instead, the organization will also be able to be certified.
- B.** You indicate that the ISO/IEC 27002 standard in this case had better not be used because this standard does not contain the initiating of security measures.
- C.** You indicate that this standard should be used wisely, because the requirements in the ISO/IEC 27002 easily can lead to an extensive range of measures.

- A. Correct. ISO/IEC 27002 describes best practices while ISO 27001 consists of the requirements. Certification is possible against ISO/IEC 27001. See Information Security Fundamentals §8.6
- B. Incorrect. The ISO/IEC 27002 consists of initiation, introduction and management of the measures.
- C. Incorrect. The ISO/IEC 27002 does not contain requirements but rather describes best practices.

**23 of 30**

Your manager is a little bit confused about standards and guidelines. She has understood that the Information Security Management System (ISMS) can be certified against an ISO standard, but she doesn't know which one, ISO has published too many standards!

What is your answer?

- A.** ISO/IEC 15408-1:2005
- B.** ISO/IEC 17799:2005
- C.** ISO/IEC 27001:2005
- D.** ISO/IEC 27002:2005

- A. Incorrect. This is the standard for information technology and security techniques.
- B. Incorrect. This is the former number of the ISO/IEC 27002:2005
- C. Correct. Information Security Management Systems can be certified against ISO/IEC 27001:2005.
- D. Incorrect. This is the Code of Practice.

**24 of 30**

You are the Information Security Manager (ISM) in your organization. You want to check if the controls that were implemented are adequate. You want to assess the controls against the complete ISO/IEC 27002 standard. The owner of one of the information systems expresses the opinion that the use of the ISO standard is an “overkill”.

What is your reaction?

- A.** You understand the criticism and ask the owner to provide a tailor-made standard document.
- B.** You state that the standard is suitable, because the enterprise-wide analysis consists of more than one information system.
- C.** You state that you will investigate whether you can use only parts of the ISO standard.

A. Incorrect. Making a standard document yourself is a large job and will cause a huge delay in the analysis.

B. Incorrect. Although the ISO standard will fit the organization in its entirety, the question is if the ISO standard is the right standard to use for this control.

C. Correct. It could be that using parts of the ISO/IEC standard is enough. See Information Security Fundamentals §8.6

**25 of 30**

What kind of legislation is in place to ensure that an enterprise maintains the confidentiality of personal information that it may hold?

- A.** A Computer Misuse Act
- B.** A Data Protection Act
- C.** A Freedom of Information Act

A. Incorrect. A computer misuse act is a provision for securing computer material against unauthorized access or modification.

B. Correct. A data protection act protects personal information. See Information Security Fundamentals §4.6

C. Incorrect. A freedom of information act defines what information public sector organizations are obliged to provide on request.

**26 of 30**

After having implemented technical and organizational controls, what security controls should an enterprise enforce before staff handle personal data?

- A.** It should ensure that all staff have access to personal data when required.
- B.** It should ensure that staff are aware of enterprise security controls.
- C.** It should introduce a new Tier 1 policy for personal data.
- D.** It should introduce biometric access control mechanisms.

- A. Incorrect. Not all staff should have access to personal data.
- B. Correct. Staff should be aware of enterprise security controls. See Data Protection Checklist
- C. Incorrect. A policy for personal data is not a separate Tier 1 policy.
- D. Incorrect. This is only a physical control, which is not enough to protect personal data.

**27 of 30**

The CIO has asked you, the Chief Information Security Officer (CISO), to help work on the security aspects of a 3rd party contract. She asks you to first investigate in ISO/IEC 27002 what should be included in the contract to make sure statutory requirements are met.

What is your finding?

- A.** Agreements can have considerable variance for different organizations and among different types of third parties. Care should be taken to include all identified risks and security requirements.
- B.** All employees, contractors and 3rd party users should return organizational assets in their possession when they terminate employment.
- C.** Background verification checks on all candidates for employment, contractors and 3rd party users should be carried out in accordance with relevant laws.
- D.** Security perimeters should be used to protect areas that contain information and information processing facilities used by the 3rd party vendor.

- A. Correct. This is an approach suggested by ISO 27002 to addressing security in 3rd party agreements. See ISO/IEC 27002:2005 §6.2
- B. Incorrect. This is a good control but it does not address the entirety of what the CIO is asking you to provide. This is a single control listed under §8.3.2 in ISO 27002:2005.
- C. Incorrect. This is a good control but it does not address the entirety of what the CIO is asking you to provide. This is a single control listed under §8.1.2 in ISO 27002:2005.
- D. Incorrect. This is a good control but it does not address the entirety of what the CIO is asking you to provide. This is a single control listed under §9.1 in ISO 27002:2005.

**28 of 30**

What should first be in place before allowing an external party access to enterprise wide information?

- A.** a security chapter in the Service Level Agreement (SLA)
- B.** background checks on the staff of the external party
- C.** full access control mechanisms
- D.** induction training for external parties

- A. Correct. First the security agreements should be defined in a contract. See Information Security Fundamentals §4.4
- B. Incorrect. This is possible but not always necessary.
- C. Incorrect. The control mechanisms should be in place but only after the contract has been signed.
- D. Incorrect. This is important but can be done after the contract has been signed.

**29 of 30**

You are the Information Security Officer (ISO) in your organization and before performing a complete risk analysis you decide to conduct a walk-about.

Which information will you have learned during the walk-about?

- A.** The employees' mind-set towards information security controls.
- B.** Whether it is necessary to do a complete risk analysis or not.
- C.** Which physical controls will be necessary for implementation.
- D.** Who is responsible for which information.

- A. Correct. A walk-about, checking if assets, cabinets, rooms are secured, will help gauge the mind-set of the employees towards controls. See Information Security Fundamentals §1.2.1
- B. Incorrect. A complete risk analysis will still be necessary.
- C. Incorrect. Conclusions about physical controls can only be drawn after a complete risk analysis.
- D. Incorrect. This is defined in a classification process.

You are one of the internal auditors in your organization. The audit plan has been determined and your team is setting up an audit program.

What is the correct order of the next steps that should be taken?

- A.** Determine the frequency of the audits, audit work programs, audit reports, storage requirements for the documentation collected during the audits, follow-up of the findings and development paths for the required audit expertise.
- B.** Execution of the audits by independent auditors, audit reports, correction of the findings, determination of the date for the next audit per analysis area and monitoring of the risk analysis and the changes thereupon.
- C.** Preparation of the audits, including follow-up of the remaining open audit findings, performance of the audits, prioritizing the recommendations, correcting the non-conformities, verification of the corrections.
- D.** The risk analysis, the audit work programs including objectives, the authorizations and responsibilities of the required (internal) auditors, audit findings and compliance thereof.

- A. Correct. Collect and process the audit findings along with improving the audit process form part of the audit program. See Audit Booklet section Internal Audit Program
- B. Incorrect. Determining the next date for an audit / audit cycle comes before the audit plan; monitoring the (changes of the) risk analysis is not mandatory.
- C. Incorrect. The storage requirements for source material and the development paths of the audit professionals are missing.
- D. Incorrect. Risk analysis is ahead of the audit plan and the development paths of the audit professionals are missing.

## Evaluation

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

<b>number</b>	<b>answer</b>	<b>points</b>
1	<b>A</b>	1
2	<b>A</b>	1
3	<b>B</b>	1
4	<b>B</b>	1
5	<b>B</b>	1
6	<b>A</b>	1
7	<b>B</b>	1
8	<b>A</b>	1
9	<b>B</b>	1
10	<b>B</b>	1
11	<b>D</b>	1
12	<b>D</b>	1
13	<b>B</b>	1
14	<b>C</b>	1
15	<b>B</b>	1

<b>number</b>	<b>answer</b>	<b>points</b>
16	<b>B</b>	1
17	<b>B</b>	1
18	<b>B</b>	1
19	<b>A</b>	1
20	<b>C</b>	1
21	<b>C</b>	1
22	<b>A</b>	1
23	<b>C</b>	1
24	<b>C</b>	1
25	<b>B</b>	1
26	<b>B</b>	1
27	<b>A</b>	1
28	<b>A</b>	1
29	<b>A</b>	1
30	<b>A</b>	1