INFORMATION SECURITY FOUNDATION

Sample Exam Questions

SECO INSTITUTE

Introduction

This document contains 5 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's Information Security Foundation certification exam.

To download our Complete Sample Exam, create a free study account at https://members.seco-institute.org

We recommend you to take the Complete Sample Exam before registering for the certification exam.

The results of the Sample Exam do not count towards your examination score.

Certification exam

You can book your exam with an accredited training partner or directly with the SECO-Institute. Attending a course is not a prerequisite for taking a certification exam.

To book an exam with the SECO-Institute, go to: https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/

By passing the certification exam and earning a SECO-Information Security Foundation certificate, you demonstrate that you have a good understanding of information security management according to ISO/IEC 27001 and ISO/IEC 27002. You are familiar with information security risks and best-practice physical, organisational and technical information security measures.

Exam format

Computer-based with remote proctoring

- 40 multiple-choice questions
- Time allowed: 60 minutes
- Closed-book exam
- Pass mark: 60%

Questions

Question 1

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

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

Question 2

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

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

Question 3

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

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

Question 4

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

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

Question 5

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

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

Answers

Question 1

The correct answer is D.

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

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

Question 2

The correct answer is A.

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

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

Question 3

The correct answer is B.

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

Module 2: Information and Security

Question 4

The correct answer is D.

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

Module 2: Information and Security

Question 5

The correct answer is B.

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

Module 2: Information and Security