INFORMATION SECURITY PRACTITIONER

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 Practitioner 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. To schedule an exam at the SECO-Institute's website, go to: https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/

By passing the certification exam and earning an Information Security Practitioner certificate, you demonstrate that you can apply information security management principles to the human, organisational and technical domains of information security. You can establish effective information security governance, you can raise information security awareness across your organisation, and you can implement effective information security controls that allow you to mitigate security risks.

Exam format

- Computer-based with remote proctoring
- Multiple-choice questions and essay-type questions
  - 10 multiple-choice questions
  - 5 open-ended questions
  - 1 essay question based on a case study

- Time allowed : 120 minutes
- Closed-book exam
- Pass mark : 60% of the total marks

Questions

Question 1

Which information reliability aspect is "completeness" a part of?

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

Question 2

What are three data protection principles set out in the GDPR?

A. Purpose limitation, availability, data minimisation
B. Purpose limitation, data minimisation, transparency
C. Target group, transparency, data minimisation
D. Purpose limitation, pudicity, transparency

Question 3

Information security measures can be categorised into different groups based on their goal. Name 4 of these groups.

Question 4

What are the most important 'security' concerns posed by Bring Your Own Device (BYOD)?

Question 5

Bicsma is outsourcing some of their IT operations to a cloud provider. Bicsma would like to sign a processing agreement with the cloud provider. What should the processing agreement include?

Answers

1. The correct answer is **C**. Completeness is a part of integrity.

2. The correct answer is **B**. Three of the GDPR's data protection principles are purpose limitation, data minimisation and transparency.

3. Information security measures can be categorised into groups depending on their goal.
   In this type of classification, the groups are: Prevention, Reduction, Detection, Repression, Correction and Evaluation.

4. The main security concerns posed by Bring Your Own Device (BYOD) are:
   - Insufficient physical control
   - Use of insecure mobile devices
   - Use of insecure networks
   - Use of apps originating from unknown parties
   - Interaction with other systems
   - Use of insecure content
   - Use of local services

   Bottom line: No more control over the IT environment!

5. Elements to include in a processing agreement:

   Processing: The processor may only process the personal data on the controller's instructions. Use of the personal data for the processor's own purposes should not be allowed (except if there is a compelling reason, for example the processor's legal obligations).

   Confidentiality: The processor must comply with a confidentiality obligation, possibly combined with a penalty clause.

   Security: The responsible party shall ensure that the processor takes appropriate technical and organisational measures to protect personal data against loss, destruction, or any other adverse event.

   Third parties: When and under what circumstances can sub-processors be involved?

   Location of data: In which countries may the data be stored?

   Audits: Agreement stating that the responsible party will perform an audit.