INFORMATION SECURITY

PRACTITIONER

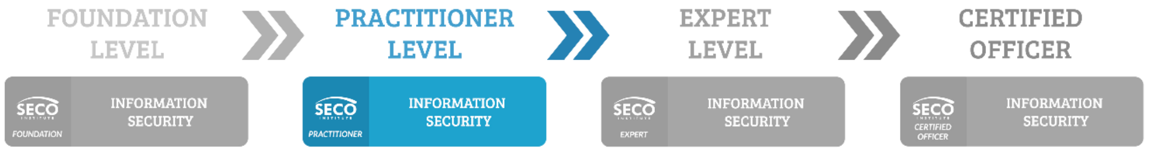
Sample Exam

SECO

INSTITUTE

Sample Exam Information Security Practitioner

SECO-Institute issues the official Cyber Security & Governance courseware to accredited training centres where students are trained by accredited instructors. Students can take their exams at an accredited exam centre or directly at the SECO-Institute. Attending an official certification course is not a prerequisite for taking an exam. Upon successful completion of a certification exam (with a passing score of 60%), students can claim their certification titles at the SECO-Institute, whereupon they will receive a title and a digital badge.


FOUNDATION LEVEL
PRACTITIONER LEVEL
EXPERT LEVEL
CERTIFIED OFFICER
SECO FOUNDATION INFORMATION SECURITY
SECO PRACTITIONER INFORMATION SECURITY
SECO EXPERT INFORMATION SECURITY
SECO CERTIFIED OFFICER INFORMATION SECURITY

This document provides a sample exam for you to familiarise yourself with the structure and topic areas of the current Information Security Practitioner examination. We strongly recommend you to test your knowledge before taking the actual assessment. The results of this test do not count towards your certification assessment.

Examination type

Computer-based

- 10 Multiple choice: 3 points per question
- 5 Open questions: 8 points per question
- 1 Case study: 30 points per case

Time allotted for examination

120 minutes

Examination details

- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam.

This sample exam consists of:

- 2 Multiple choice questions
- 8 Open questions
- 1 Case study

Note that the certification assessment contains 10 multiple choice questions and 5 open questions. This sample exam contains less multiple choice and more open questions to help students better prepare for questions addressing the practical application of the acquired knowledge.

Questions

Question 1

Which of these reliability aspects is "completeness" a part of?

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

Question 2

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

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

Question 3

Measures can be divided into different categories. Name 4 of these categories.

Question 4

One of the ways Internet of Things (IoT) devices can communicate with each other (or ‘the outside world’) is using a so-called short-range radio protocol. Which kind of short-range radio protocol makes it possible to use your phone as a credit card?

A. Near Field Communication (NFC)
B. Bluetooth
C. Radio Frequency Identification (RFID)
D. The 4G protocol

Question 5

Explain how adaptive authentication works, and why it is more secure than traditional methods.

Question 6

Describe the relationship between the information security organisation and the business on one hand, and the relationship between the information security organisation and the line organisation on the other. When describing these relationships, strive to demonstrate the added value of an information security organisation.

Question 7

You’re starting a job at an organisation where information security doesn't really exist yet. You are asked to draw up a security policy plan. Name the elements that should be included in the plan and describe what links can be established between these elements. Describe in what order you would develop the elements.

Question 8

Describe the difference between ISO/IEC 27001 and ISO/IEC 27002. Describe how these two documents are related.

Question 9

Describe briefly how a control measure from ISO/IEC 27001 should be implemented.

Question 10

Why do organisations need a vision on information security?

Case Study

Implementation of a control measure: access control of software source code

12.4 Securing system files
Objective: Ensure system file security.

Access to system files and software source code should be controlled. IT projects and supporting activities should be carried out in a secure way. Exposure of sensitive data in test environments should be prevented.

12.4.3 Access control of software source code

Control measure

Access to software source code should be limited.

Implementation guidelines

Access to software source code and related things (such as designs, specifications, verification and validation plans) shall be strictly controlled to prevent unauthorised functionality and avoid unintended changes. For program source code, this can be achieved through a controlled central storage of the code, preferably in source code libraries. That provided, the following guidelines should be considered (also see Chapter 11) to control access to these source code libraries and, consequently, reduce the chance of computer software corruption:

- *wherever possible, avoid storing source code libraries in production systems;*
- *software source code and source code libraries should be controlled according to established procedures;*
- *maintenance staff should not be granted unlimited access to source code libraries;*
- *the update of source code libraries and related issues should only be performed after appropriate authorisation has been received;*
- *program launchings? should be kept in a secured environment (see 10.7.4);*
- *any access to source code libraries should be recorded in an audit log file;*
- *maintaining and copying source code libraries should be subject to strict change control procedures (see 12.5.1).*

Additional information

Software source code is programmed code compiled (and linked) to obtain executable code. Certain programming languages don't make a formal distinction between source code and executable code because executable code is created at the time of activation.

ISO 10007 and ISO/IEC 12207 provide further information about configuration management and the life cycle process of software.

Question

Elaborate the “Access control of software source code” control measure in concrete implementing measures and describe how the measures should be implemented. Explain how planning and quality should be monitored during implementation. Delegate tasks, powers and responsibilities to the relevant roles within your organisation. You can also use Bicsma as your model organisation when answering this question.

Hint: If necessary, you can make assumptions about the functioning of your model organisation. In such cases, indicate clearly what assumptions you have made so that it is also clear to the assessor.

Answers

1. C

2. B

3. Prevention, Reduction, Detection, Repression, Correction, Evaluation

4. The correct answer is A.

   Explanation:

   B: incorrect; Bluetooth is used to connect devices (e.g. a phone) to a wireless speaker.

   C: incorrect; RFID is used for 'logistics' identification, e.g. timing athletes in a marathon, tracking attendees at a conference, or asset tracking (using smart tags).

   D: incorrect; 4G is a mobile telephone protocol (also known as LTE-A).

5. Adaptive authentication is the analysis of multiple factors of, for example, a login attempt and adaptive risk management. Is the attempt made from a known device? Is the IP address legitimate? Is the identity profile correct? Is the attempt made from a known location? Is the time of the event part of the user's normal behaviour? If any of these factors is not correct, access can be refused.

6. The information security organisation forms a link between the business and the implementation organisation regarding the selection and implementation of the appropriate control measures. The business sets goals and frameworks for the primary processes, derives goals from these for information security, and manages risks. The information security organisation controls risks, and thereby ensures the reliability of the business processes. The measures taken safeguard the availability, integrity and confidentiality of information in such a way that the feasibility of the business goals is optimally supported. The implementation organisation implements the selected measures, whereby risks are addressed.

7. List the most important elements of the ISMF and describe their mutual relationships. General knowledge of ISMF.

8. ISO/IEC 27001 describes a quality management system for information security (ISMS). It also defines control objectives and control measures that such a system must comply with. The annex further elaborates on the necessary control objectives and control measures. Implementation, however, is not taken into account in this standard. ISO/IEC 27002 is based on the same control objectives and control measures. It describes what has to be done as well as the optimal way of doing it. ISO/IEC 27001, thus, has a normative character, whereas ISO/IEC 27002 is of descriptive nature. ISO/IEC 27002 provides an overview of best practices and has no normative role.

9. Theoretically, implementation follows the PDCA cycle. This means: Ask yourself if the control measure is relevant for the organisation and how the goal you set can be achieved in the most effective and efficient way. Thereafter, agree on who will do what: delegate tasks and responsibilities and prioritise plans and activities.
   Implement: Simply do what has been agreed upon and remember to control quality and progress.
   Demonstrate: Show stakeholders that the agreements made have been properly implemented.
   Evaluate: Check if the goal has really been achieved or if there is still room for improvement.

10. Because every information security measure must be related to the business. A vision on information security shows how information security can optimally support the business and how it can contribute to the success of the organisation.

11. **Case study**

    Draw up a framework including policy, procedures and tools that ensure that access to the source code is granted exclusively according to pre-defined ways. You need to ensure that the pre-defined way also is the only means of access in practice, and that there is posterior compliance control.

    During the development of this control, also consider that you can never put it together alone and that you shouldn't even try it (as you don't want to be seen as someone "too operational" instead of "managerial"). You should create an infrastructure where you can monitor both quality and progress yourself, but where others can also do their own job. Also consider that an auditor must be able to assess whether you fulfilled the control objectives in a concrete and sufficient manner and as agreed upon.

    Where you can and should fulfil an important role is facilitating the work of those who are carrying the tasks out. Clarify what exactly you expect from them and provide them with resources that facilitate their work. You need to define criteria in order to enable colleagues to monitor when access should or shouldn't be granted as well as how granting access should take place. In addition, consider templates / forms or software that ensure a high degree of uniformity in the process.

    The slides on standards provide an overview ("Implementation of ISO/IEC 27001 and ISO/IEC 27002 measures") of the things the Security Manager should arrange for this purpose, as well as the questions Security Managers should ask themselves to chart all relevant information.

How to book your exam?

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://www.seco-institute.org/certification-exams/how-to-book-exam/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

Review the examination rules at
https://www.seco-institute.org/html/filesystem/storeFolder/10/Rules-and-Regulations-for-SECO-Institute-Examinations-2017-11.pdf

Claim your title and digital badge

Upon successful completion of an exam, students can claim their **S-ISP title** at the SECO-Institute. Each certification level requires a certain number of Continuing Professional Education (CPE) hours over an annual and a three-year-period. This requirement must be met in order to retain a certification. Practitioner certifications require a minimum of 20 CPE credits yearly (60 in the three-year certification cycle).

SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

Claim your title at: https://www.seco-institute.org/claim-your-title

ISP-Sample_Exam-EN-v1.0

Although the SECO Institute has done everything to prevent irregularities in this document, errors may still occur. Therefore, any person who acts on the basis of the content of this document does so at his/her own risk and is aware of the fact that the SECO Institute cannot be held accountable for any possible damage ensuing from his/her actions.

The authors of this document have done their utmost to identify all possible rightful parties other than the SECO Institute. Should you be a rightful party, or represent one, or know one, and be of the opinion that this document unjustly contains copyrighted material, please do not hesitate to contact the SECO Institute.