



# Self Assessment Report II

---



Funded by the  
Erasmus+ Programme  
of the European Union



Funded by the  
Erasmus+ Programme  
of the European Union



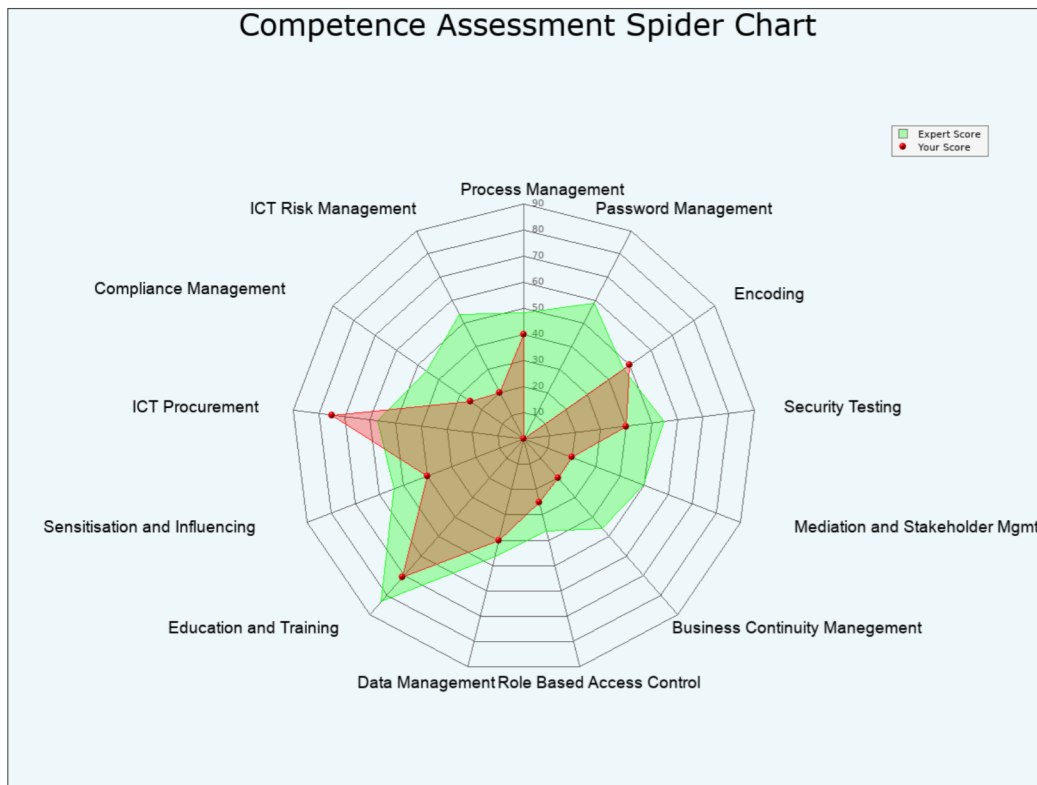
This document is licensed under CC BY-SA 4.0.

This document was produced as part of the ERASMUS+ project "Partial certification in the professional field of information security - TeBeiSi", Project ID: 2018-1-EN02-KA202-005218.

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

# Competence Assessment Information

## Security in SME



**DISCLAIMER:** Please note that this result is not the exact representation of once knowledge and cannot be used as an official confirmation of your achievement to any authorised community or organization. The survey was created by experts in information security curriculum standard creators, to give an overview of individual area of improvements. We do not take any responsibility in the event that your result fails to display or for any error in your result, weather due to technical error or administrative procedure. We do not store any personal data of the test taker, we generate and store a random ID for the each test and that ID can not be linked to the user or the network/system user submitted the test on.

# Certificate of Recognition

This certificate is awarded to

*Sample Report*

---

In recognition of the successful completion of the Information Security Assessment for SMEs.

29/10/2021

Date

---



# Process Management

---

## ABOUT

To analyse business processes and produce a strategic report concerning data protection and information security

Your Assessment Percentage: 40%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of a structured process analysis in a firm. They are capable to recognise processes which evoke the necessity of further analysis considering their data and information security exposure. Participants are being familiar with process documentation and are capable to monitor changes in the working routine. They are capable to prepare documentation which allows for the formulation of recommendations for action.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- You need to learn more about Information security that you can explain to other people in your organization
- You need to learn how to apply GDPR guidelines
- Learn about communication techniques and channels.

# ICT Risk Management

---

## ABOUT

Track changes in and outside the firm which have an impact on the firm's security strategy and produce reports for employees.

Your Assessment Percentage: 20%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand dynamics of technological change and their influence on the firm's strategy to mitigate risks. They are capable to decide upon the urgency of reacting to these risks. Participants will be able to track technological developments within and outside the firm and to provide assessments on the firm's risk exposure.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Learn about risk exposures in the firm.
- You should focus on learning about new developments and upcoming new threats
- You should know about how to get rid of the vulnerabilities.
- Know about determining the volume and purpose of personal data which is processed within the firm.

# Compliance Management

---

## ABOUT

Write company guidelines on how to deal with specific information and data.

Your Assessment Percentage: 25%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of codifying company behavioural guidelines in order to establish proper conduct with data and information. They learn how to set guidelines which establish compliance among employees. They understand the importance of preparing for foreseen and unforeseen contingencies and setting out companywide rules how to behave and measured to be taken in critical situations.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Read about identifying the strengths and weaknesses of potential solutions to compliance management related problems.
- You must learn data and information units that require special protection or treatment in the internal processes of organization.
- You should learn how to identify potential risks and threats to information security and data protection in the internal processes of organization.

# ICT Procurement

---

## ABOUT

Produce recommendations regarding items to be procured considering information security and data protection requirements of the firm.

Your Assessment Percentage: 75%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of procurement to support the implementation of information security and data protection. They learn how to position the own expertise in the procurement process of the firm. The participants are capable of exerting influence upon the purchase of new technology and machinery and to evaluate the adequacy and usability in terms of the firm's data protection and information security guidelines.

## WHAT IT MEANS FOR YOU

**Almost a perfect score! You might want to consider these points:**

- Learn to communicate the importance of security-relevant features when new technology is to be purchased.



# Sensitisation and Influencing

---

## ABOUT

Conduct (informational) activities to sensitise employees for security risks in their working routine and to spread awareness among the workforces.

Your Assessment Percentage: 40%

0-----50%-----100%

## WHAT IT COVERS

The participant learns to understand the importance of sensitizing employees and members of the board regarding data protection and information security concerns. They will learn to raise awareness for common threats and build capacities among the workforce to detect likely threats in their daily working routine. Participants will be capable of conducting analysis about the level of awareness in the firm and to implement corresponding awareness rising measures.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- You should be aware of most likely threats to your daily work and the work of your colleagues.
- Know the role of risk awareness among your employees.
- Learn to carry out an employee awareness analysis.

# Education and Training

---

## ABOUT

Create training plans for the company in order to be able to regularly train the employees with regard to information security and data protection.

Your Assessment Percentage: 71%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of education with regards to data protection and information security requirements. They learn to educate both themselves and employees of the firm. Participants will be capable to consult reliable sources and to derive training needs upon consultation or interaction with employees. Participants learn to prepare training material and train employees to incorporate adequate working routines in their daily work.

## WHAT IT MEANS FOR YOU

**You are good! You just need to know a few things:**

- Learn to find relevant information on Data Protection (GDPR).
- Learn to independently conduct trainings on Information Security and Data protection in our company.

# Data Management

---

## ABOUT

Conduct routinised back-ups of data and apply methods of proper conduct under GDPR to the data processing in the firm.

Your Assessment Percentage: 40%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of storing and processing data and information according to agreed guidelines. They learn about proper conduct with Data under consideration of the GDPR. Participants will be capable to evaluate the storage and processing of physical and electronic data in the firm and to identify potential misconduct. Participants learn to suggest alteration in the firms processes in order to mitigate these risks.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Learn to determine the volume and purpose of personal data that are being stored/processed within the organization.
- Learn to create regular backups to reduce the risk of losing valuable data and information.
- Learn to work within the group to efficiently extract information to improve processes.

# Role Based Access Control

---

## ABOUT

Establish administrator accounts and restrict access-rights among employees according to defined security levels.

Your Assessment Percentage: 25%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of limiting accessibility to data, information, or physical infrastructure when possible, and to grant access only to a group of relevant employees. They learn how to establish appropriate restrictions according to a defined security level. Participants will be capable to assign roles within the firm to clearance levels and to make access to specific information traceable if necessary.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Learn to formulate the three basic rules of RBAC.
- Learn to clearly define roles for staff in our company following the guidelines given by the management.
- Learn to assign appropriate roles to employees following the guidelines given by the management.

# Business Continuity Management

---

## ABOUT

Establish guidelines and procedures for the emergence of possible contingencies.

Your Assessment Percentage: 20%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of conducting “what if” scenarios. They learn to analyse theoretical contingencies and to prepare strategic guidelines accordingly. The participants will be capable of establishing guidelines and to predefine measures in order to be prepared and to respond coordinated to new situations when they arise.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- You must know the importance of scenarios in the safety analysis process.
- You should be able to identify theoretical emergency situations and scenarios in your company.
- You should be able to prepare guidelines for emergency situations.
- You should be able to identify measures for emergency situations.

# Mediation and Stakeholder Mgmt.

---

## ABOUT

Coordinate the needs of the firms'™ executives and employees, providing both parties with information and insights from within the firm.

Your Assessment Percentage: 20%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of coordinating with all stakeholders in the firm regarding their role and their impact on data protection and information security. They learn how to effectively communicate with different hierarchy levels (employees and management) and to align their needs and interests when changes to organisational routines occur.

Participants will be capable of interacting with stakeholders in a diplomatic way and to deal with possible resistance towards the own influence.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- You must be able to coordinate with stakeholders in the company needed in the data protection process.
- Learn, how effective communication on different levels can influence information security.
- Learn why communication technique and choice of message matter for information security.
- Learn how the person responsible for information security overcome resistance from other company employees.

# Security Testing

---

## ABOUT

Install a firewall and anti-virus software. Perform updates and apply basic methods to test the security of software used in the firm and produce a corresponding documentation.

Your Assessment Percentage: 40%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of testing existing ICT infrastructure for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) penetration testing tools to ensure the security of firewalls and communication channels.

There is an infinite number of ways to break an application. And, security testing, by itself, is not the only (or the best) measure of how secure an application is. But it is highly recommended that security testing is included as part of the standard software development process.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Learn to install anti-virus software and firewalls.
- Learn to apply basic methods to test the security of communication channels.
- Learn to document strategic changes and updates carried out.

# Encoding

---

## ABOUT

Work on securitisation of mobile devices, communication channels and data storage units via passwords or other means of authentication.

Your Assessment Percentage: 50%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of password encoding for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) password encoding tools to ensure the security of firewalls and communication channels.

Password Encoding is the process in which a password is converted from a literal text format into a humanly unreadable sequence of characters. If done correctly, it is very difficult to revert back to the original password and so it helps secure user credentials and prevent unauthorized access to a website.

## WHAT IT MEANS FOR YOU

**You are good! You just need to know a few things:**

- Learn to apply methods to encrypt email and messenger communications.
- Learn to recognise resources, information and technologies used in the firm which should be encoded.



# Password Management

---

## ABOUT

Establish passwords for individual access among employees and allow for a safe storage and recovery process.

Your Assessment Percentage: 0%

0-----50%-----100%

## WHAT IT COVERS

The participants learn to understand the importance of centralising the management of password utilisation within the firm. They will learn how to define passwords which ensure authentication (among employees) and how to reset passwords. Participants learn how to structurally create, use/manage, store and change passwords of employees.

## WHAT IT MEANS FOR YOU

**There is a scope of improvement. You could start focusing on following:**

- Learn to Restrict access to certain information through individually assigned passwords.