Identification of Competence Profiles

Analysis of reference profiles in the domain of Information Security and Data Protection

Funded by the Erasmus+ Programme of the European Union

TeBelSi

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – 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.

.

Content

1 INTRODUCTION – THE TEBEISI PROJECT 1

2 PURPOSE OF THIS REPORT 2

3 ESCO AS THE BASIS FOR COMPETENCE PROFILES 3

3.1 What is ESCO? 3

3.2 The structure of ESCO 4

3.3 The knowledge, skills and competences pillar 5

3.4 ESCO Benefits for the TeBeISi project 6

4 ESCO & RELATED EU TRANSPARENCY INSTRUMENTS 7

4.1 ESCO & ISCO-08 8

4.2 ECVET – Learning outcomes & Validation 9

4.3 EQF – European Qualifications Framework 9

4.4 European-e-Competence-Framework 11

4.5 DIGCOMP - The Digital Competence Framework 13

5 ESCO-PROFILES RELEVANT FOR TEBEISI 15

5.1 ICT security manager 15

5.2 ICT security administrator 18

5.3 Ethical Hacker 20

5.4 Policy Manager (Data protection Manager) 22

5.5 ICT security consultant (Data protection Consultant) 23

6 REQUIREMENTS IDENTIFIED BY FIELD RESEARCH 25

6.1 Method of field research 25

6.2 Participants of field research 26

6.3 Cases collected from our field research 30

6.4 First analysis of expert interviews 32

7 TEBEISI REQUIREMENTS MATCHED WITH ESCO PROFILES 33

7.1 Information Security Manager (strategic and operational level) 37

7.2 Information Security Administrator (operational level) 44

7.3 Data Protection Manager (strategic and operational level) 51

7.4 Data Protection Administrator (operational level) 58

8 TEBEISI JOB PROFILE “DP-IS OFFICER IN SME’S” 61

9 NEXT STEPS IN THE TEBEISI PROJECT 62
REFERENCES .... **Fehler! Textmarke nicht definiert.**
ANNEXES 64
Annex 1 – Cases collected from field research 64
Annex 2 – Job Profile 'DP-IS OFFICER IN SME'S' 64
RELATED DOCUMENTS 64
National Reports – Desk Research 64
National Reports – Field Research 64

List of Figures

Figure 1: What is ESCO? 3
Figure 2: ESCO three-pillar structure 4
Figure 3: The three ESCO pillar 5
Figure 4: ESCO communication gap. 6
Figure 5: ESCO mapping.. 7
Figure 6: ESCO transparency instruments. 8
Figure 7: ECVET in Europe. 9
Figure 8: Austrian example of the NQR. 10
Figure 9: DigComp into Action.. 13
Figure 10: Mapping of the competence areas of DigComp and an ESCO example. 14
Figure 11: Screenshot ESCO Portal. 15

List of Tables

Table 1: Interview Candidates from the partner Countries 30
Table 2: Mapping of Information Security Manager (strategic and operational level) 44
Table 3: Mapping of Information Security Administrator (operational level)............. 50
Table 4: Mapping of Data Protection Manager (strategic and operational level) 57
Table 5: Mapping of Data Protection Administrator (operational level)..................... 63

1 INTRODUCTION – THE TEBEISI PROJECT

The IT sector is generally characterized by short innovation and product cycles among developers and manufacturers. Due to the constantly changing requirements in the IT sector, learning and recognition of informal aspects is becoming a decisive factor in the area of information security as well. The lack of certification opportunities results in a lack of experts in the field of information security (worldwide). This problem has been known for years and poses serious challenges for the economy. Therefore, on September 3, 2018, the „Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V.“ (BF/M-Bayreuth) started the European joint project TeBeISi - "Partial Certification in the Occupational Field of Information Security" to identify and evaluate competencies in the field of information security. The Europe-wide uniform assessment and recognition of informally acquired qualifications has enormous potential in terms of combating the shortage of skilled workers in the field of information security.

The project will help to promote the recognition and certification of qualifications and competences, including those acquired through non-formal and informal learning. Through European exchange between the institutions, the certifications ofoccupational profiles that are specifically prevalent in the countries are to be processed and incorporated into newly developed occupational profiles in the exchange of experience. The project aims to transfer these profiles including certification procedures to the European partner countries and to implement them successfully in practice. The focus is on the validation of learning outcomes from non-formal and informal learning.

A large number of instruments are needed to work on the project. In order to determine the required information security competencies, extensive literature research, expert interviews and focus groups with companies are conducted. These findings serve as a basis for the creation of a catalogue of requirements. For a Europe-wide establishment, the development of recommendations for action is required. This is done, among other things, by involving associations and associated partners from the economy. The next step is the development of an online personnel questionnaire to determine information security competencies. Here the focus will be on social competences. In addition, further project steps will include the development of further education modules for training of specific sub-competencies, taking social and technical components into account. In the final project phase, a strategy paper based on the new data protection regulation, a glossary for application and the research report "Status Quo Information Security Training for SMEs" will be developed. Especially the final steps should guarantee a broad transfer of the acquired knowledge into practice, in order to finally open up chances to overcome the lack of skilled workers and to counteract the challenges of the economy.

2 PURPOSE OF THIS REPORT

In IO1 we have set ourselves the goal of finding out what concrete requirements SME's have in the fields of information security and data protection.

The findings on required information security and data protection competencies started in each partner country with a Desk Research Report, which was supplemented by Field Research Reports by each partner: We invited 60 experts for interviews and organized focus groups in order to find out more about the real needs in SME's. The outcomes of these activities serve as the basis for this current Report on Identification of Competence Profiles, which aims to further identify competences needed, both in the field of Information Security and Data Protection.

Since the aim of this transnational project is to achieve at least a partial certification of a new competence profile, we start by presenting instruments at EU level that can support us in this process. The focus is on ESCO, the instrument that enables transnational recognition of competences - even those that have not been formally acquired (see chapter 3 and 4).

In a next step we analyzed which existing ESCO profiles are most relevant for the goals of the TeBeISi project (see Chapter 5).

We then summarized the requirements resulting from the field research and carried out an initial analysis covering all partner countries (see Chapter 6).

The next important step was to match these requirements with the ESCO Profiles in order to get more concrete results. We have introduced an intermediate step: We worked with 4 fictitious profiles (or better "ideal profiles") to cover the requirements as broadly as possible (see Chapter 7).

It goes without saying that small and medium-sized enterprises cannot afford 4 jobs that deal exclusively with the topics of information security and data protection. Therefore, we have tried to break down the necessary competences into a concrete and realistic job profile of a "DP-IS Officer in SME'S" (see chapter 8).

In chapter 9 you can learn more about the further procedure and the next steps in the project.

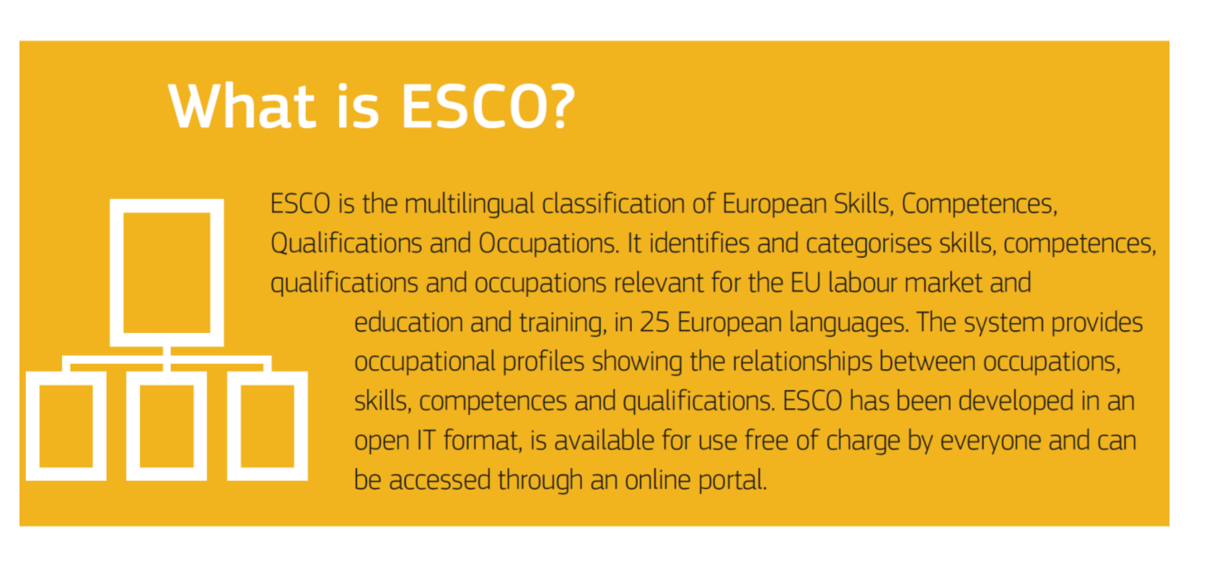
Concerning the method of presentation in the current report: We mainly refer to publications of the European Commission (see references) in order to enable the project partners to get started quickly. In a next step, e.g. in the elaboration of the curriculum (IO4), we will go into depth and establish direct contact with the relevant experts of the EU Commission and the national competent bodies (e.g. ESCO, ECVET, NQF).

But let us now start with an overview on EU-transparency tools to bring all partners of the project to the same level of knowledge.

3 ESCO AS THE BASIS FOR COMPETENCE PROFILES

In this project, we will use ESCO as the basis for the identification of skills, competences and qualifications required for suitable TeBeISi job profiles. For this reason, we first want to describe ESCO's capabilities in detail and then refer to other EU initiatives that can be perfectly integrated into the ESCO method to describe competence profiles in order to develop training curricula in a transparent and cross-national way.

3.1 What is ESCO?



What is ESCO?

ESCO is the multilingual classification of European Skills, Competences, Qualifications and Occupations. It identifies and categorises skills, competences, qualifications and occupations relevant for the EU labour market and education and training, in 25 European languages. The system provides occupational profiles showing the relationships between occupations, skills, competences and qualifications. ESCO has been developed in an open IT format, is available for use free of charge by everyone and can be accessed through an online portal.

Figure 1: What is ESCO?

Source: European Commission Directorate (2013, p. 2)

To help bridge the gap between the world of education and training and the labour market, the European Commission is developing ESCO. By introducing a standard terminology for occupations, skills, competences and qualifications, ESCO can help education and training systems and the labour market to better identify and manage the availability of required skills, competences and qualifications. Its multilingual character facilitates increased international transparency and cooperation in the area of skills and qualifications.

However, education provides people with qualifications that differ between Member States. Qualifications do not always keep pace with the evolution of knowledge, skills and competences needed by the labour market. Employment services do not share the same IT and classification systems to manage information on the supply and demand of jobs. (European Commission Directorate 2013, p. 2)

The European Commission has developed ESCO with the following aims:

- to improve the communication between the education and training sector and the EU labour market;

- to support geographical and occupational mobility in Europe;
- to make data more transparent and easily available for use by various stakeholders, such as public employment services, statistical organisations and education organisations;
- to facilitate the exchange of data between employers, education providers and jobseekers irrespective of language or country;
- to support evidence-based policy making by enhancing the collection, comparison and dissemination of data in skills intelligence and statistical tools, and enabling better analysis of skills supply and demand in real-time based on big data.

See European Commission Directorate (2017a, p. 9)

3.2 The structure of ESCO

ESCO is organised in three pillars:

- the occupations pillar;
- the knowledge, skills and competences pillar;
- the qualifications pillar.

Overall, this three-layered structured approach allows ESCO to organise terminology for the European labour market and the education/training sector in a consistent, transparent and usable way. (European Commission Directorate 2017a, p. 10)

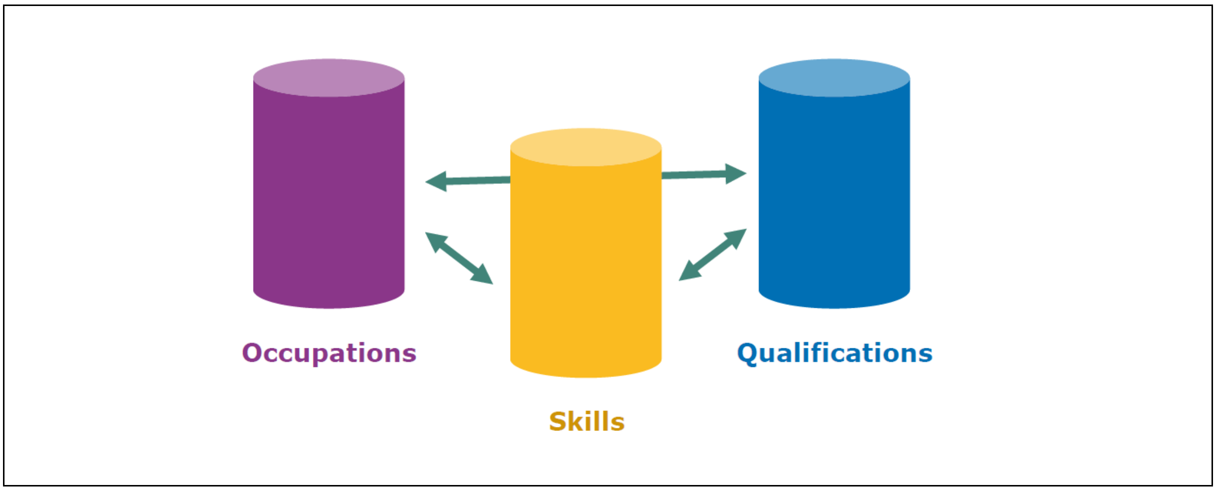


Figure 2: ESCO three-pillar structure

Source: European Commission Directorate (2017a, p. 10)

More importantly, the pillars are interlinked to show the relationships between them. Occupational profiles show whether skills and competences are essential or optional and what qualifications are relevant for each ESCO Occupation. Alternatively, the user can identify a specific skill and see which occupation or qualification this skill is relevant to.

See European Commission Directorate (2013, p. 2)

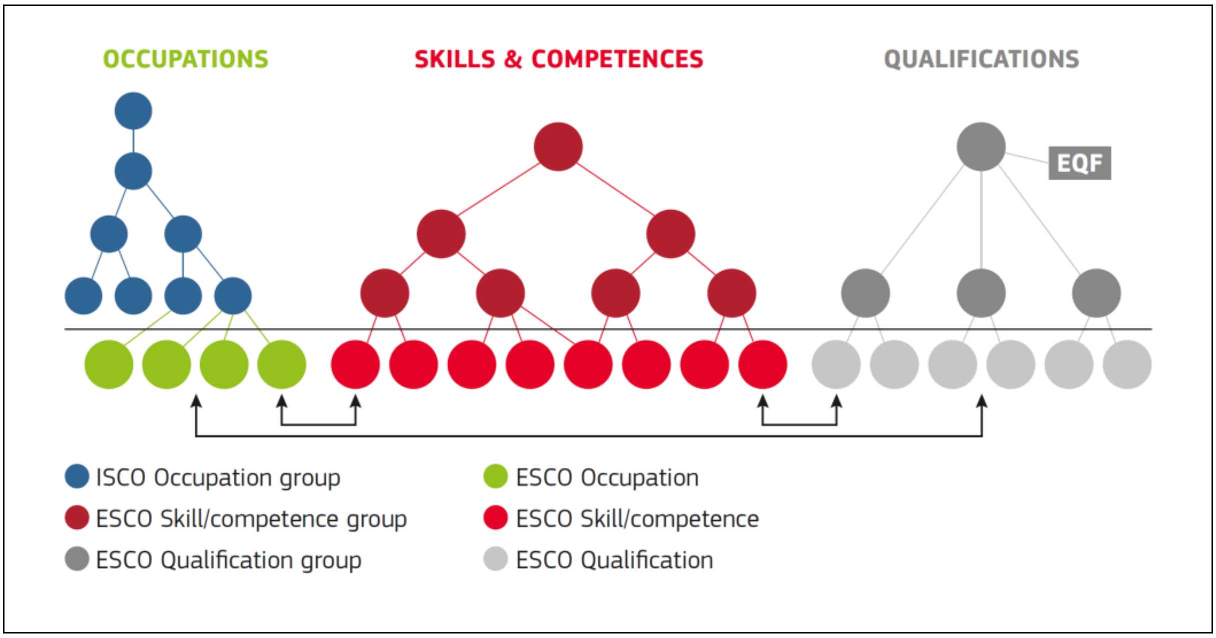


Figure 3: The three ESCO pillar

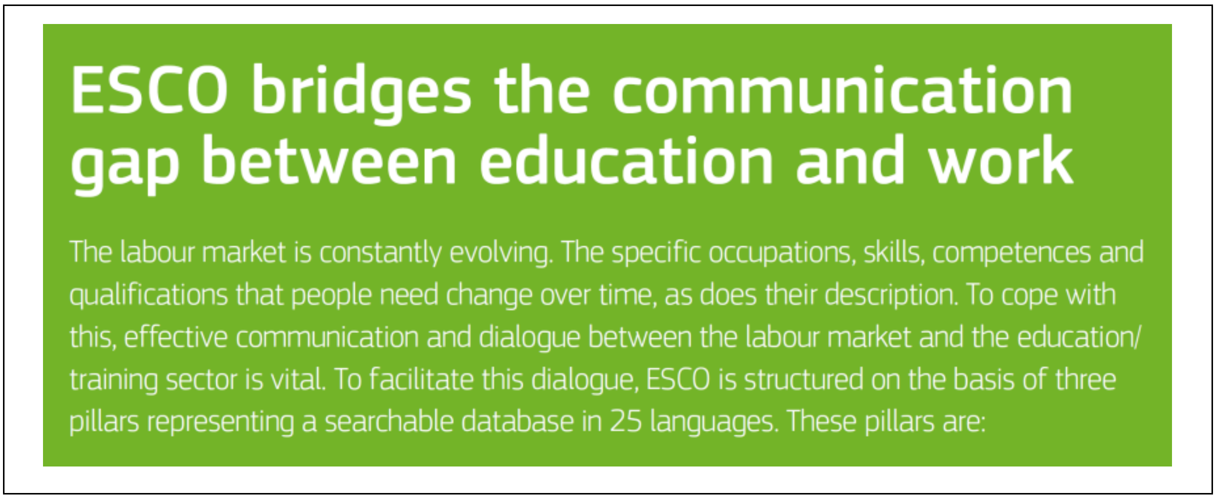
Source: European Commission Directorate (2013, p. 2)

3.3 The knowledge, skills and competences pillar

This pillar is the most important one for the project at this stage. In the Handbook the pillar is defined as follows:

- **Knowledge:** The body of facts, principles, theories and practices that is related to a field of work or study. Knowledge is described as theoretical and/or factual and is the outcome of the assimilation of information through learning.
- **Skill:** The ability to apply knowledge and use know-how to complete tasks and solve problems. Skills are described as cognitive (involving the use of logical, intuitive and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments).
- **Competence:** The proven ability to use knowledge, skills and personal, social and/or methodological abilities, in work or study situations, and in professional and personal development.

See European Commission Directorate (2017a, p. 18)



ESCO bridges the communication gap between education and work

The labour market is constantly evolving. The specific occupations, skills, competences and qualifications that people need change over time, as does their description. To cope with this, effective communication and dialogue between the labour market and the education/training sector is vital. To facilitate this dialogue, ESCO is structured on the basis of three pillars representing a searchable database in 25 languages. These pillars are:

Figure 4: ESCO communication gap.

Source: European Commission Directorate (2013, p. 9)

3.4 ESCO Benefits for the TeBeISi project

- Education and training institutions can use ESCO in curriculum development and assessment.
- Other organisations developing and/or awarding qualifications can use ESCO to express the learning outcomes of their qualifications, to reflect emerging skill needs and to facilitate the understanding of their qualifications across borders.
- Human resources managers and people offering career guidance can use ESCO to enhance planning and make aptitude or ability tests and skills and interest inventories more accurate.

See European Commission Directorate (2013, p. 2)

4 ESCO & RELATED EU TRANSPARENCY INSTRUMENTS

ESCO supports other initiatives developed by the European Commission aimed at making labour market and education systems more transparent, stimulating mobility and creating opportunities. Interested parties can reference their classification to ESCO. This is typically done by creating mapping tables that establish a relationship between each concept in their classification to a concept in ESCO.

As a result, each party that uses ESCO v1 or a classification that is mapped to it can exchange information across systems and language barriers.

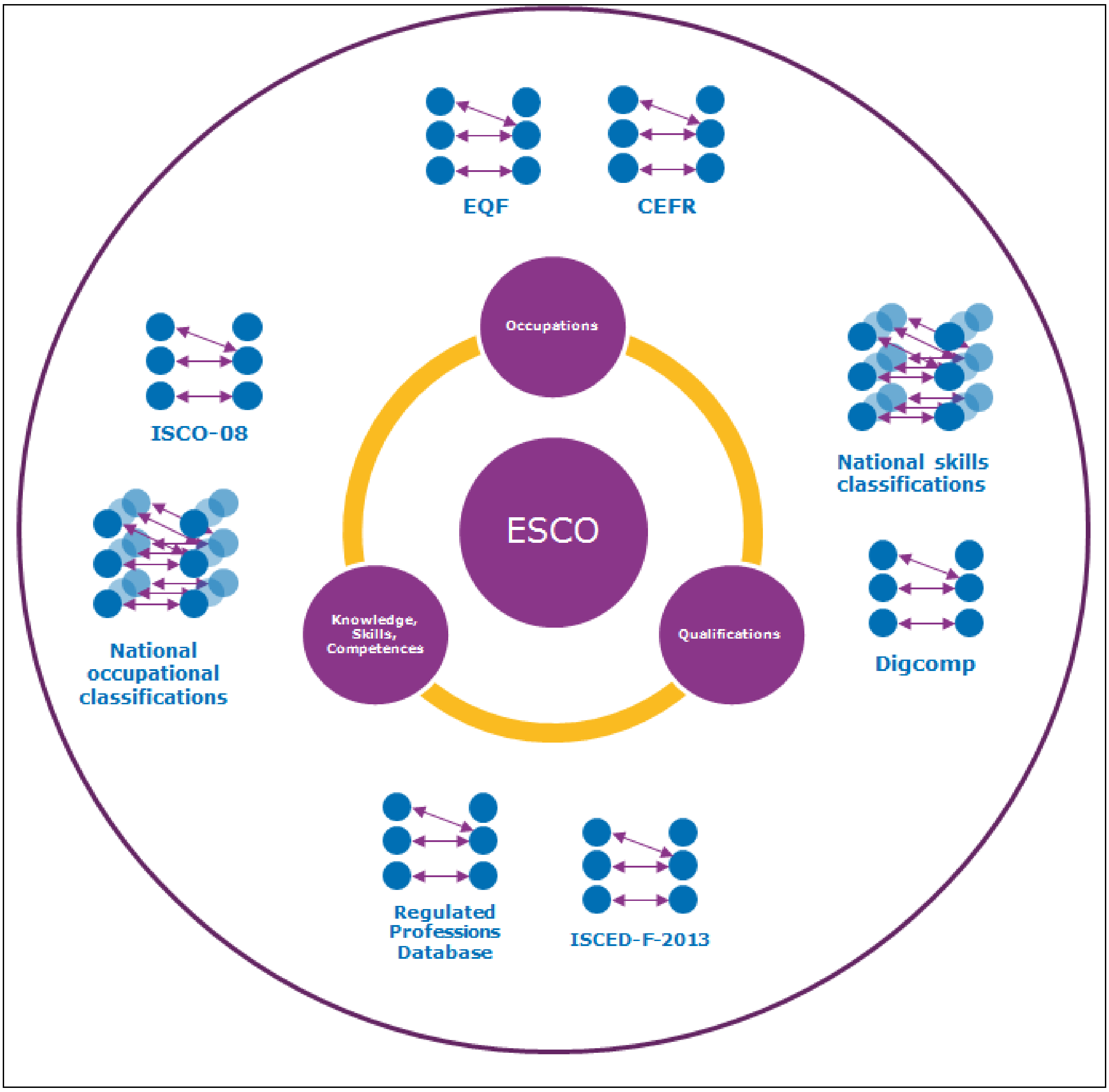

EQF
CEFR
ISCO-08
Occupations
National skills classifications
ESCO
National occupational classifications
Knowledge, Skills, Competences
Qualifications
Digcomp
Regulated Professions Database
ISCED-F-2013

***Figure 5: ESCO* mapping.**

Source: European Commission Directorate (2017a, p. 29)

The Member States and the Commission's activities in the field of regulated professions are reflected in ESCO. As ESCO is based on labour market realities, it makes use of the information in the Commission Database of Regulated Professions on access to professions or their scope of practice in Member States. However, ESCO links to information on the regulatory aspect of occupations, but it does not aim to regulate the access to professions or to define their scope of practice.

By connecting transparency instruments, ESCO provides a clearer and more complete picture of labour market and education-related information. The resulting product is put at the disposal of practical tools through the Linked Open Data approach. This ensures a low threshold for owners of labour market systems to use ESCO and enable better services.

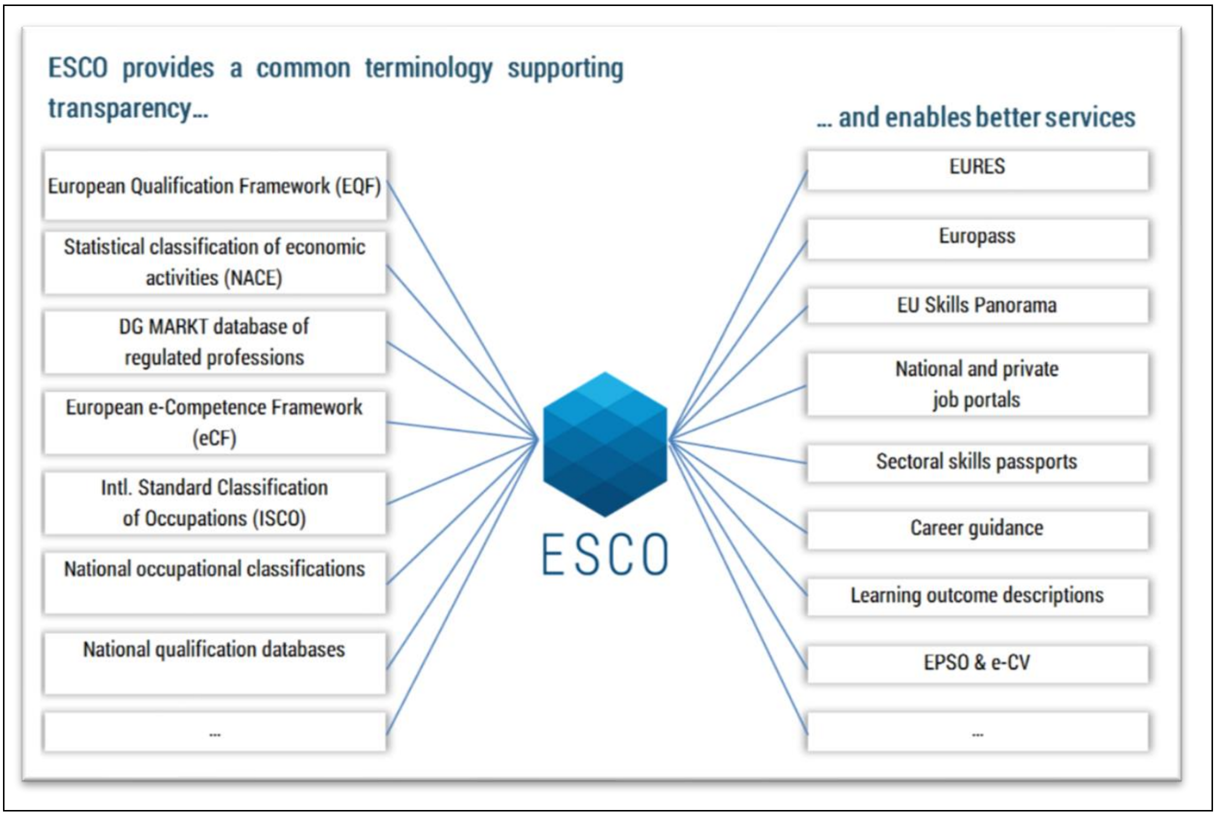

ESCO provides a common terminology supporting transparency...
... and enables better services
European Qualification Framework (EQF)
Statistical classification of economic activities (NACE)
DG MARKT database of regulated professions
European e-Competence Framework (eCF)
Intl. Standard Classification of Occupations (ISCO)
National occupational classifications
National qualification databases
...
ESCO
EURES
Europass
EU Skills Panorama
National and private job portals
Sectoral skills passports
Career guidance
Learning outcome descriptions
EPSO & e-CV
...

Figure 6: ESCO transparency instruments.

Source: European Commission Directorate (2017b, p. 9)

4.1 ESCO & ISCO-08

ISCO-08, developed by the ILO, provides a system for classifying and aggregating occupational information obtained by means of statistical censuses and surveys, as well as from administrative records. It is a four-level hierarchically structured classification that allows occupations to be classified into 436 unit groups.

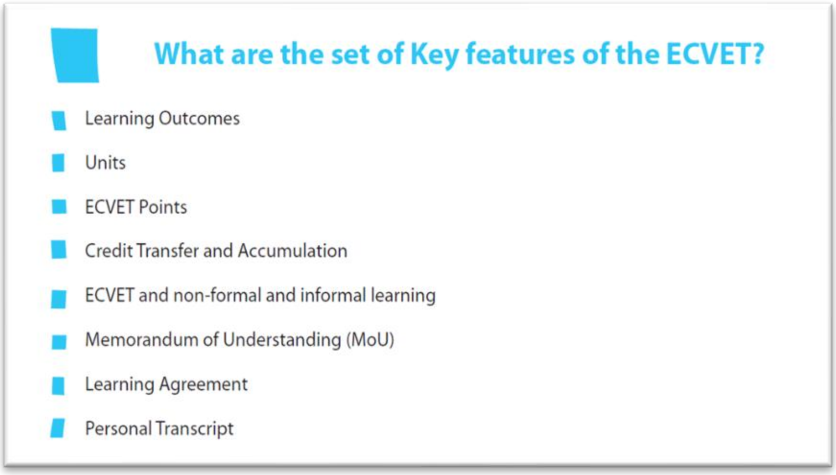
Since each ESCO occupation is mapped to one ISCO-08 unit group, the two classifications are interoperable. This allows ESCO to build on the international acceptance of ISCO. This is particularly important because most national occupational classifications are currently mapped to ISCO-08. This will also make it easier to map27 them to ESCO. Additionally, since ISCO-08 is currently used to enhance the international comparability of statistical data, it makes ESCO an interesting tool to support labour market statistical reporting. (European Commission Directorate 2013, p. 29)

4.2 ECVET – Learning outcomes & Validation

The term ECVET refers to the European Credit System for Vocational Education and Training.

“In simple terms, ECVET is a system which translates learning experiences in VET into units of learning outcomes that build up to a qualification based on ECVET points. This system enhances permeability between education strands as it may be put in parallel to its counterpart ECTS system in Higher Education. The ECVET is a new European instrument for promoting lifelong learning. It should facilitate the recognition and transferability of full vocational qualifications, and awards, or partial vocational qualifications across-borders, hence enhancing and facilitating student mobility across Europe within the VET sector. The whole process is coordinated by tools and a methodological technical framework which should present a systematic way of establishing a common understanding, as well as a user-friendly language for transparency during the transfer and recognition of learning outcomes of study units.”

In the above cited brochure ‘ECVET in Europe’ you will find a definition of each key feature stated above. For our project we will concentrate on the LEARNING OUTCOMES:



What are the set of Key features of the ECVET?

- Learning Outcomes
- Units
- ECVET Points
- Credit Transfer and Accumulation
- ECVET and non-formal and informal learning
- Memorandum of Understanding (MoU)
- Learning Agreement
- Personal Transcript

Figure 7: ECVET in Europe.

Source: Malta Qualifications Council and National Commission for Higher Education (2020, p. 3)

4.3 EQF – European Qualifications Framework

In the context of EQF, knowledge is described as theoretical and/or factual. Skills are described as cognitive (involving the use of logical, intuitive and creative thinking) and practical (involving manual dexterity and the use of methods, materials, tools and instruments). ECVET is, so to speak, the important framework into which EQF and

NQF are embedded via various tools, with the description of learning outcomes being the central point.

The qualifications pillar of ESCO is developed in a way that is consistent with the EQF. This will allow building on the results achieved during the work on the EQF. National qualification databases will be a valuable source for ESCO.

See: https://ec.europa.eu/esco/portal/escopedia/European_Qualifications_Framework__40_EQF_41

This closes the circle on how the EQF can be embedded in this type of meta-systems. But let's take a closer look at the idea of the EQF:

The EQF is a tool for transparency, comparability, and translation that makes it possible to compare and understand the various national qualifications throughout Europe. It covers the entire education and training system, from general and vocational training and continuing education to higher education and non-formal and informal learning. The purpose of the EQF and its classification into eight reference levels is to serve as a reference framework for the education systems of member states for mapping their national qualifications. This framework defines eight levels which aim to cover the entire range of educational qualifications. Every level is defined by 'descriptors'. These descriptors do not refer to aspects such as the training duration, the location of training but to the outcomes of learning processes, that is: what a learner knows understands and is able to do at the end of his/her education or training programme.

See Linking of ECVET – EQF/NQF – Europass: www.ecvet-info.at

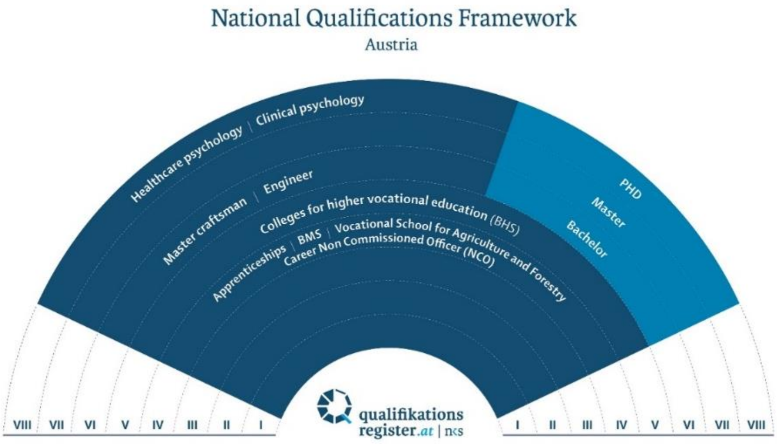

National Qualifications Framework
Austria
Healthcare psychology | Clinical psychology
Master craftsman | Engineer
Colleges for higher vocational education (BHS)
Apprenticeships | BMS | Vocational School for Agriculture and Forestry
Career Non Commissioned Officer (NCO)
PHD
Master
Bachelor
VIII VII VI V IV III II I
I II III IV V VI VII VIII
qualifikations
register.at | nks

Figure 8: Austrian example of the NQR.

"The EQF defines learning outcomes as knowledge, skills and competence. Knowledge is described as theoretical and/or factual. Skills are described as cognitive (involving the use of logical, intuitive and creative thinking) and practical (involving manual dexterity and the use of methods, materials, tools and instruments). In the context of the EQF, competence is described in terms of responsibility and autonomy.

As the level increases, the description of the required knowledge-, skills- and competence-related aspects becomes more and more demanding, comprehensive and complex. Whereas Level 1 is characterised by basic knowledge and skills and a low degree of autonomy and responsibility, Level 8 comprises specialist knowledge, highly specialist skills and a high degree of autonomy and responsibility.”

Linking of ECVET – EQF/NQF – Europass: www.ecvet-info.at

Descriptors defining levels in the European Qualifications Framework (EQF): Each of the 8 levels is defined by a set of descriptors indicating the learning outcomes relevant to qualifications at that level in any system of qualifications. Here you can find the entire table of descriptors:

See European Commission Directorate

The national implementation of the Qualification Framework (mostly called NQR, DQR in Germany) is inevitably complex because they have to be based on social and cultural traditions and the institutions of the respective country. The EQF Recommendation requires that the link between the levels of national qualifications and the levels of the EQF is defined based on learning outcomes. It is widely acknowledged that there is not a common approach in using learning outcomes; however, a common understanding of the main concepts and principles would facilitate the implementation of common European tools such as the EQF, ECVET, and ECTS, which are all based on learning outcomes.

“The European and national level discussions have also highlighted the need for some common ground with respect to learning outcomes so that European level tools (EQF, ECVET, the developing taxonomies of knowledge, skills and competences) can function efficiently. This does not imply that there should be a common approach to defining and using learning outcomes across countries. As explained above, such a restrictive approach would not account for important differences in the ways in which learning can be described within national systems.” (European Commission 2011, p. 8)

See European Commission (2011)

4.4 European-e-Competence-Framework

The European e-Competence Framework (e-CF) is a common European framework for ICT Professionals in all industry sectors. The European e-Competence Framework version 3.0 (CWA 16234) is published in four parts, which may be downloaded free of charge from the CEN website (www.cen.eu) or the e-CF website:

www.ecompetences.eu

The Framework, the User guidelines and sample Case studies are available in English, German, French and Italian versions.

The European e-Competence Framework is a component of the European Union's strategy on «e-Skills for the 21st Century». It is also supporting key policy objectives of the «Grand Coalition for Digital Skills» launched in March 2013. It is promoted as a very useful tool to boost digital skills and the recognition of competences and qualifications across countries and to foster ICT professionalism in Europe. The European ICT Professional Profiles (CWA 16458:2012) is a set of 23 profiles, which may be used for reference or as a starting point to develop further profiles. This document can also be accessed (free of charge) via the CEN website and the e-CF website.

Given the growing importance of Information and Communication Technologies (ICT) in the context of the global economy and the enormous potential of this sector in terms of creating employment, there is a need for a common framework that enables ICT professionals to describe and develop their capabilities, and which also allows companies and employers to identify which individuals possess the skills they require.

e-CF brochure by CEN (European Committee for Standardization), www.cencenelec.eu

The European e-Competence Framework (e-CF) version provides a reference of 40 competences as required and applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills and capability levels that can be understood across Europe. As the first sector-specific implementation of the European Qualifications Framework (EQF), the e-CF is designed to be used by ICT service, user and supply companies, for managers and human resources (HR) departments, for education institutions and training bodies including higher education, for market watchers and policy makers, and other organizations in public and private sectors.

The e-CF was developed through a process of collaboration between experts and stakeholders from many different countries. The current version 3.0 is marked by overall framework maturity and builds upon multiple application experiences in practice.

e-CF brochure by CEN (European Committee for Standardization), www.cencenelec.eu

4.5 DIGCOMP - The Digital Competence Framework

The European Digital Competence Framework, known as DigComp, offers a tool to improve citizen's digital competence. Today, being digitally competent means that people need to have competences in all areas of DigComp.

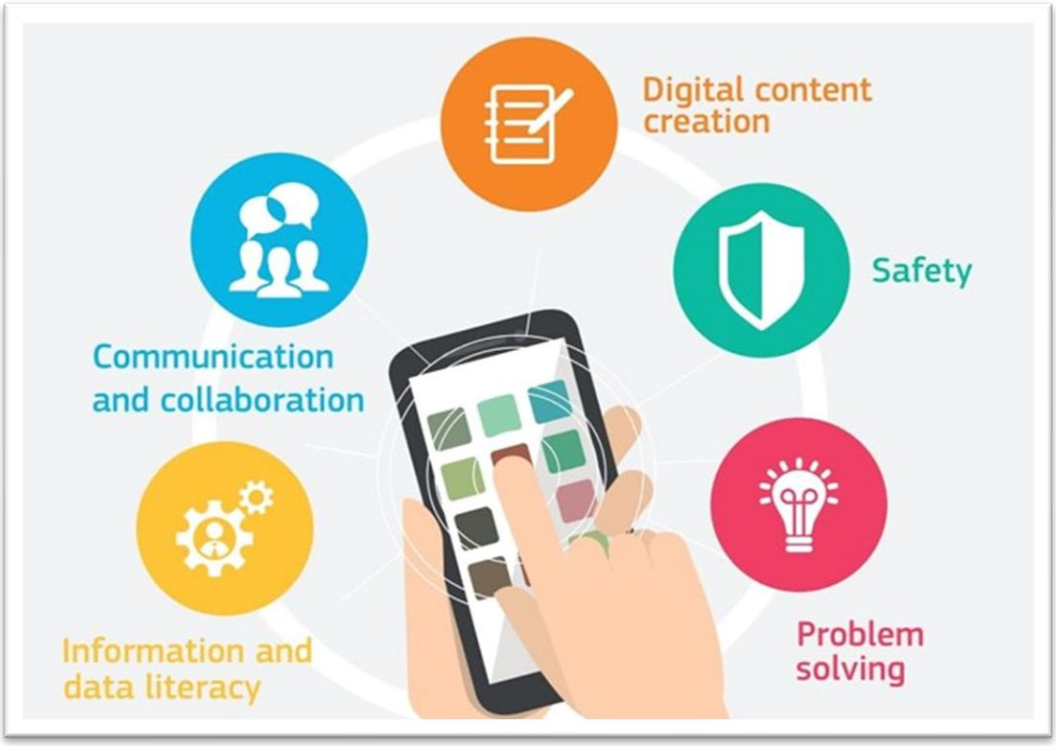

Digital content creation
Communication and collaboration
Safety
Information and data literacy
Problem solving

Figure 9: DigComp into Action.

Source: Publications Office of the European Union (2018)

The Digital Competence Framework helps to monitor citizen's digital skills and to support curricula development.

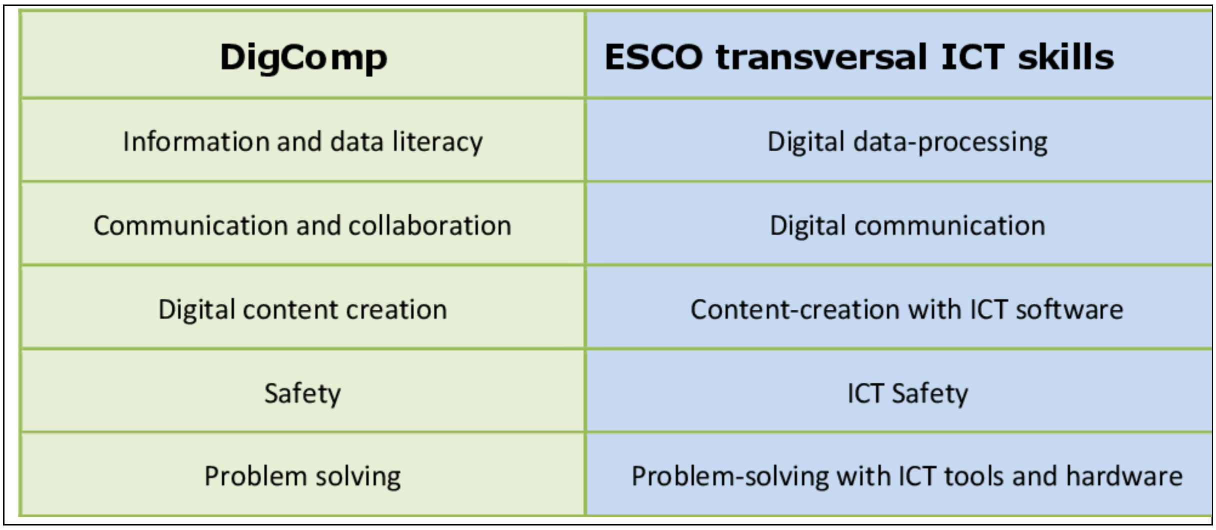
For policymakers it can be beneficial to know where citizens stand for digital competence at the country level. The EU-wide Digital Economy and Society Index (DESI) offers an indicator for Digital Skills that uses the DigComp framework.

The "digital skills" indicator is one part of the many indicators to measure Human Capital which is needed to take advantage of the possibilities offered by a digital society. The Digital Agenda Scoreboard offers an online tool to view the data in an interactive way.

See https://ec.europa.eu/jrc/en/digcomp

DigComp describes which competences are needed today to use digital technologies in a confident, critical, collaborative and creative way to achieve goals related to work, learning, leisure, inclusion and participation in our digital society.

Here is one example of mapping DigComp with ESCO:



DigComp	ESCO transversal ICT skills
Information and data literacy	Digital data-processing
Communication and collaboration	Digital communication
Digital content creation	Content-creation with ICT software
Safety	ICT Safety
Problem solving	Problem-solving with ICT tools and hardware

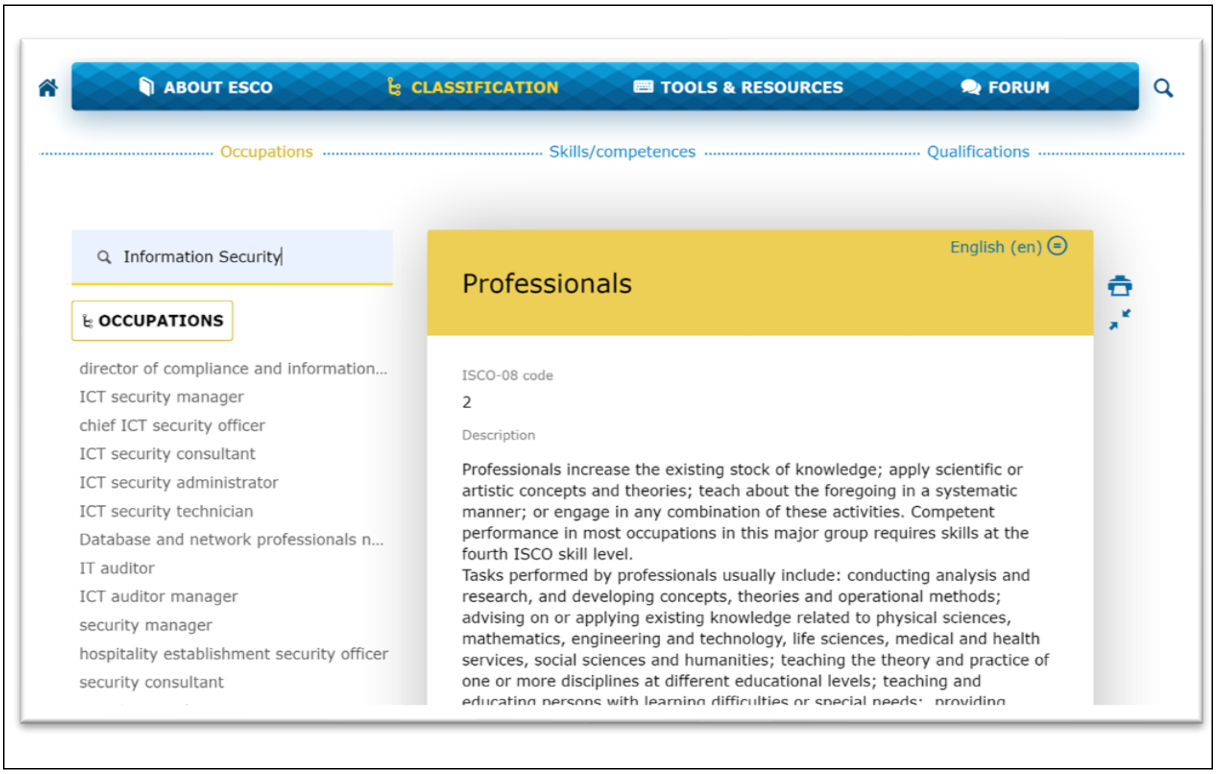
Figure 10: Mapping of the competence areas of DigComp and an ESCO example.

Source: Vuorikari R et al. (2016)

5 ESCO-PROFILES RELEVANT FOR TEBEISI

For the TeBeISi project, we have looked at existing ESCO profiles that come closest to our desired competence profiles. It should be noted that ICT information security is much better covered than data protection.

The ESCO database contains more detailed explanations of all sub profiles and skills. Therefore, use the links below the profiles to gather more detailed information.



Information Security

director of compliance and information...
ICT security manager
chief ICT security officer
ICT security consultant
ICT security administrator
ICT security technician
Database and network professionals n...
IT auditor
ICT auditor manager
security manager
hospitality establishment security officer
security consultant

Professionals

ISCO-08 code

2

Description

Professionals increase the existing stock of knowledge; apply scientific or artistic concepts and theories; teach about the foregoing in a systematic manner; or engage in any combination of these activities. Competent performance in most occupations in this major group requires skills at the fourth ISCO skill level.
Tasks performed by professionals usually include: conducting analysis and research, and developing concepts, theories and operational methods; advising on or applying existing knowledge related to physical sciences, mathematics, engineering and technology, life sciences, medical and health services, social sciences and humanities; teaching the theory and practice of one or more disciplines at different educational levels; teaching and educating persons with learning difficulties or special needs; providing

Figure 11: Screenshot ESCO Portal.

Source: European Commission Directorate 2020fEuropean Commission Directorate (2020f)

5.1 ICT security manager

Description

ICT security managers propose and implement necessary security updates. They advise, support, inform and provide training and security awareness and take direct action on all or part of a network or system.

Alternative label (selection)

- Security coordinator
- ICT technical security expert
- Information security manager

Essential skills and competences

- define security policies
- develop information security strategy
- establish an ICT security prevention plan
- implement ICT risk management
- lead disaster recovery exercises
- maintain ICT identity management
- manage IT security compliances
- manage disaster recovery plans
- solve ICT system problems

Essential Knowledge

- ICT problem management techniques
- ICT project management
- ICT quality policy
- ICT security standards
- ICT system user requirements
- Internet of Things
- computer forensics
- information security strategy
- internal risk management policy
- internet governance
- legal requirements of ICT products

Optional skills and competences

- define technology strategy
- execute ICT audits
- identify ICT security risks
- provide technical documentation

- use ICT ticketing system

Optional Knowledge

- Hybrid model
- ICT encryption
- ICT network security risks
- ICT process quality models
- ICT recovery techniques
- ICT security legislation
- Open source model
- Outsourcing model
- SaaS (service-oriented modelling)
- audit techniques
- cyber-attack counter-measures
- cyber security
- decision support systems
- information confidentiality
- investment analysis
- levels of software testing
- mobile device management
- organisational resilience
- service-oriented modelling
- systems development life-cycle
- tools for ICT test automation
- web application security threats

See European Commission Directorate (2020c)

5.2 ICT security administrator

Description

ICT security administrators plan and carry out security measures to protect information and data from unauthorised access, deliberate attack, theft and corruption.

Alternative label (selection)

- network security administrator
- system security administrator
- ICT security administrators

Essential skills and competences

- apply company policies
- attend to ICT systems quality
- ensure proper document management
- identify ICT system weaknesses
- interpret technical texts
- maintain ICT identity management
- maintain database security
- manage IT security compliances
- perform ICT troubleshooting
- solve ICT system problems

Essential Knowledge

- ICT network security risks
- Internet of Things
- Cyber-attack counter-measures
- database development tools
- internet governance
- mobile device management
- organisational resilience

- quality assurance methodologies
- system backup best practice

Optional skills and competences

- define technology strategy
- execute ICT audits
- identify ICT security risks
- provide technical documentation
- use ICT ticketing system

Optional Knowledge

- Hybrid model
- ICT encryption
- ICT network security risks
- ICT process quality models
- ICT recovery techniques
- ICT security legislation
- Open source model
- Outsourcing model
- SaaS (service-oriented modelling)
- audit techniques
- cyber attack counter-measures
- cyber security
- decision support systems
- information confidentiality
- investment analysis
- levels of software testing
- mobile device management
- organisational resilience
- service-oriented modelling

- systems development life-cycle
- tools for ICT test automation
- web application security threats

See European Commission Directorate (2020b)

5.3 Ethical Hacker

Description

Ethical hackers perform security vulnerability assessments and penetration tests in accordance with industry-accepted methods and protocols. They analyse systems for potential vulnerabilities that may result from improper system configuration, hardware or software flaws, or operational weaknesses.

Alternative label

- vulnerability analyst
- ICT security tester
- system security tester

Essential skills and competences

- address problems critically
- analyse the context of an organisation
- develop code exploits
- execute ICT audits
- execute software tests
- identify ICT security risks
- identify ICT system weaknesses
- monitor system performance
- perform security vulnerability assessments
- provide technical documentation

Essential Knowledge

- computer forensics
- cyber-attack counter-measures

- legal requirements of ICT products
- penetration testing tool
- software anomalies
- tools for ICT test automation
- web application security threats

Optional skills and competences

- define security policies
- maintain ICT server
- manage IT security compliances
- perform project management
- solve ICT system problems

Optional Knowledge

- Hybrid model
- ICT network security risks
- ICT security legislation
- ICT security standards
- Internet of Things
- Nessus
- Nexpose
- Open source model
- SaaS (service-oriented modelling)
- information security strategy
- internet governance

See European Commission Directorate (2020a)

5.4 Policy Manager (Data protection Manager)

The description POLICY MANAGER is the most appropriate match to the TeBelSi concept of a DATA PROTECTION MANAGER in the ESCO-System:

Description

Policy managers are responsible for managing the development of policy programs and ensuring that the strategic objectives of the organization are met. They oversee the production of policy positions, as well as the organization's campaign and advocacy work in fields such as environmental, ethics, quality, transparency, and sustainability.

Alternative label

- policy advocacy manager
- business ethicist
- advocacy coordinator

Essential skills and competences

- advise on efficiency improvements
- develop company strategies
- ensure compliance with policies
- integrate strategic foundation in daily performance
- monitor company policy

Essential Knowledge

- business analysis
- corporate social responsibility
- organisational policies
- strategic planning

Optional skills and competences

- develop organisational policies
- disseminate internal communications

- ensure compliance with company regulations
- ensure compliance with legal requirements
- follow the statutory obligations
- gather feedback from employees
- gather technical information
- get involved in the day-to-day operation of the company
- identify legal requirements
- identify undetected organisational needs
- liaise with government officials
- meet the requirements of legal bodies
- promote organisational communication
- provide improvement strategies
- provide legal advice
- train employees

See European Commission Directorate (2020e)

5.5 ICT security consultant (Data protection Consultant)

The description ICT Security Consultant in the ESCO-System matches with the TeBelSi profiles of Data Protection Manager & Administrator.

Description

ICT security consultants advise and implement solutions to control access to data and programs. They promote a safe exchange of information.

Alternative label

- IT security expert
- ICT security advisor
- ICT security consultants

Essential skills and competences

- define security policies
- develop information security strategy
- educate on data confidentiality
- identify ICT security risks
- identify ICT system weaknesses
- manage IT security compliances
- provide ICT consulting advice
- verify formal ICT specifications

Essential Knowledge

- ICT security legislation
- ICT security standards
- Cyber-attack counter-measures
- Information security strategy
- Organisational resilience

Optional skills and competences

- create project specifications
- ensure proper document management
- give live presentation
- lead disaster recovery exercises
- manage ICT change request process
- manage changes in ICT system
- optimise choice of ICT solution
- perform project management
- provide user documentation
- track key performance indicators

See European Commission Directorate (2020d)

6 REQUIREMENTS IDENTIFIED BY FIELD RESEARCH

6.1 Method of field research

The field research is based on the results of desk research conducted in all partner countries. All staff members who conducted interviews with the experts were familiar with the results of the national findings and were able to adapt the questions to the national characteristics.

In August and September 2019, the partnership interviewed more than 60 experts in the fields of Data protection and Data security, Information security and IT security in small and medium-sized enterprises (SMEs). It was important to us to gather personal opinions and experiences on these topics (either individually or in focus groups).

The aim of our interviews was to gain a deeper insight into the need for SMEs to employ personnel in the field of information security. We have taken a lot of time for the surveys in order to gather as much information as possible - including informal information. This should enable us to find the most comprehensive picture possible of information and data security in everyday professional life.

Some examples of questions are:

- What causes an acute need?
- How acute (in terms of time) is it?
- Which areas and processes are affected by this need?
- Which competences are relevant for the occupational field?
- What strengths and weaknesses do you see in yourself and your employees?
- What problems do you encounter in your daily work environment?
- What tips can you give us for our project?

As was already the case for desk research, national reports were written for field research, which illustrate the country-specific results in detail. An important result of the field research is that at least 10 concrete case studies from practice were documented per country. These cases then formed the basis for the collection of required / desired competences in both fields, Information Security and Data Protection.

BF/M Bayreuth, the coordinating institution of the TeBeISi project started then with a first analysis of expert interviews and provided us with a cloud, which aggregates the list of coding and creates a word cloud, with larger printed codes according to the amount of times the code has been mentioned. Here we can, thanks to BF/M Bayreuth, already present a preliminary version (see below).

In the next step we created four - so to speak fictitious - Job Profiles to match them with already existing ESCO Profiles. This resulted in a kind of catalogue of requirements, which should make it easier for us to find a clearer Job Profile that can be adapted to the possibilities of SME. Of course, small and medium-sized companies do not have the possibilities to create four jobs in the areas of information security and data protection. In any case, we will always refer back to this catalogue of competencies for further processing in IO3 and IO4.

Finally, in this report we present the preliminary job profile of a "DP-IS Officer in SMEs". This profile is an attempt to enumerate and classify the most important competences. This profile is also still too detailed and vague in its present form, but it forms the basis for further processing in IO3. The next steps are described in a concluding point at the end of this report.

In summary, it can be said that we have so far laid the foundations to work on a clear job profile, to have the right methods how to describe learning outcomes for the curriculum and all partners are informed on the possibilities of certification processes on EU level.

6.2 Participants of field research

All experts who participated in this interview session signed a Privacy policy and a Declaration of consent. They also had the possibility to choose whether their interview should be recorded or not. All interviews are anonymous. To be able to identify which interview belongs to which protocol-file and which country we used the code “Candidate_No_Country” (e.g. Candidate_01_AT) for “ID”.

ID DE	INTERVIEW PARTNER FROM SECTOR	PROFESSIONAL FIELD OF INFORMATION SECURITY
Candidate_1_DE	Energy (CRITIS)	CISO
Candidate_2_DE	IT Services (SME)	Managing Director
Candidate_3_DE	IT Services (SME)	Senior HR Manager
Candidate_4_DE	IT Services (SME)	Managing Director
Candidate_5_DE	IT Services (SME)	Managing Director
Candidate_6_DE	Textile Supplier (SME)	CISO

Candidate_7_DE	Telecommunication (CRITIS)	Procurement
Candidate_8_DE	Manufacturing	CISO
Candidate_9_DE	Service and Consulting	Managing Director
FG_1_DE	IT Start-ups (6 SMEs)	CEOs
FG_2_DE	IT Services (5 SMEs and 1 CRITIS, 2 Ltd)	CEOs, Consultants, ISOs
ID IT	**INTERVIEW PARTNER FROM SECTOR**	**PROFESSIONAL FIELD OF INFORMATION SECURITY**
Candidate_01_IT	Company services	Job consultant and lawyer
Candidate_02_IT	Company services	Consultant and DPO
Candidate_03_IT	IT services	Software Developer, IT- & Data Security
Candidate_04_IT	IT services	Software Developer, IT- & Data Security
Candidate_05_IT	Entrepreneur in IT sector	Managing Director
Candidate_06_IT	Public body (elderly care centre)	IT- & Data Security manager
Candidate_07_IT	IT services	Software Developer, IT- & Data Security
Candidate_08_IT	Regional VET centre	IT security manager
Candidate_09_IT	Regional VET centre	Data protection manager
Candidate_10_IT	Company services	Consultant and DPO
Candidate_11_IT	IT services	Software Developer, IT- & Data Security
Candidate_12_IT	IT services	Software Developer, IT- & Data Security
Candidate_13_IT	Management consultant	Software Developer
Candidate_14_IT	IT services / platforms company	Software Developer, IT- & Data Security
Candidate_15_IT	IT services	Software Developer, IT- & Data Security
Candidate_16_IT	IT services / networks	Software Developer, IT- & Data Security
Candidate_17_IT	Micro SMEs association	IT security manager

Candidate_18_IT	Company services	Consultant and DPO
Candidate_19_IT	Business competences centre	IT security manager

ID LT	INTERVIEW PARTNER FROM SECTOR	PROFESSIONAL FIELD OF INFORMATION SECURITY
Focus group_01_LT		
Candidate_01_LT	Social services institutions	Data Protection Officer
Candidate_02_LT	Social services institutions	Data Protection Officer
Candidate_03_LT	Social services institutions	Lawyer / Data Protection Officer
Candidate_04_LT	Social services institutions	Data Protection Officer
Candidate_06_LT	Social services institutions	Data Protection Officer
Focus group_02_LT		
Candidate_01_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_02_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_03_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_04_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_05_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_06_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_07_LT	Small and medium-sized business representatives	IT & Data Security
Candidate_08_LT	Small and medium-sized business representatives	IT & Data Security
Interview Candidate_01_LT	High education Institution	Data Protection Officer
Interview Candidate_02_LT	The company specializes in personal data protection	Data Protection Officer
Interview Candidate_03_LT	Advisory service	Consultant IT & Data Security
Interview Candidate_04_LT	High education Institution	Researcher, Associated professor, PhD in law, expert in privacy and data protection.

ID AT	**INTERVIEW PARTNER FROM SECTOR**	**PROFESSIONAL FIELD OF INFORMATION SECURITY**
Candidate_01_AT	IC-Technology (CRITIS)	Software Developer, IT- & Data Security
Candidate_02_AT	Transportation Systems (CRITIS)	Software Developer, IT- & Data Security
Candidate_03_AT	IC-Technology (CRITIS)	Product Manager, IT-Security
Candidate_04_AT	Gouvernement &Admin (CRITIS)	Office Manager, Data Security
Candidate_05_AT	IC-Technology (CRITIS)	Quality Manager, Data Security
Candidate_06_AT	IC-Technology (CRITIS)	Business Analyst, IT-Security
Candidate_07_AT	Tourism	Managing Director, Data Security
Candidate_08_AT	Graphic Design & Eventmgmt.	Managing Director, Data Security
Candidate_09_AT	Dry-cleaning company	Product Manager, Data Security
Candidate_10_AT	IC-Technology (CRITIS)	Managing Director, IT- & Data Security
ID PL	**INTERVIEW PARTNER FROM SECTOR**	**PROFESSIONAL FIELD OF INFORMATION SECURITY**
Candidate_01_POL	Transportation (CRITIS)	Data Protection Inspector, Data Security
Candidate_02_POL	Healthcare (CRITIS)	Information security inspector, IT- & Data Security
Candidate_03_POL	Financial Services (CRITIS)	Data protection specialist, Data Security
Candidate_04_POL	IC-Technology (CRITIS)	Senior Coordinator for IT- & Data Security
Candidate_05_POL	Financial Services (CRITIS)	IT security expert at the Department of Security, IT- & Data Security
Candidate_06_POL	Production	A specialist in creating policies and standards for IS/DS
Candidate_07_POL	Government & Administration (CRITIS)	Inspector at the Organization Department IT- & Data Security
Candidate_08_POL	Logistics (CRITIS)	Information Security Specialist, Data Security
Candidate_09_POL	Education	Dean of the faculty at the university, Data Security
Candidate_10_POL	Financial Services (CRITIS)	Information security specialist, Data Security

Table 1: Interview Candidates from the partner Countries

6.3 Cases collected from our field research

An important result of the field research is that at least 10 concrete case studies from practice were documented per country. These cases then formed the basis for the collection of required / desired competences in both fields, Information Security and Data Protection.

A list of all cases can be found as an appendix to this report. Here we only briefly summarize the main findings. Main outcomes from expert interviews in the field research:

Main outcomes from DE:

There are two key findings which can be highlighted: on the one hand, WORKING EXPERIENCE and a set of social skills are highly appreciated by all respondents. On the other hand, tasks of AWARENESS CREATION have been found to be particularly important.

- There was a general agreement that Information Security will play an increasingly important role in the upcoming years (even more than data protection), and that the labour market forces companies to react
- The current need can be attributed to legal and technical developments. Companies are anticipating this upcoming need; however, SME don't possess the resources required to cover the need themselves, which is why a growing market for consulting services tries to meet these demands.
- Information Security is not covered by SME, as roles cannot be viably filled. Instead, services are being purchased from third party providers.
- Due to the scarcity in labour supply, firms publish job offers with vary vague requirements, in the hope to find suitable personnel via direct communication (i.e. getting to know their social skills).
- Hands-on experience has been found to be equally or even more important than a formal qualification. Next to social skills, certificates are often seen as a useful tool to signal knowledge and to verify working experience.

Main outcomes from AT:

One result is anticipated: It is interesting that all respondents, however different the cases may be, named AWARENESS RISING as a core task.

- All respondents agree that IT security and data security as well as data protection will become even more important in the coming years. Therefore, an increasing number of well-trained employees will be needed.
- One difference has emerged from the questionnaires: While medium-sized companies become active themselves and train their employees in both areas, small companies are increasingly interested in finding external partners to help them find suitable training.
- One problem that in turn affects small businesses is that they feel overwhelmed by the legal requirements. While medium-sized companies bring legal experts into the company, this is usually not possible for them.
- It is obvious that larger companies are better equipped with guidelines and experts than smaller companies. Nevertheless, they obviously share the problem that employees must first be persuaded to abide by the rules.

Main outcomes from PL:

All companies interviewed have their own information security management strategy, but it is not always implemented. Employees' often desired skill in the area of information security is FLEXIBILITY, OPENNESS TO CHANGES AND WILLINGNESS TO LEARN.

- 8 of our 10 interviewees work in a CRITIS related domain.
- This means that they typically have to comply with stricter requirements in terms of both IT security and data protection.
- Information security is important in every area, only from different perspectives.
- Not all employees are aware of the risks and dangers in the event of non-compliance with information security principles.
- In most cases, trainings are organized, but most often they are internal trainings, without certificates.
- Often, employees emphasize that formal education is less important than professional experience in the area of IT and information security.
- In the area of administration, there is an overlap of employee competences,

which causes a crisis in the area of information security - employees have too many responsibilities and do not always reliably fulfil them.

- Verification of learning outcomes usually occurs when performing specific tasks in the area of information security.

As can be seen in the case studies of IT and LT (see annex), the current situation is very similar to the above examples and therefore the points are no longer listed individually.

6.4 First analysis of expert interviews

BF/M Bayreuth, the coordinating institution of the TeBeISi project started with the analysis of expert interviews via a “list of coding”, a tool which is used to qualitatively analyse the interviews. Every code represents a statement by an expert, making it possible to allow the quantification of statements made and at the same time to conduct further analysis, like inter-country comparisons. Currently, the list consists of 480 codes, whereby the coding of the interviews is not yet complete, and the final output will be presented at a later stage within IO3.

This cloud aggregates the list of coding and creates a word cloud, with larger printed codes according to the amount of times the code has been mentioned. Here we can, thanks to BF/M Bayreuth, already present a preliminary version.

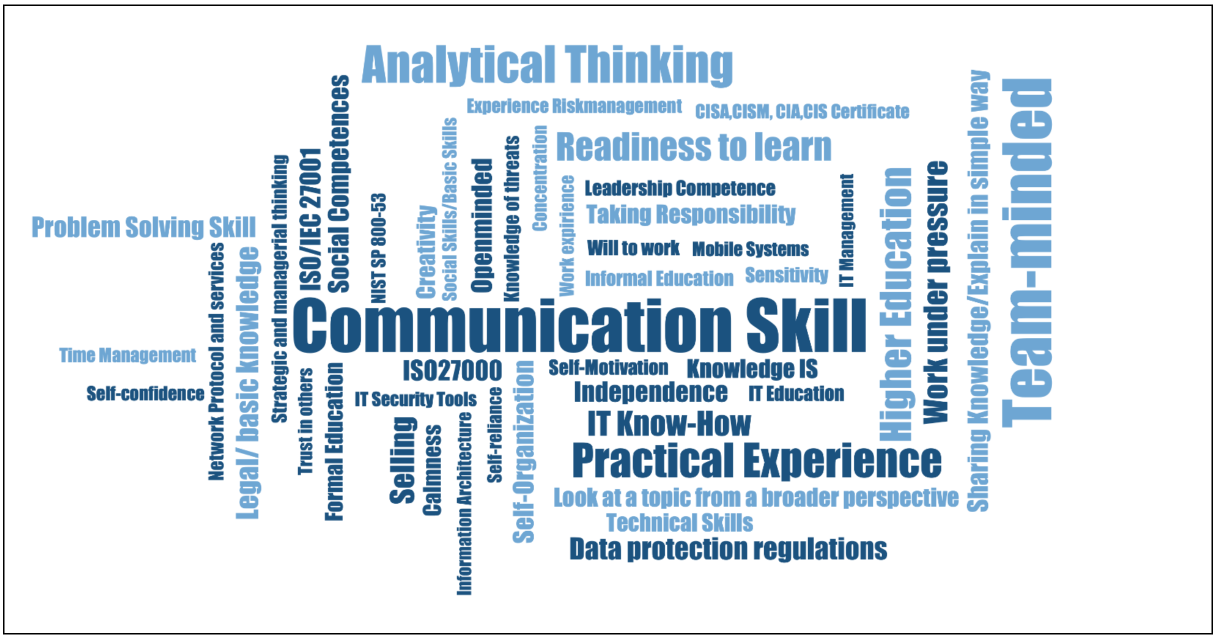


Figure 12: Preliminary version of word cloud from Simon Rath from BF/M Bayreuth (Coordinator of the TeBeISi project) – final version to be presented in IO3

7 TEBEISI REQUIREMENTS MATCHED WITH ESCO PROFILES

In the section below we present our first mapping of our outcomes with the ESCO profiles. We indicated in the last two rows which inputs come from ESCO profiles and which inputs we gathered from the project so far (interviews with experts, cases & desk research).

As a next step we created four - so to speak fictitious - Job Profiles to match them with already existing ESCO Profiles. This resulted in a kind of CATALOGUE OF REQUIREMENTS, which should make it easier for us to find one clear Job Profile that can be adapted to the possibilities of SME. Of course, small and medium-sized companies do not have the possibilities to create four jobs in the areas of information security and data protection. In any case, we will always refer back to this sort of catalogue of requirements for further processing in IO3 and IO4.

We did this first mapping with four fictitious profiles as indicated on the next page

7.1 Information Security Manager (strategic and operational level)

Description

ICT security managers propose and implement necessary security measures. They advise, support, inform and provide training and security awareness and take direct action on all or part of a network or system.

	ESCO matched with TeBelSi profile	Description (based on ESCO & adapted to TeBelSi needs)	ESCO input	TeBelSi input
I.	**ESSENTIAL FIELDS OF KNOWLEDGE**			
	ICT project management	The methodologies for the planning, implementation, review and follow-up of ICT projects, such as the development, integration, modification and sales of ICT products and services, as well as projects relating technological innovation in the field of ICT.	X	X
	ICT quality policy	The quality policy of the organisation and its objectives, the acceptable level of quality and the techniques to measure it, its legal aspects and the duties of specific departments to ensure quality.	X	X
	ICT problem management techniques	The techniques related to identifying the solutions of the root cause of ICT incidents.	X	X
	ICT security standards	The standards regarding ICT security such as ISO and the techniques required to ensure compliance of the organisation with them.	X	X
	Internet of Things (IoT)	The general principles, categories, requirements, limitations and vulnerabilities of smart connected devices (most of them with intended internet connectivity).	X	

	Computer forensics	The process of examining and recovering digital data from sources for legal evidence and crime investigation.	X	
	Information Security Strategy	The plan defined by a company which sets the information security objectives and measures to mitigate risks, define control objectives, establish metrics and benchmarks while complying with legal, internal and contractual requirements.	X	X
	Internet governance	The principles, regulations, norms and programs that shape the evolution and use of internet, such as internet domain names management, registries and registrars, according to ICANN/IANA regulations and recommendations, IP addresses and names, name servers, DNS, TLDs and aspects of IDNs and DNSSEC.	X	X
	Internal risk management policy	The process of examining and recovering digital data from sources for legal evidence and crime investigation.	X	
	ICT security legislation	The set of legislative rules that safeguards information technology, ICT networks and computer systems and legal consequences which result from their misuse. Regulated measures include firewalls, intrusion detection, anti-virus software and encryption. (Some specific rules come from GDPR legislation!)	X	X
	Organisational resilience	The strategies, methods and techniques that increase the organisation's capacity to protect and sustain the services and operations that fulfil the organisational mission and create lasting values by effectively addressing the combined issues of security, preparedness, risk and disaster recovery.	X	X
	Quality assurance methodologies	Quality assurance principles, standard requirements, and the set of processes and activities used for measuring, controlling and ensuring the quality of products and processes. ISO / UNI standards could help these processes.	X	X
	Information security policy	A prosperous enterprise cannot afford the loss or unauthorized disclosure of confidential data, which is why securing data storage or information	X	X

		processing is becoming an extremely important activity undertaken by companies and public institutions.		
	Cloud Technologies	The technologies which enable access to hardware, software, data and services through remote servers and software networks irrespective of their location and architecture.	X	X
	Business Continuity Management	BCM is a framework for identifying an organization's risk of exposure to internal and external threats. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.		X
	Assertiveness	The attitude to stand up for yourself and be treated with respect without upsetting others, being aggressive, rude or submissive.	X	X
	Sales argumentation	Techniques and sales methods used in order to present a product or service to customers in a persuasive manner and to meet their expectations and needs.	X	X
	Systems thinking	The integrated approach to understanding how various constituents of a system interrelate, interact and influence one another within a whole logistic system.	X	X
II.	**Professional Skills & Competences: You need to know how to**			
	▪ define security policies	Design and execute a written set of rules and policies that have the aim of securing an organisation concerning constraints on behaviour between stakeholders, protective mechanical constraints and data-access constraints.	X	X
	▪ develop information security strategy	Create company strategy related to the safety and security of information in order to maximise information integrity, availability and data privacy.	X	X

	▪ establish an ICT security prevention plan	Define a set of measures and responsibilities to ensure the confidentiality, integrity and availability of information. Implement policies to prevent data breaches, detect and respond to unauthorised access to systems and resources, including up-to-date security applications and employee education.	X	
	▪ implement ICT risk management	Develop and implement procedures for identifying, assessing, treating and mitigating ICT risks, such as hacks or data leaks, according to the company's risk strategy, procedures and policies. Analyse and manage security risks and incidents. Recommend measures to improve digital security strategy. In that case, i.e. ISO 9001 (or similar) standard could strongly help the implementation process.	X	X
	▪ maintain ICT identity management	Administer identification, authentication and authorisation of individuals within a system and control their access to resources by associating user rights and restrictions with the established identity.	X	
	▪ manage IT security compliances	Guide application and fulfilment of relevant industry standards, best practices and legal requirements for information security.	X	X
	▪ manage disaster recovery plans	Prepare, test and execute, when necessary, a plan of action to retrieve or compensate lost information system data.	X	X
	▪ solve ICT system problems	Identify potential component malfunctions. Monitor, document and communicate about incidents. Deploy appropriate resources with minimal outage and deploy appropriate diagnostic tools.	X	X
	▪ lead disaster recovery exercises	Head exercises which educate people on what to do in case of an unforeseen disastrous event in the functioning or security of ICT systems, such as on recovery of data, protection of identity and information and which steps to take in order to prevent further problems.	X	

	▪ train employees (= awareness rising measure)	Lead and guide employees through a process in which they are taught the necessary skills for the perspective job. Organise activities aimed at introducing the work and systems or improving the performance of individuals and groups in organisational settings.	X	X
	▪ define technology strategy	Create an overall plan of objectives, practices, principles and tactics related to the use of technologies within an organisation and describe the means to reach the objectives.	X	
	▪ execute ICT audits	Organise and execute audits in order to evaluate ICT systems, compliance of components of systems, information processing systems and information security. Identify and collect potential critical issues and recommend solutions based on required standards and solutions.	X	
	• cyclical training	Training is a program that helps employees learn specific knowledge or skills to improve performance in their current roles. Development is more expansive and focuses on employee growth and future performance, rather than an immediate job role.	X	X
	• analytical and logical thinking skills	Analytical thinking is about breaking down problems logically, into small bites and without emotions. People with strong analytical skills will find a well-thought-out solution in any situation, based on information and facts.	X	X
	• drawing conclusions from mistakes made	This is important for the continuous improvement of related processes.	X	X
	▪ ability to work under time pressure	The ability to work under pressure involves dealing with constraints which are often outside of your control - these might be resource or time constraints, the difficulty of the task or having insufficient knowledge required to complete the task, or unforeseen changes or problems.		X

	▪ maintain ICT identity management	Administer identification, authentication and authorisation of individuals within a system and control their access to resources by associating user rights and restrictions with the established identity.	X	X
	▪ perform risk analysis	Identify and assess factors that may jeopardise the success of a project or threaten the organisation's functioning. Implement procedures to avoid or minimise their impact.	X	X
	▪ manage processes	Manage processes by defining, measuring, controlling and improving processes with the goal to meet customer requirements profitably.	X	X
	▪ think analytically	Produce thoughts using logic and reasoning in order to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.	X	X
	▪ broker ideas to Executive Management	Defend new investments into security assets against budget cuts and intends to spend less money for fewer capabilities.		X
III.	**Social Competences: You should be able to**			
	▪ address problems critically	Identify the strengths and weaknesses of various abstract, rational concepts, such as issues, opinions, and approaches related to a specific problematic situation in order to formulate solutions and alternative methods of tackling the situation.	X	X
	▪ raise awareness on Information Security	Intervene and implement programs or activities that raise awareness of issues relevant for the respective company or clients regarding Information Security measures.		X
	▪ be aware of the risk people might cause	It is helpful to anticipate possible errors as much as possible. Of course, this is not always possible. This setting helps: You learn from mistakes.		X

	▪ motivate yourself and others	Motivate staff to take information security more seriously. Sometimes it might help to do that humorously…		X
	▪ do not fear change	The acceptance to get involved in change and to adapt to new situations is important for you and your employees.		X
	▪ communicate clearly	Speak clearly in addressing employees or clients; communicate information related to their knowledge and be aware of the fact, that not everybody is an expert in Information Security.		X
	▪ exercise patience	Have patience by dealing with unexpected actions from your employees or customers. Not everybody has your background of knowledge.	X	X
	▪ openness to changes	Openness to change refers to an individual's level of acceptance and conscious awareness of the possibility that change may be needed across a range of situations and scenarios, together with the appetite or drive to enact that change.		X
	▪ have good time-management	A fundamental part of time management is planning. Being efficient in planning out your day, meetings and how you will accomplish things will help you stick to your schedule.		X
	▪ work in a group	Whatever form the group work takes, the opportunity to work with others, rather than on your own, can provide distinct benefits: increased productivity and performance, skills development and knowing more about yourself.		X
	▪ demonstrate willingness to learn	Show a positive attitude towards new and challenging demands that can only be met via lifelong learning.	X	X
	▪ focus on service	Actively look for efficient ways to help people.	X	X
	▪ relate empathetically	Recognise, understand and share emotions and insights experienced by another.	X	X

	▪ react calmly in stressful situations	React quickly, calmly, and safely to unexpected situations; provide a solution that solves the problem or diminishes its impact.	X	X
	▪ manage emergency procedures	React quickly in case of emergency and set planned emergency procedures in motion.	X	X

Table 2: Mapping of Information Security Manager (strategic and operational level)

7.2 Information Security Administrator (operational level)

Description

The Information Security Administrators plan and carry out security measures to protect information and data from unauthorized access, deliberate attack, theft and corruption.

	ESCO matched with TeBelSi profile	Description (based on ESCO & adapted to TeBelSi needs)	ESCO input	TeBelSi input
I.	**ESSENTIAL FIELDS OF KNOWLEDGE**			
	ICT network security risks	The security risk factors, such as hardware and software components, devices, interfaces and policies in ICT networks, risk assessment techniques that can be applied to assess the severity and the consequences of security threats and contingency plans for each security risk factor.	X	X
	Internet of Things (IoT)	The general principles, categories, requirements, limitations and vulnerabilities of smart connected devices (most of them with intended internet connectivity).	X	

	Cyber-attack counter-measures	The strategies, techniques and tools that can be used to detect and avert malicious attacks against organisations' information systems, infrastructures or networks. The awareness level of workers and employer is fundamental.	X	X
	Internet governance	The principles, regulations, norms and programs that shape the evolution and use of internet, such as internet domain names management, registries and registrars, according to ICANN/IANA regulations and recommendations, IP addresses and names, name servers, DNS, TLDs and aspects of IDNs and DNSSEC.	X	X
	Organisational resilience	The strategies, methods and techniques that increase the organisation's capacity to protect and sustain the services and operations that fulfil the organisational mission and create lasting values by effectively addressing the combined issues of security, preparedness, risk and disaster recovery. It is also a matter of motivation and responsibility inside the organisations.	X	X
	Quality assurance methodologies	Quality assurance principles, standard requirements, and the set of processes and activities used for measuring, controlling and ensuring the quality of products and processes.	X	X
	System backup best practice	The procedures related to preparing for recovery or continuation of technology infrastructure vital to an organisation.	X	X
	Information Security Strategy	The plan defined by a company which sets the information security objectives and measures to mitigate risks, define control objectives, establish metrics and benchmarks while complying with legal, internal and contractual requirements.	X	X
	ICT security legislation	The set of legislative rules that safeguards information technology, ICT networks and computer systems and legal consequences which result	X	X

		from their misuse. Regulated measures include firewalls, intrusion detection, anti-virus software and encryption. See also GDPR contents and rules.		
	Information security policy	A prosperous enterprise cannot afford the loss or unauthorized disclosure of confidential data, which is why securing data storage or information processing is becoming an extremely important activity undertaken by companies and public institutions.	X	X
	Cloud Technologies	The technologies which enable access to hardware, software, data and services through remote servers and software networks irrespective of their location and architecture.	X	X
	Business Continuity Management	BCM is a framework for identifying an organization's risk of exposure to internal and external threats. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.		X
	Systems thinking	The integrated approach to understanding how various constituents of a system interrelate, interact and influence one another within a whole logistic system.	X	X
II.	**Professional Skills & Competences: You need to know how to**			
	▪ apply company policies	Apply the principles and rules that govern the activities and processes of an organisation.	X	X
	▪ attend to ICT systems quality	Ensure correct operations which comply fully with specific needs and outcomes in terms of the development, integration, security and overall management of ICT systems.	X	X

	▪ identify ICT system weaknesses	Analyse the system and network architecture, hardware and software components and data in order to identify weaknesses and vulnerability to intrusions or attacks.	X	X
	▪ maintain database security	Master a wide variety of information security controls in order to pursue maximal database protection.	X	
	▪ manage IT security compliances	Guide application and fulfilment of relevant industry standards, best practices and legal requirements for information security.	X	X
	▪ perform ICT troubleshooting	Identify problems with servers, desktops, printers, networks, and remote access, and perform actions which solve the problems.	X	X
	▪ solve ICT system problems	Identify potential component malfunctions. Monitor, document and communicate about incidents. Deploy appropriate resources with minimal outage and deploy appropriate diagnostic tools.	X	X
	▪ lead disaster recovery exercises	Head exercises which educate people on what to do in case of an unforeseen disastrous event in the functioning or security of ICT systems, such as on recovery of data, protection of identity and information and which steps to take in order to prevent further problems.	X	
	▪ train employees (= awareness rising measure)	Lead and guide employees through a process in which they are taught the necessary skills for the perspective job. Organise activities aimed at introducing the work and systems or improving the performance of individuals and groups in organisational settings.	X	X
	• cyclical training	Training is a program that helps employees learn specific knowledge or skills to improve performance in their current roles. Development is more expansive and focuses on employee growth and future performance, rather than an immediate job role.	X	X

	• analytical and logical thinking skills	Analytical thinking is about breaking down problems logically, into small bites and without emotions. People with strong analytical skills will find a well-thought-out solution in any situation, based on information and facts.	X	X
	• drawing conclusions from mistakes made	This is important for the continuous improvement of related processes.	X	X
	▪ ability to work under time pressure	The ability to work under pressure involves dealing with constraints which are often outside of your control - these might be resource or time constraints, the difficulty of the task or having insufficient knowledge required to complete the task, or unforeseen changes or problems.		X
	▪ maintain ICT identity management	Administer identification, authentication and authorisation of individuals within a system and control their access to resources by associating user rights and restrictions with the established identity.	X	X
	▪ perform risk analysis	Identify and assess factors that may jeopardise the success of a project or threaten the organisation's functioning. Implement procedures to avoid or minimise their impact.	X	X
	▪ manage processes	Manage processes by defining, measuring, controlling and improving processes with the goal to meet customer requirements profitably.	X	X
	▪ think analytically	Produce thoughts using logic and reasoning in order to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.	X	X
III.	**Social Competences: You should be able to**			
	▪ address problems critically	Identify the strengths and weaknesses of various abstract, rational concepts, such as issues, opinions, and approaches related to a specific	X	X

		problematic situation in order to formulate solutions and alternative methods of tackling the situation.		
	▪ raise awareness on Information Security	Intervene and implement programs or activities that raise awareness of issues relevant for the respective company or clients regarding Information Security measures.		X
	▪ be aware of the risk people might cause	It is helpful to anticipate possible errors as much as possible. Of course, this is not always possible. This setting helps: You learn from mistakes.		X
	▪ motivate yourself and others	Motivate staff to take information security more seriously. Sometimes it might help to do that humorously…		X
	▪ do not fear change	The acceptance to get involved in change and to adapt to new situations is important for you and your employees.		X
	▪ communicate clearly	Speak clearly in addressing employees or clients; communicate information related to their knowledge and be aware of the fact, that not everybody is an expert in Information Security.		X
	▪ exercise patience	Have patience by dealing with unexpected actions from your employees or customers. Not everybody has your background of knowledge.	X	X
	▪ openness to changes	Openness to change refers to an individual's level of acceptance and conscious awareness of the possibility that change may be needed across a range of situations and scenarios, together with the appetite or drive to enact that change.		X
	▪ have good time-management	A fundamental part of time management is planning. Being efficient in planning out your day, meetings and how you will accomplish things will help you stick to your schedule.		X

	▪ work in a group	Whatever form the group work takes, the opportunity to work with others, rather than on your own, can provide distinct benefits: increased productivity and performance, skills development and knowing more about yourself.		X
	▪ demonstrate willingness to learn	Show a positive attitude towards new and challenging demands that can only be met via lifelong learning.	X	X
	▪ focus on service	Actively look for efficient ways to help people.	X	X
	▪ relate empathetically	Recognise, understand and share emotions and insights experienced by another.	X	X
	▪ react calmly in stressful situations	React quickly, calmly, and safely to unexpected situations; provide a solution that solves the problem or diminishes its impact.	X	X
	▪ manage emergency procedures	React quickly in case of emergency and set planned emergency procedures in motion.	X	X

Table 3: Mapping of Information Security Administrator (operational level)

7.3 Data Protection Manager (strategic and operational level)

Description

Data protection managers are responsible for managing the development of policy programs and ensuring that the strategic objectives of the organization are met. They oversee the production of policy positions, as well as the organization's campaign and advocacy work in fields of data protection / privacy.

	ESCO matched with TeBelSi profile	Description (based on ESCO & adapted to TeBelSi needs)	ESCO input	TeBelSi input
I.	**ESSENTIAL FIELDS OF KNOWLEDGE**			
	Business analysis	The research field which addresses the identification of business needs and problems and the determination of the solutions that would mitigate or prevent the smooth functioning of a business. Business analysis comprises IT solutions, market challenges, policy development and strategic matters, with strong focus on Data Protection measures.	X	
	Corporate social responsibility	The handling or managing of business processes in a responsible and ethical manner considering the economic responsibility towards shareholders as equally important as the responsibility towards environmental and social stakeholders, focussed on privacy themes. E.g. in Italy, CSR level of awareness is strongly increasing which permits a better overall business processes managing.	X	X
	Organisational policies	The policies to achieve set of goals and targets regarding the development and maintenance of an organisation.	X	X

	Organisational resilience	The strategies, methods and techniques that increase the organisation's capacity to protect and sustain the services and operations that fulfil the organisational mission and create lasting values by effectively addressing the combined issues of security, preparedness, risk and disaster recovery.	X	X
	Information Security Strategy	The plan defined by a company which sets the information security objectives and measures to mitigate risks, define control objectives, establish metrics and benchmarks while complying with legal, internal and contractual requirements.	X	X
	ICT security legislation	The set of legislative rules that safeguards information technology, ICT networks and computer systems and legal consequences which result from their misuse. Regulated measures include firewalls, intrusion detection, anti-virus software and encryption. See also GDPR contents and rules.	X	X
	Anonymization of data	It means the transformation of personal data, after which it is no longer possible to assign individual personal or material information to a specific or identifiable natural person or it can be done only with a disproportionate expenditure of time, costs and forces.		X
	Audit	Systematic and independent assessment of a given organization, system, process, project or product. The subject of the audit is examined for compliance with a specific reference point - checklist, legal provisions, norms, standards or internal regulations of a given organization (policies, procedures).		X
	Cloud Technologies	The technologies which enable access to hardware, software, data and services through remote servers and software networks irrespective of their location and architecture.	X	X

	Business Continuity Management	BCM is a framework for identifying an organization's risk of exposure to internal and external threats. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.		X
II.	**Professional Skills & Competences: You need to know how to**			
	▪ apply company policies	Apply the principles and rules that govern the activities and processes of an organisation regarding data privacy.	X	X
	▪ attend to ICT systems quality	Ensure correct operations which comply fully with specific needs and outcomes in terms of the development, integration, security and overall management of privacy measures.	X	X
	▪ ensure compliance with policies	To ensure compliance with legislation and company procedures in respect of data protection in the workplace and public areas, at all times. To ensure awareness of and compliance with all Company Policies in relation to privacy in the workplace.	X	
	▪ monitor company policy	Monitor the company's policy and propose improvements to the company with strong focus on privacy / data protection. I.e. an external consultant could monitor and assess, periodically, these aspects.	X	X
	▪ develop organisational policies	Develop and supervise the implementation of policies aimed at documenting and detailing the procedures for the operations of the organisation in the lights of privacy / data protection measures.	X	X

	▪ ensure compliance with company regulations	Guarantee that employees' activities follow company regulations, as implemented through client and corporate guidelines, directives, policies and programmes with focus on privacy.	X	X
	▪ ensure compliance with legal requirements	Guarantee compliance with established and applicable standards and legal requirements such as specifications, policies, standards or law regarding data protection and privacy.	X	X
	▪ follow the statutory obligations	Understand, abide by, and apply the statutory obligations of the company in the daily performance of the job.	X	X
	▪ get involved in the day-to-day operation of the company	Collaborate and perform hands-on work with other departments, managers, supervisors, and workers in different aspects of the business in order to raise awareness for data protection.	X	X
	▪ identify legal requirements	Conduct research for applicable legal and normative procedures and standards, analyse and derive legal requirements that apply to the organisation, its policies and products.	X	X
	▪ liaise with government officials	Consult and cooperate with government officials who handle matter that is relevant to privacy / data security.	X	X
	▪ meet the requirements of legal bodies	Ensure the practice methods and procedures used are in compliance with the regulations and requirements of the legal governing authority in the field.	X	X
	▪ provide legal advice	Provide advice in order to ensure that privacy measures are compliant with the law, and provide information, documentation, or advice in your company. E.g. Copyright Legislation describing the protection of the rights of original authors over their work, and how others can use it.	X	

	▪ manage changes in ICT system	Plan, realise and monitor system changes and upgrades. Maintain earlier system versions. Revert, if necessary, to a safe older system version.	X	X
	▪ educate on data confidentiality	Share information with and instruct users in the risks involved with data, especially risks to the confidentiality, integrity, or availability of data. Educate users on how to ensure data protection.	X	X
	▪ train employees (= awareness rising measure)	Lead and guide employees through a process in which they are taught the necessary skills for the perspective job. Organise activities aimed at introducing the work and systems or improving the performance of individuals and groups in organisational settings.	X	X
	▪ cyclical training	Training is a program that helps employees learn specific knowledge or skills to improve performance in their current roles. Development is more expansive and focuses on employee growth and future performance, rather than an immediate job role.	X	X
	▪ analytical and logical thinking skills	Analytical thinking is about breaking down problems logically, into small bites and without emotions. People with strong analytical skills will find a well-thought-out solution in any situation, based on information and facts.	X	X
	▪ drawing conclusions from mistakes made	Related processes have then to be adapted accordingly.	X	X
	▪ ability to work under time pressure	The ability to work under pressure involves dealing with constraints which are often outside of your control - these might be resource or time constraints, the difficulty of the task or having insufficient knowledge required to complete the task, or unforeseen changes or problems.		X
	▪ perform risk analysis	Identify and assess factors that may jeopardise the success of a project or threaten the organisation's functioning. Implement procedures to avoid or minimise their impact.	X	X

	▪ manage processes	Manage processes by defining, measuring, controlling and improving processes with the goal to meet customer requirements profitably.	X	X
	▪ think analytically	Produce thoughts using logic and reasoning in order to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.		X
III.	**Social Competences: You should be able to**			
	▪ address problems critically	Identify the strengths and weaknesses of various abstract, rational concepts, such as issues, opinions, and approaches related to a specific problematic situation in order to formulate solutions and alternative methods of tackling the situation.	X	X
	▪ raise awareness on data protection	Intervene and implement programs or activities that raise awareness of issues relevant for the respective company or clients regarding privacy measures.		X
	▪ be aware of the risk people might cause	It is helpful to anticipate possible errors as much as possible. Of course, this is not always possible. This setting helps: You learn from mistakes.		X
	▪ motivate yourself and others	Motivate staff to take privacy more seriously. Sometimes it might help to do that humorously…		X
	▪ do not fear change	The acceptance to get involved in change and to adapt to new situations is important for you and your employees.		X
	▪ communicate clearly	Speak clearly in addressing employees or clients; communicate information related to their knowledge and be aware of the fact, that not everybody is an expert in Information Security.		X
	▪ exercise patience	Have patience by dealing with unexpected actions from your employees or customers. Not everybody has your background of knowledge.	X	X

	▪ openness to changes	Openness to change refers to an individual's level of acceptance and conscious awareness of the possibility that change may be needed across a range of situations and scenarios, together with the appetite or drive to enact that change.		X
	▪ have good time-management	A fundamental part of time management is planning. Being efficient in planning out your day, meetings and how you will accomplish things will help you stick to your schedule.		X
	▪ work in a group	Whatever form the group work takes, the opportunity to work with others, rather than on your own, can provide distinct benefits: increased productivity and performance, skills development and knowing more about yourself.		X
	▪ demonstrate willingness to learn	Show a positive attitude towards new and challenging demands that can only be met via lifelong learning.	X	X
	▪ focus on service	Actively look for efficient ways to help people.	X	X
	▪ relate empathetically	Recognise, understand and share emotions and insights experienced by another.	X	X
	▪ react calmly in stressful situations	React quickly, calmly, and safely to unexpected situations; provide a solution that solves the problem or diminishes its impact.	X	X
	▪ manage emergency procedures	React quickly in case of emergency and set planned emergency procedures in motion.	X	X

Table 4: Mapping of Data Protection Manager (strategic and operational level)

7.4 Data Protection Administrator (operational level)

Description

Data protection administrators advise and implement solutions to control access to data and programs. They promote a safe exchange of information.

	ESCO matched with TeBelSi profile	Description (based on ESCO & adapted to TeBelSi needs)	ESCO input	TeBelSi input
I.	**ESSENTIAL FIELDS OF KNOWLEDGE**			
	Organisational policies	The policies to achieve set of goals and targets regarding the development and maintenance of an organisation.	X	X
	Organisational resilience	The strategies, methods and techniques that increase the organisation's capacity to protect and sustain the services and operations that fulfil the organisational mission and create lasting values by effectively addressing the combined issues of security, preparedness, risk and disaster recovery.	X	X
	Information Security Strategy	The plan defined by a company which sets the information security objectives and measures to mitigate risks, define control objectives, establish metrics and benchmarks while complying with legal, internal and contractual requirements.	X	X
	ICT security legislation	The set of legislative rules that safeguards information technology, ICT networks and computer systems and legal consequences which result from their misuse. Regulated measures include firewalls, intrusion detection, anti-virus software and encryption. See also GDPR contents and rules.	X	X

	Anonymization of data	It means the transformation of personal data, after which it is no longer possible to assign individual personal or material information to a specific or identifiable natural person or it can be done only with a disproportionate expenditure of time, costs and forces.		X
	Audit	Systematic and independent assessment of a given organization, system, process, project or product. The subject of the audit is examined for compliance with a specific reference point - checklist, legal provisions, norms, standards or internal regulations of a given organization (policies, procedures).		X
	Data pseudonymization	Restricts the ability to associate a data set with the true identity of the data subject.		X
	Business Continuity Management	BCM is a framework for identifying an organization's risk of exposure to internal and external threats. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.		X
II.	**Professional Skills & Competences: You need to know how to**			
	▪ attend to ICT systems quality	Ensure correct operations which comply fully with specific needs and outcomes in terms of the development, integration, security and overall management of privacy measures.	X	X
	▪ identify ICT system weaknesses	Analyse the system and network architecture, hardware and software components and data in order to identify weaknesses and vulnerability to intrusions or attacks.	X	X

	▪ ensure compliance with policies	To ensure compliance with legislation and company procedures in respect of data protection in the workplace and public areas, at all times. To ensure awareness of and compliance with all Company Policies in relation to privacy in the workplace.	X	
	▪ monitor company policy	Monitor the company's policy and propose improvements to the company with strong focus on privacy / data protection.	X	X
	disseminate internal communications	Disseminate internal communications using the different communication channels that a company has at its disposal (=awareness rising)	X	X
	▪ ensure compliance with company regulations	Guarantee that employees' activities follow company regulations, as implemented through client and corporate guidelines, directives, policies and programmes with focus on privacy.	X	X
	▪ ensure compliance with legal requirements	Guarantee compliance with established and applicable standards and legal requirements such as specifications, policies, standards or law regarding data protection and privacy.	X	X
	follow the statutory obligations	Understand, abide by, and apply the statutory obligations of the company in the daily performance of the job.	X	X
	▪ gather feedback from employees	Communicate in an open and positive manner in order to assess levels of satisfaction with employees, their outlook on the work environment, and in order to identify problems and devise solutions.	X	X
	▪ educate on data confidentiality	Share information with and instruct users in the risks involved with data, especially risks to the confidentiality, integrity, or availability of data. Educate them on how to ensure data protection.	X	X
	▪ ensure proper document management	Guarantee that the tracking and recording standards and rules for document management are followed, such as ensuring that changes are	X	X

		identified, that documents remain readable and that obsoleted documents are not used.		
	▪ train employees (= awareness rising measure)	Lead and guide employees through a process in which they are taught the necessary skills for the perspective job. Organise activities aimed at introducing the work and systems or improving the performance of individuals and groups in organisational settings.	X	X
	▪ cyclical training	Training is a program that helps employees learn specific knowledge or skills to improve performance in their current roles. Development is more expansive and focuses on employee growth and future performance, rather than an immediate job role.	X	X
	▪ analytical and logical thinking skills	Analytical thinking is about breaking down problems logically, into small bites and without emotions. People with strong analytical skills will find a well-thought-out solution in any situation, based on information and facts.	X	X
	▪ analytical and logical thinking skills	Analytical thinking is about breaking down problems logically, into small bites and without emotions. People with strong analytical skills will find a well-thought-out solution in any situation, based on information and facts.	X	X
	▪ drawing conclusions from mistakes made	Related processes have then to be adapted accordingly.	X	X
	▪ ability to work under time pressure	The ability to work under pressure involves dealing with constraints which are often outside of your control - these might be resource or time constraints, the difficulty of the task or having insufficient knowledge required to complete the task, or unforeseen changes or problems.		X
	▪ perform risk analysis	Identify and assess factors that may jeopardise the success of a project or threaten the organisation's functioning. Implement procedures to avoid or minimise their impact.	X	X

	▪ manage processes	Manage processes by defining, measuring, controlling and improving processes with the goal to meet customer requirements profitably.	X	X
	▪ think analytically	Produce thoughts using logic and reasoning in order to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.		X
III.	**Social Competences: You should be able to**			
	▪ address problems critically	Identify the strengths and weaknesses of various abstract, rational concepts, such as issues, opinions, and approaches related to a specific problematic situation in order to formulate solutions and alternative methods of tackling the situation.	X	X
	▪ raise awareness on data protection	Intervene and implement programs or activities that raise awareness of issues relevant for the respective company or clients regarding privacy measures.		X
	▪ be aware of the risk people might cause	It is helpful to anticipate possible errors as much as possible. Of course, this is not always possible. This setting helps: You learn from mistakes.		X
	▪ motivate yourself and others	Motivate staff to take privacy more seriously. Sometimes it might help to do that humorously…		X
	▪ do not fear change	The acceptance to get involved in change and to adapt to new situations is important for you and your employees.		X
	▪ communicate clearly	Speak clearly in addressing employees or clients; communicate information related to their knowledge and be aware of the fact, that not everybody is an expert in Information Security.		X
	▪ exercise patience	Have patience by dealing with unexpected actions from your employees or customers. Not everybody has your background of knowledge.	X	X

	▪ openness to changes	Openness to change refers to an individual's level of acceptance and conscious awareness of the possibility that change may be needed across a range of situations and scenarios, together with the appetite or drive to enact that change.		X
	▪ have good time-management	A fundamental part of time management is planning. Being efficient in planning out your day, meetings and how you will accomplish things will help you stick to your schedule.		X
	▪ work in a group	Whatever form the group work takes, the opportunity to work with others, rather than on your own, can provide distinct benefits: increased productivity and performance, skills development and knowing more about yourself.		X
	▪ demonstrate willingness to learn	Show a positive attitude towards new and challenging demands that can only be met via lifelong learning.	X	X
	▪ focus on service	Actively look for efficient ways to help people.	X	X
	▪ react calmly in stressful situations	React quickly, calmly, and safely to unexpected situations; provide a solution that solves the problem or diminishes its impact.	X	X
	▪ manage emergency procedures	React quickly in case of emergency and set planned emergency procedures in motion.	X	X

Table 5: Mapping of Data Protection Administrator (operational level)

8 TEBEISI JOB PROFILE “DP-IS OFFICER IN SME’S”

This first draft of the Job Profile “Data Protection & Information Security Officer in SME’s” (DP-IS Officer in SME’s) is based on the results described in detail in the sections above in this report:

Main outcomes of Field Research: The partnership interviewed more than 60 experts in the fields of Data protection and Data security, Information security management and IT security in small and medium-sized enterprises (SMEs). It was important to us to gather personal opinions and experiences on these topics, either individually or in focus groups. **All partners collected at least 10 cases from their field research.**

Based on these findings we created a first **‘List of Competences needed in SMEs’:** We have considered different questions to find out how the experts assess the required competencies of employees. Then we presented a short summary of competences identified by our experts for SMEs in fields, Data protection and Information Security.

In the section ‘TeBeISi Requirements matched with ESCO Profiles’ we presented our first mapping of our TeBeISi outcomes (results from interviews with experts, case studies & desk research) with the identified ESCO profiles. We drafted 4 different fictitious sample profiles: Information Security Manager, Information Security Administrator, Data Protection Manager and Data Protection Administrator. This step was important to first time apply the results of desk and field research to concrete job profiles.

The project partners, as well as external partners, concluded that this breakdown into four profiles was far too extensive for the majority of SMEs. We also examined how we could better address the needs of micro and small enterprises in particular and agreed to go one step further:

We drafted one concrete job profile of a **"DATA PROTECTION & INFORMATION SECURITY OFFICER IN SME'S" (DP-IS OFFICER IN SME'S).**

We have divided the requirements into the following thematic areas in order to find a clearer presentation for a DP-IS Officer in SME’s:

- Legal Aspects - basic knowledge
- Personality
- Technical Skills
- Social Skills
- Methodologies

The full profile can be found in Annex 2 Job Profile 'DP-IS OFFICER IN SME'S’

9 NEXT STEPS IN THE TEBEISI PROJECT

The results presented in this report form an important basis for further processing in the project, e.g. in IO3, where the preliminary results are further specified.

'IO3 - the online questionnaire' builds on the findings of IO1 and will provide the basis for IO4 – the TeBeISi Curriculum. The aim of IO3 will be the development of a questionnaire, which SMEs to determine a possible gap of existing competencies for information security and data protection within the firm. Managers shall be facilitated to identify potentials within the workforce, meanwhile employees have the possibility to explore their suitability for a new role. The main Work packages of IO3 are:

WP1: Evaluation of Expert Interviews/Focus Groups

In order to substantiate our findings, we need to finalize the analysis of our field research from IO1. This is especially important with regards to IO6, the Scientific Research paper. To this end, a methodology of how to analyse the interviews in a structured way ("coding of answers") will be further developed by BF/M.

WP2: Transformation of Job Profile 'DP-IS OFFICER IN SME'S'

In order to improve the quality of the questionnaire, the output of IO1 needs to be revised, and the content shall be transformed into competences, based on a commonly aligned methodology. This methodology needs to be established and shall clarify how to derive and formulate competences. Finally, it needs to be checked if all competences are clear cut in their relation to other items.

WP3: Questionnaire for Experts

In order to break the items from the job profile down to a workable list, experts from the field will be asked to give their opinion on the importance and relevance of the items. These experts must work in the area of Information Security or Data Protection. To this end, questions must be developed which allow the experts to properly state their perceived relevance and importance. As a result of WP3, a job profile with 3-4 competences per category will remain, which represents a feasible requirement profile for SMEs.

WP4: Development of online questionnaire

In the final step of the process, the self-assessment tool needs to be created. The tool shall be used by employees in SME to assess their suitability to carry out the tasks of an IS-DP Officer. It must therefore be evaluated, how such an assessment can be properly conducted.

Links

Digital Competence Framework: https://ec.europa.eu/jrc/en/digcomp

ESCO portal: https://ec.europa.eu/esco

ESCO mapping: *https://ec.europa.eu/esco/portal/document/en/0a89839c-098d-4e34-846c-54cbd5684d24*

ESCO transparency instruments: *https://ec.europa.eu/esco/portal/document/en/0a89839c-098d-4e34-846c-54cbd5684d24*

ECVET in Europe, *https://www.cedefop.europa.eu/en/publications-and-resources/publications/5556*

European e-Competence Framework (e-CF): www.ecompetences.eu

e-CF brochure by CEN (European Committee for Standardization), *www.cencenelec.eu*

EQF: https://ec.europa.eu/esco/portal/escopedia/European_Qualifications_Framework__40_EQF_41

EQF descriptors: *https://ec.europa.eu/ploteus/content/descriptors-page*

USING LEARNING OUTCOMES, European Qualifications Framework Series: Note 4, *https://ec.europa.eu/ploteus/sites/eac-eqf/files/EQF_note4_en.pdf*

Linking of ECVET – EQF/NQF – Europass: *www.ecvet-info.at*

NQR in Austria: *https://www.qualifikationsregister.at/en/*

ANNEXES

Annex 1 – Cases collected from field research

Annex 2 – Job Profile 'DP-IS OFFICER IN SME'S'

RELATED DOCUMENTS

National Reports – Desk Research

- TeBelSi IO1 Desk Research AT
- TeBelSi IO1 Desk Research DE
- TeBelSi IO1 Desk Research IT
- TeBelSi IO1 Desk Research LT
- TeBelSi IO1 Desk Research PL

National Reports – Field Research

- TeBelSi IO1 Report on Expert Interviews AT
- TeBelSi IO1 Report on Expert Interviews DE
- TeBelSi IO1 Report on Expert Interviews IT
- TeBelSi IO1 Report on Expert Interviews LT
- TeBelSi IO1 Report on Expert Interviews PL

10 Publication bibliography

European Commission (2011): Using learning outcomes – European Qualifications Framework Series: Note 4. Available online at https://ec.europa.eu/ploteus/sites/eac-eqf/files/EQF_note4_en.pdf.

European Commission Directorate: Description of the eight EQF levels. Available online at https://europa.eu/europass/en/description-eight-eqf-levels, checked on 8/10/2021.

European Commission Directorate (2013): ESCO - European Classification of Skills, Competences, Qualifications and Occupations. Publications Office of the European Union. Luxembourg. Available online at https://ec.europa.eu/social/BlobServlet?docId=15721&langId=en, checked on 8/10/2021.

European Commission Directorate (2017a): ESCO handbook - European Skills, Competences, Qualifications and Occupations. Available online at https://ec.europa.eu/esco/portal/document/en/0a89839c-098d-4e34-846c-54cbd5684d24, checked on 8/10/2021.

European Commission Directorate (2017b): ESCO strategic framework. Available online at https://ec.europa.eu/esco/portal/document/en/89a2ca9a-bc79-4b95-a33b-cf36ae1ac6db, checked on 8/10/2021.

European Commission Directorate (2020a): ESCO Ethical hacker. Available online at http://data.europa.eu/esco/occupation/76ef0a87-6afe-4560-b5d0-9a086abe45c5, checked on 8/10/2021.

European Commission Directorate (2020b): ESCO ICT security administrator. Available online at http://data.europa.eu/esco/occupation/0464b062-cea6-4164-b10d-956c61956ae7, checked on 8/10/2021.

European Commission Directorate (2020c): ESCO ICT security manager. Available online at https://ec.europa.eu/esco/portal/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F7754d570-9519-48c2-b1c9-8e165f8bca0f&conceptLanguage=en&full=true#&uri=http://data.europa.eu/esco/occupation/7754d570-9519-48c2-b1c9-8e165f8bca0f, checked on 8/10/2021.

European Commission Directorate (2020d): ESCO Occupations. Available online at https://ec.europa.eu/esco/portal/occupation.

European Commission Directorate (2020e): ESCO Policy manager. Available online at http://data.europa.eu/esco/occupation/64e38ce7-3901-4261-bfee-77c7a77397f2, checked on 8/10/2021.

European Commission Directorate (2020f): ESCO Professionals. Available online at http://data.europa.eu/esco/isco/C2, checked on 8/10/2021.

Malta Qualifications Council; National Commission for Higher Education (2020): ECVET in Europe. A New European Tool for Promoting, Facilitating and Enhancing Lifelong Learning and Mobility. Available online at http://www.ecvet-projects.eu/Admin/Documents/ECVET%20Europe%20Final.pdf, checked on 8/10/2021.

Publications Office of the European Union (2018): DigComp into Action - Get inspired, make it happen. Available online at https://publications.jrc.ec.europa.eu/repository/handle/JRC110624, checked on 8/10/2021.

Rammstedt, Beatrice; Kemper, Christoph J.; Klein, Mira Céline; Beierlein, Constanze; Kovaleva, Anastassiya (2013): A Short Scale for Assessing the Big Five Dimensions of Personality. 10 Item Big Five Inventory (BFI-10). In *GESIS - methoden, daten, analyse* 7 (2), pp. 233–249.

Vuorikari R; Punie Y; Carretero Gomez S; Van Den Brande G. (2016): DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: The Conceptual Reference Model. Available online at https://publications.jrc.ec.europa.eu/repository/handle/JRC101254, checked on 8/10/2021.

Identification of Competence Profiles

We thank the co-authors and from:

BF/M-Bayreuth

Mykolas Romeris University

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Funded by the Erasmus+ Programme of the European Union

https://information-security-in-sme.eu/.