Information Security Competences

A qualitative analysis of Expert Interviews on Knowledge and Skills of Professionals in Information Security

Funded by the Erasmus+ Programme of the European Union

TeBelSi

This document is licensed under CC BY-SA 4.0.

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.

List of Content

List of Figures

List of Tables

1 What is important for interviewees (evaluation of codes)

1.1 Brief introduction to the code-system

At this stage of work, there are 33 taken interviews: ten from Poland and ten from Austria, nine from Germany, and four from Lithuania. All of them have been analysed in MAXQDA. Each interview marked up with unique codes that represent different important interviewees' issues. All codes have a special structure and hierarchy (see Figure 1). They are divided into five main groups:

1. qualification;
2. mistakes;
3. attack vectors;
4. tasks and activities;
5. competences critical for success.

As we can see on Figure 2, the two most popular groups are *"competences critical for success"* and *"tasks and activities"*. Together they have been discussed with respondents in ~87% of cases. The other ~13% has been dedicated to *“mistakes”*, *“attack vectors”, and “qualification”*. All of these categories we will discuss in further chapters.

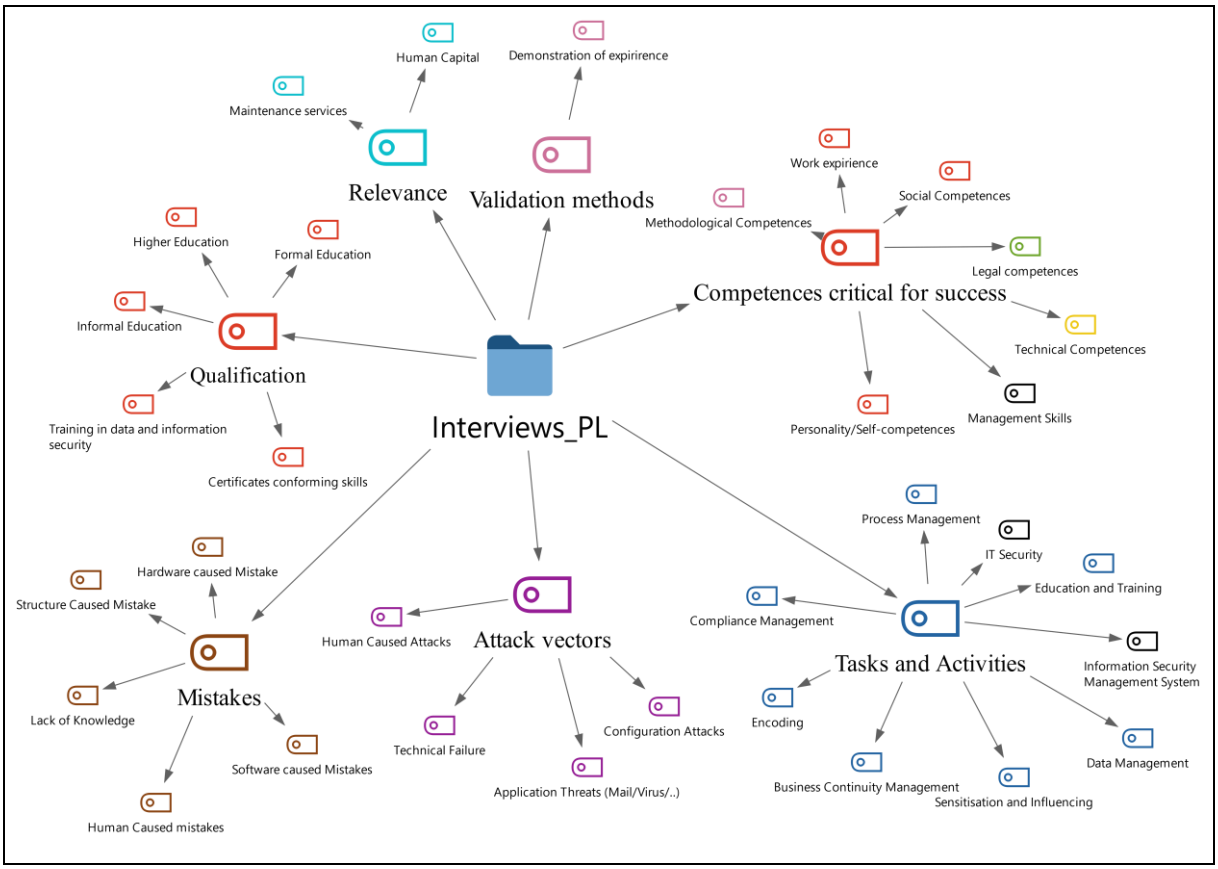

Figure 1: Code hierarchy

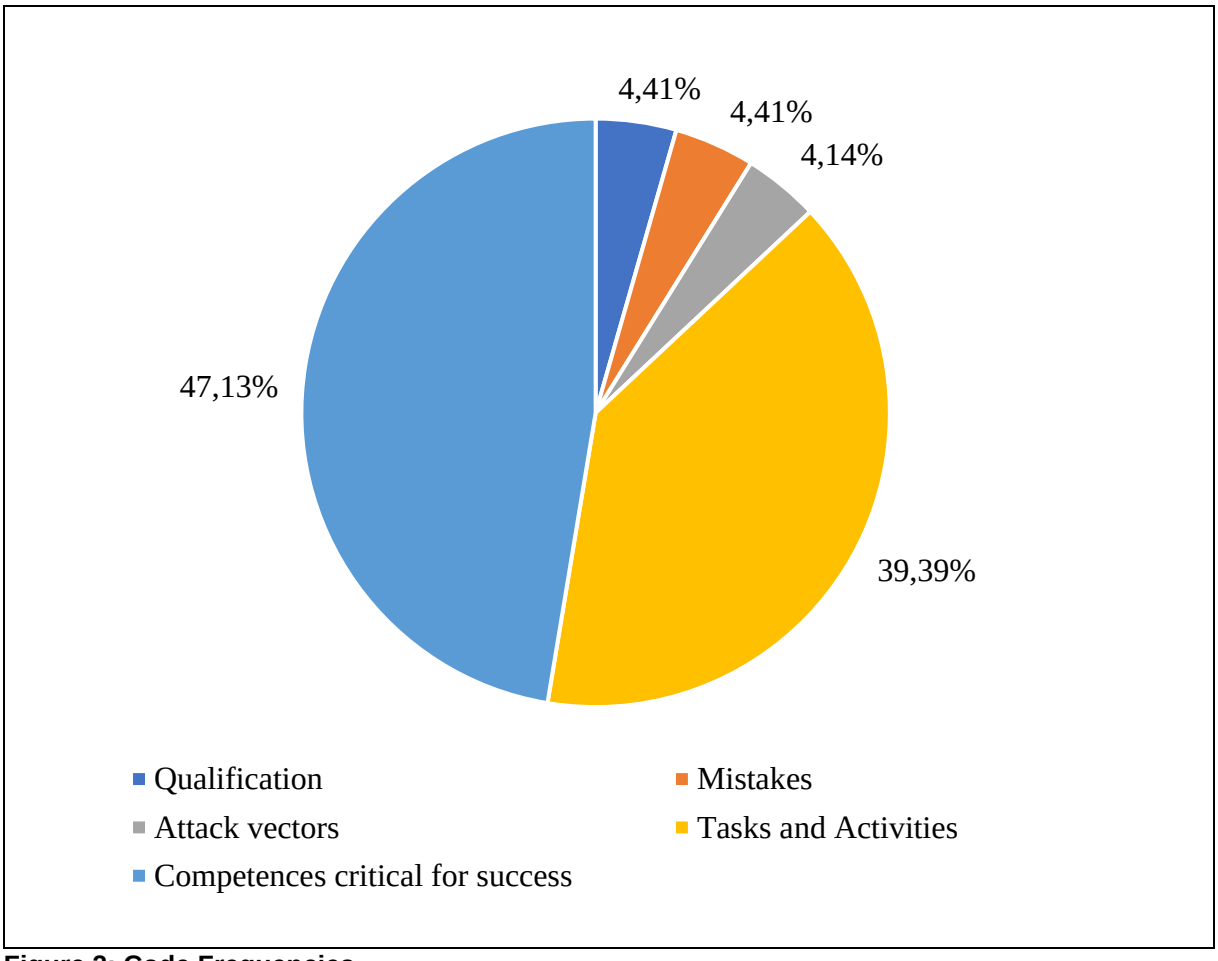

Figure 2: Code Frequencies

1.2 Competences critical for success

This category includes codes that are marked as critical for the successful functioning of the firm. There are seven groups in this category:

No.	Item (Tasks and Activities)	Percentage share
1	Social competences	31%
2	Personality/self-competences	30%
3	Technical competences	13%
4	Legal competences	12%
5	Work experience	7%
6	Management skills	5%
7	Methodological competences	2%

Table 1. Competences critical for success

From our interviewees' point of view, the two crucial groups of such competencies are "social competences" and "personality/Self-competences" (together 61%). However technical competences (13%) and legal competences (12%) are important too. Further we will look at these groups in detail

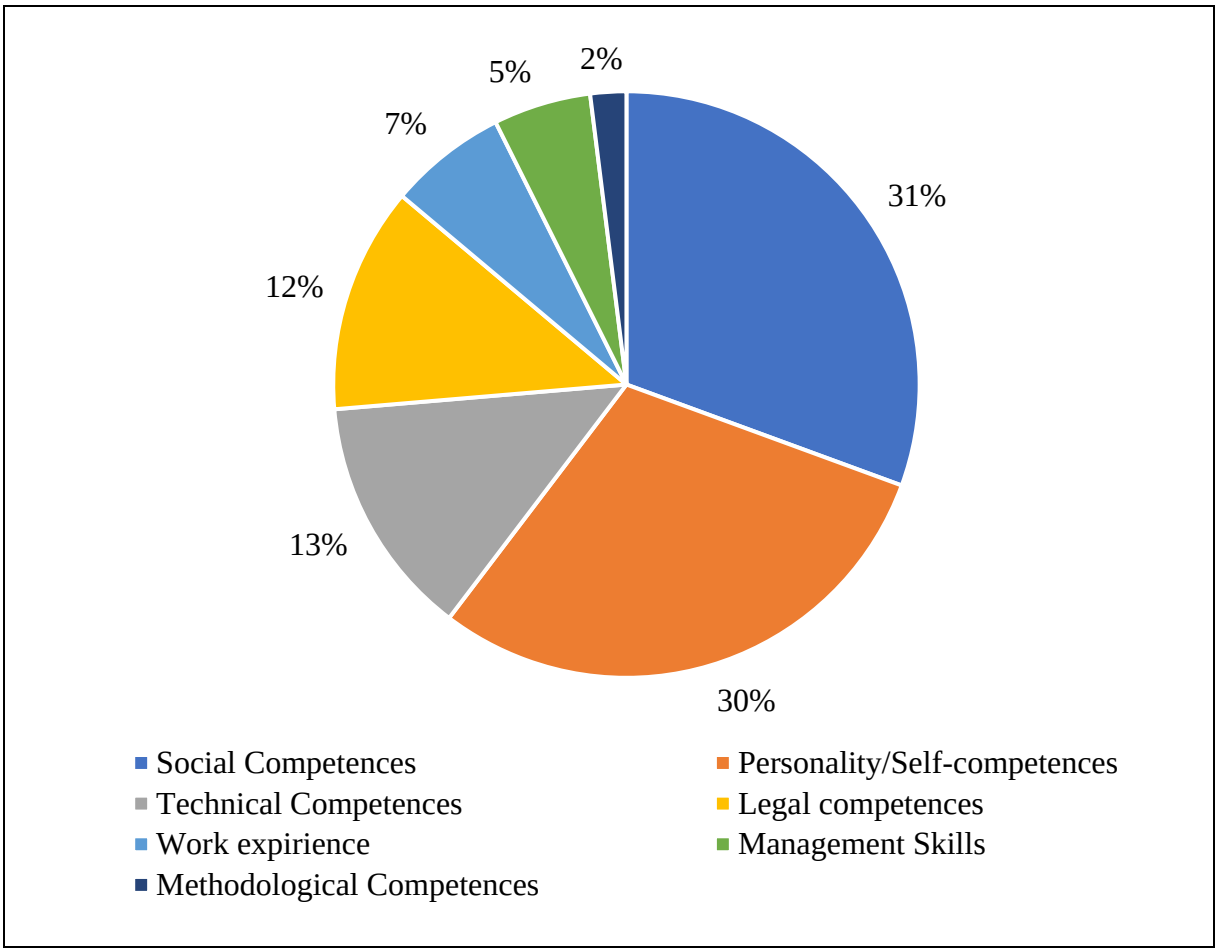

Figure 3. Competences critical for success

1.2.1 Social competences

For one's turn, social competences are supposed to describe the particular worker's ability to interact with the team. For example, in this group, we have the following codes:

No.	Item (Tasks and Activities)	Percentage share
1	Communication skill	32%
2	Team-minded	29%
3	Work under pressure	9%
4	Selling	9%
5	Problem solving skill	6%
6	Sharing knowledge/explain in simple way	6%
7	Time management	6%

CC BY-SA 4.0

8	Other competences, which frequency are less than 2%(logical thinking, intelligence techniques, commitment to action, English skills).	6%

Table 2. Social competences

According to respondents' answers, they are usually looking for team-minded persons with good communication skills.

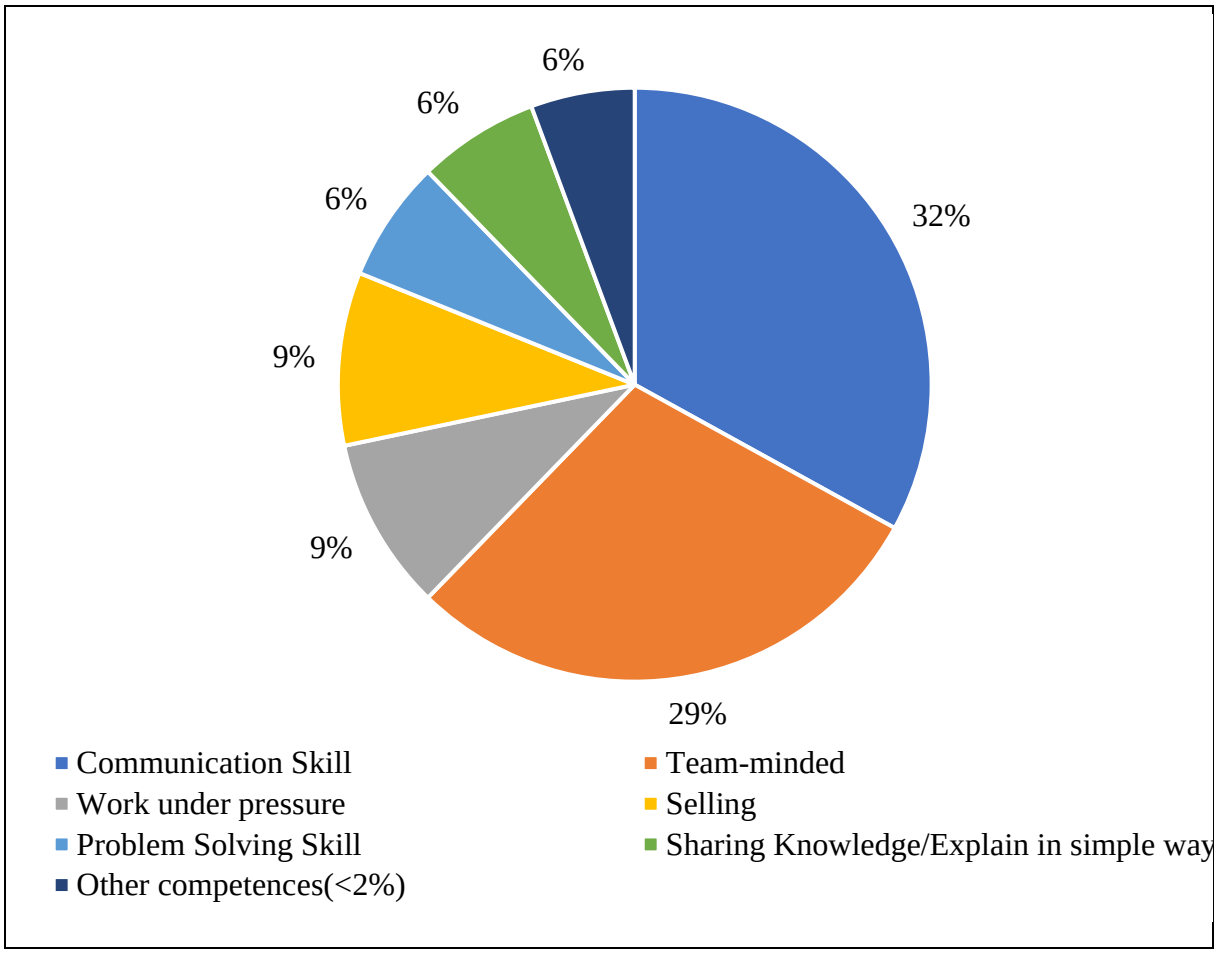

Figure 4. Social Competences

1.2.2 Self-competences

This group contains personal traits that might be important for the work, for example:

No.	Item (Tasks and Activities)	Percentage share
1	Analytical thinking	20%
2	Readiness to learn	14%
3	Open-minded	7%

4	Independence	7%
5	Taking responsibility	7%
6	Social competences	7%
7	Self-organization	7%
8	Creativity	6%
9	Empathy	5%
10	Calmness	4%
11	Self-motivation	3%
12	Will to work	3%
13	Other competences, which frequency are less than 2%(trust in others, concentration, self-reliance, self-confidence, resilience, attend to details, should know what he wants, perseverance, mistake handling).	12%

Table 3. Self-competences

As we can see, respondents would like to see open-minded and independent employees with analytical thinking who are ready to take responsibility and learn more.

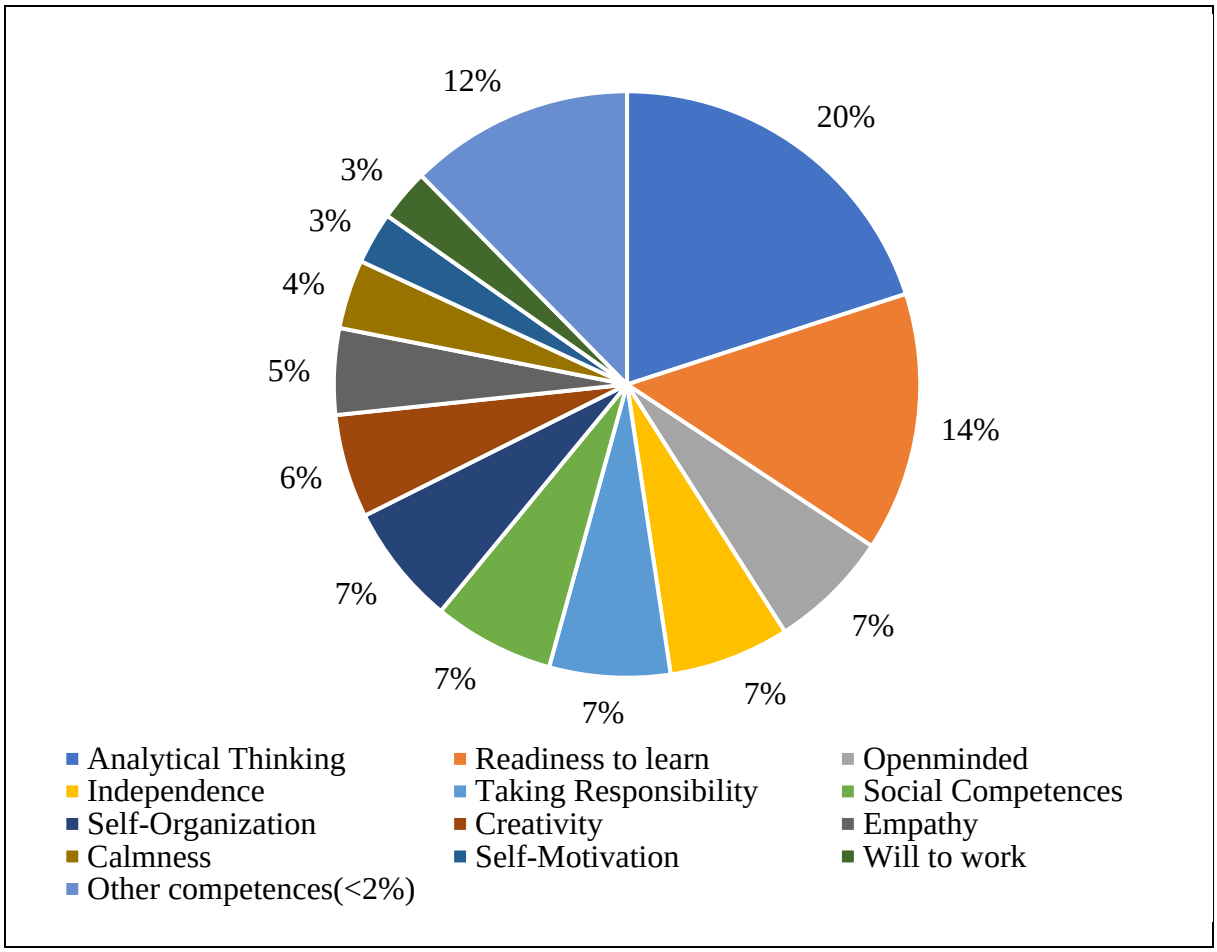

Figure 5. Self-competences

1.2.3 Technical competences

For this group, the competences to interact with different technical equipment are crucial. This group includes the following codes:

No.	Item (Tasks and Activities)	Percentage share
1	IT know-how	34%
2	Technical skills	15%
3	Knowledge IS	13%
4	Attack vectors	9%
5	System environment and ICT components	4%
6	Information management	4%
7	Incident control	4%
8	Database	4%

9	Mobile systems	4%
10	Administration	2%
11	Cloud computing	2%
12	Identity and access management(IAM)	2%
13	Knowledge security audits	2%

Table 4. Technical competences

As we can see, interviewees are looking mostly for workers who can interact with complex technics. However, we cannot infer from the answer IT-know-how what this specifically means for each respondent. We can only assume that a minimum understanding of the functioning of IT landscapes were meant.

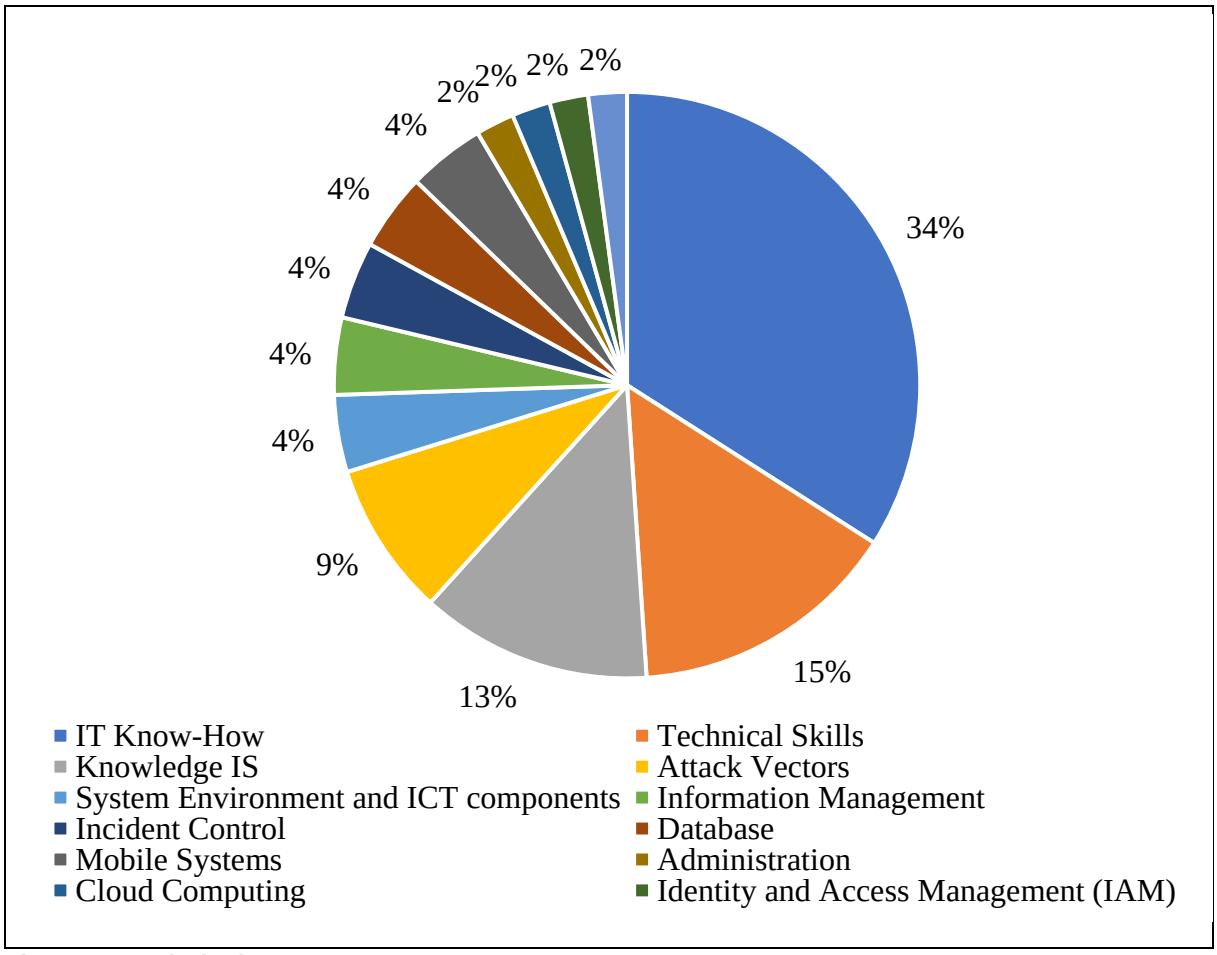

Figure 6. Technical competences

1.2.4 Legal competences

Last but not least is the group of legal competences, which contains the following codes:

No.	Item (Tasks and Activities)	Percentage share
1	Data protection regulations	20%
2	ISO/IEC 27001	16%
3	ISO27000	16%
4	Policy application	5%
5	Familiarity with legal requirements	5%
6	NIST SP 800-53	5%
7	CISA, CISM, CIA, CIS Certificate	5%
8	Data protection policy	2%
9	ISO 31000	2%
10	ISO 22301	2%
11	ISO/IEC 17799	2%

Table 5. Legal competences

For our respondents, data security issues are critical. That is why they want their employees to be familiar with data protection regulations and different ISO standards (especially ISO/IEC 27001 and ISO27000).

Some of the respondents want their employees to be not only educated for such requirements but able to use this knowledge. For example, candidate one from Germany says:

> *"Data protection regulation should not only be known but also understood."(DE_1)*

CC BY-SA 4.0

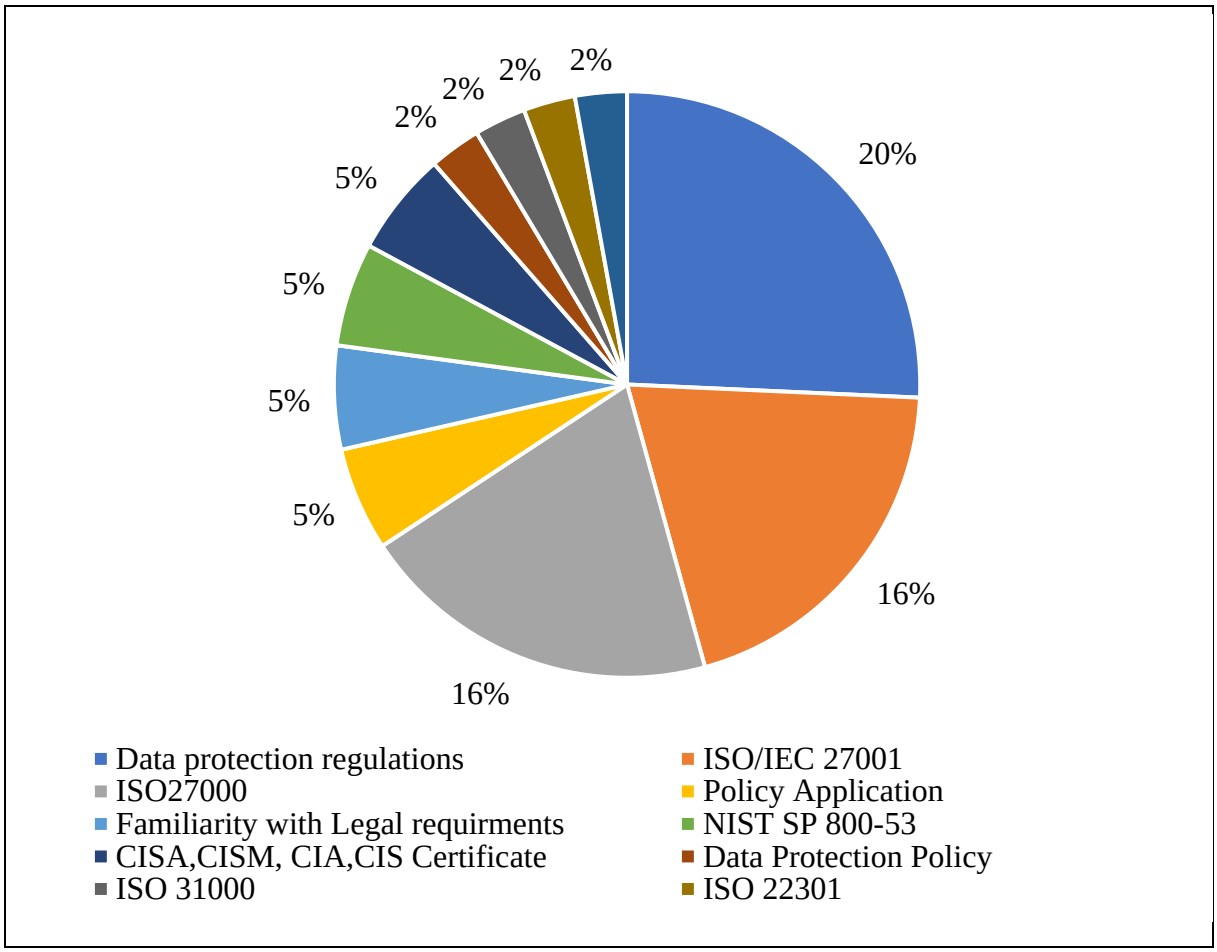

Figure 7. Legal competences

Social Competences	Self-Competences	Technical Skills	Legal Competences
Communication skill (32%)	Analytical thinking (20%)	IT know-how (34%)	Data protection regulations (20%)
Team-minded (29%)	Readiness to learn (14%)	Technical skills (15%)	ISO/IEC 27001 (16%)
Work under pressure (9%)	Open-minded (7%)	Knowledge IS (13%)	ISO27000 (16%)
Selling (9%)	Independence (7%)	Attack vectors (9%)	Policy application (5%)
Problem solving skill 6%)	Taking responsibility (7%)	System environment and ICT components (4%)	Familiarity with legal requirements (5%)
Sharing knowledge/explain in simple way (6%)	Social competences (7%)	Information management (4%)	NIST SP 800-53 (5%)
Time management (6%)	Self-organization (7%)	Incident control (4%)	CISA CISM CIA CIS Certificate (5%)
Other competences (6%)	Creativity (6%)	Database (4%)	Data protection policy (2%)
	Empathy (5%)	Mobile systems (4%)	ISO 31000 (2%)

Calmness (4%)	Administration (2%)	ISO 22301 (2%)
Self-motivation (3%)	Cloud computing (2%)	ISO/IEC 17799 (2%).
Will to work (3%)	Identity and access management (IAM) (2%)	Data protection regulations (20%)
Other competences (12%)	Knowledge security audits (2%)	

Table 6. Summary of significant competences critical for success

1.3 Tasks and Activities

This category is reflecting the possible activities of employees and includes the following groups:

No.	Item (Tasks and Activities)	Percentage share
1	Compliance Management	20%
2	Education and Training	17%
3	Process Management	15%
4	Information Security Management System	11%
5	Risk Management	8%
6	Sensitisation and Influencing	6%
7	Business Continuity Management	6%
8	Data Management	6%
9	IT Security	3%
10	Security Testing	3%
11	Other tasks and activities, which frequency are less than 2% (procurement, mediation and stakeholder management, change management, encoding, advise, personnel decision, password management, role-based access control).	5%

Table 7. Tasks and Activities

Thus, workers' essential activities should direct on both compliance, process and information security management and education and training. Further, we will look at activities' groups in detail.

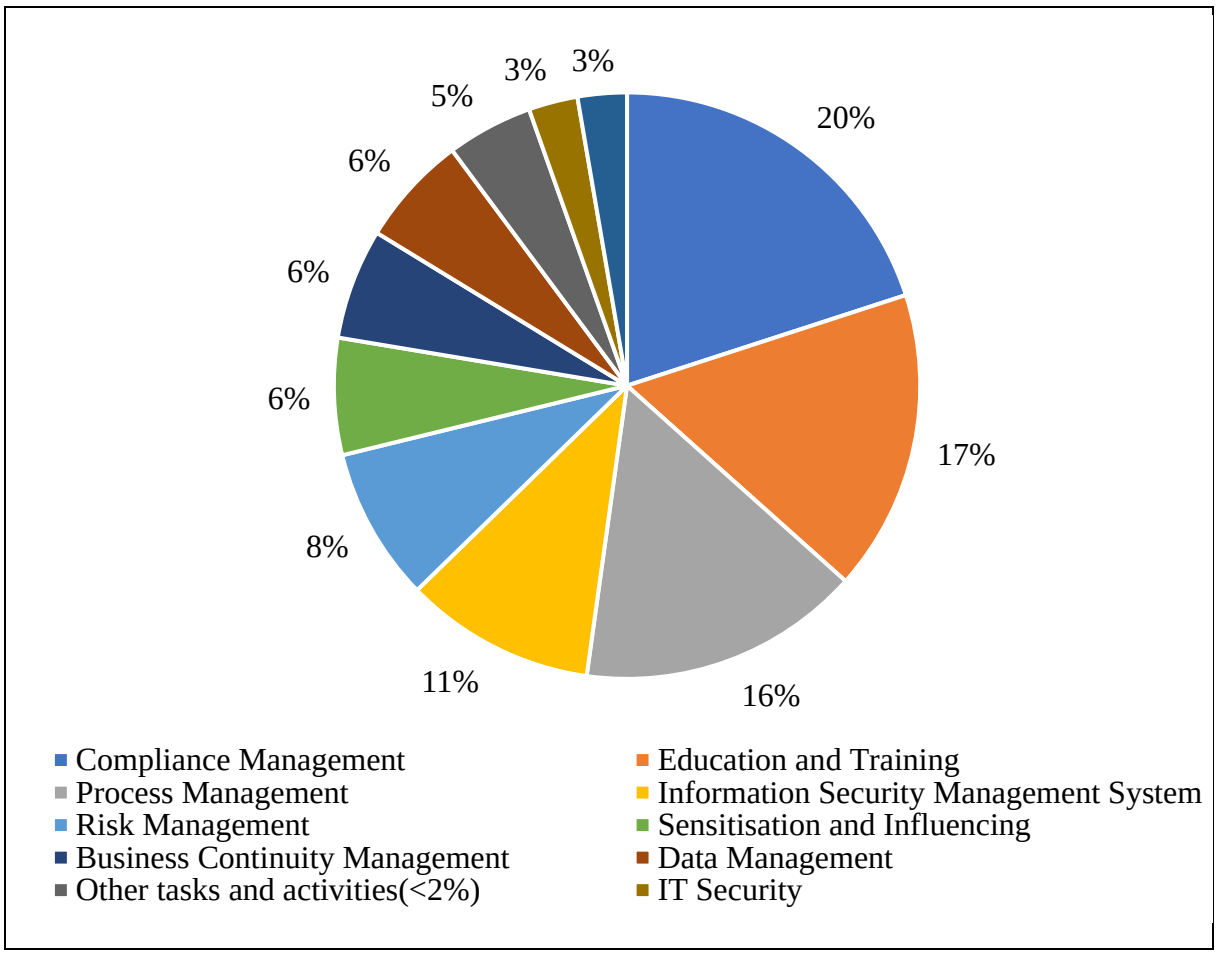

Figure 8. Tasks and Activities

1.3.1 Complacence management

According to our respondents, complacence management focus on the following tasks:

No.	Item (Tasks and Activities)	Percentage share
1	Establish guideline/policies	42%
2	Compliance activities	19%
3	Compliance monitoring	15%
4	Analysis of regulations	8%
5	Creating IS documentation	7%

CC BY-SA 4.0

6	Monitor compliance with the law	3%
7	Supervision	3%
8	Compliance testing	2%

Table 8. Complacence management

Most of all, interviewees want their workers to create complacence policies for the company. These policies can be different. For example, candidate five from Austria mark that his company...

> *"...has developed its own comprehensive privacy policy."(AT_5)*

Another possible way to create specific policies is data protection. Candidate six from Austria says:

> *"Our company takes the issues of data protection and IT security very seriously and the management stands behind the guidelines."(AT_6)*

Candidate ten from Austria mark up the fact that their company's guidelines are made together with IT-specialists:

> *"We develop the implementation of new guidelines together with the technical staff and therefore always have a good level of knowledge."(AT_10)*

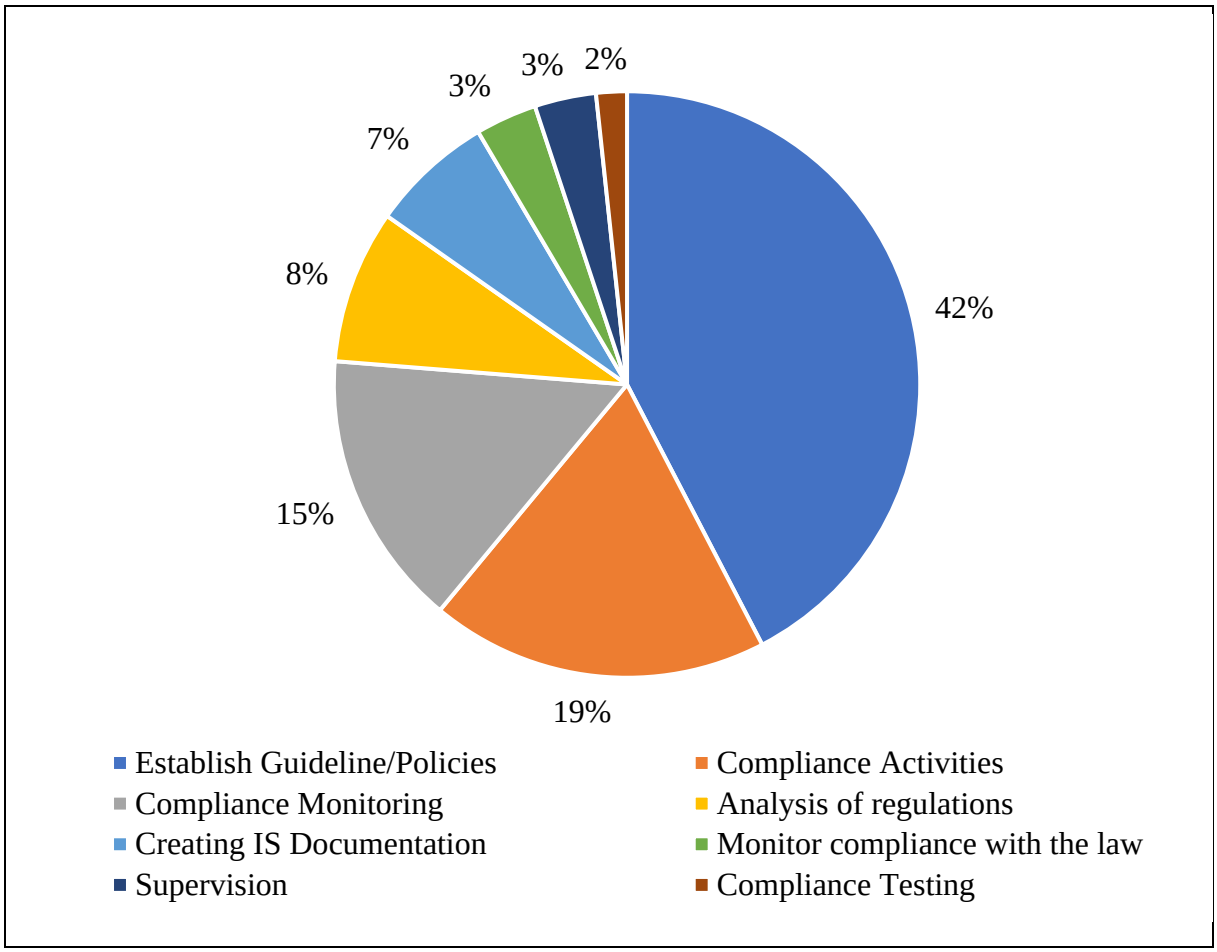

Figure 9. Complacence management

1.3.2 Education and training

There is only one significant code in this group, which duplicate the name of the group's name. However, there are a few interesting examples. According to candidate nine from Poland:

> *"the frequency of training should be increased so that every employee is aware of the danger that the university may face in the event of improper and unreliable compliance with information on security rules." (POL_9)*

At the same time, in the company of candidate nine from Austria:

> *"All employees are trained in the basic knowledge of GDPR" (AT_9)*

1.3.3 Process management

This group contain codes that are related to the different process in the company:

No.	Item (Tasks and Activities)	Percentage share
1	Process Definition	26%

2	Process Optimization	22%
3	Process Implementation	22%
4	Process Identification	13%
5	Process Assessment	9%
6	Process Standardization	7%

Table 9. Process management

As we can see, respondents mostly want their employees to create a plan of work, optimize it, and then implement it. Identification of the process, together with assessment and standardization, for example, are rarely needed.

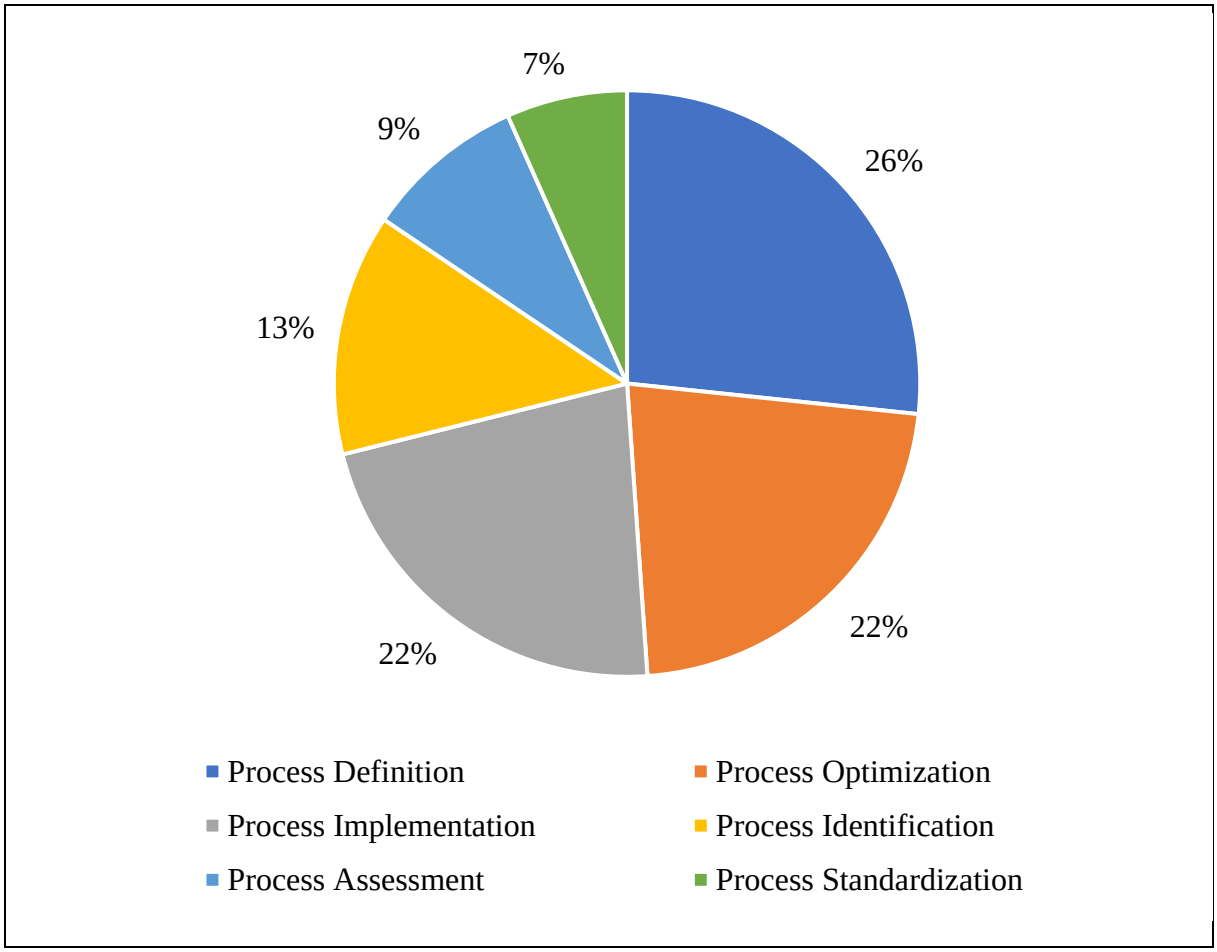

Figure 10. Process Management

1.3.4 Information Security Management System(ISMS)

This group is dealing with information security and contains the following codes:

No.	Item (Tasks and Activities)	Percentage share
1	Monitoring	29%
2	Implement ISMS	23%
3	Define requirements for ISMS	10%
4	Event management	6%
5	Maintaining ISMS	6%
6	Procedures	6%
7	Establishing ISMS	3%
8	Safety	3%
9	Methods and management	3%
10	Responsibility for IS	3%
11	Maintaining IS	3%

Table 10. Information Security Management System(ISMS)

Under monitoring, we understand here an examination of information security status. As we can see, it is crucial for candidates. For instance, candidate three from Poland stays that:

> *"Lack of regular analysis (of security status) may result in instability and be a source of danger." (POL_3)*

Nevertheless, not only monitoring is essential. Also, respondents pay attention to the implication of ISMS and creating requirements of ISMS.

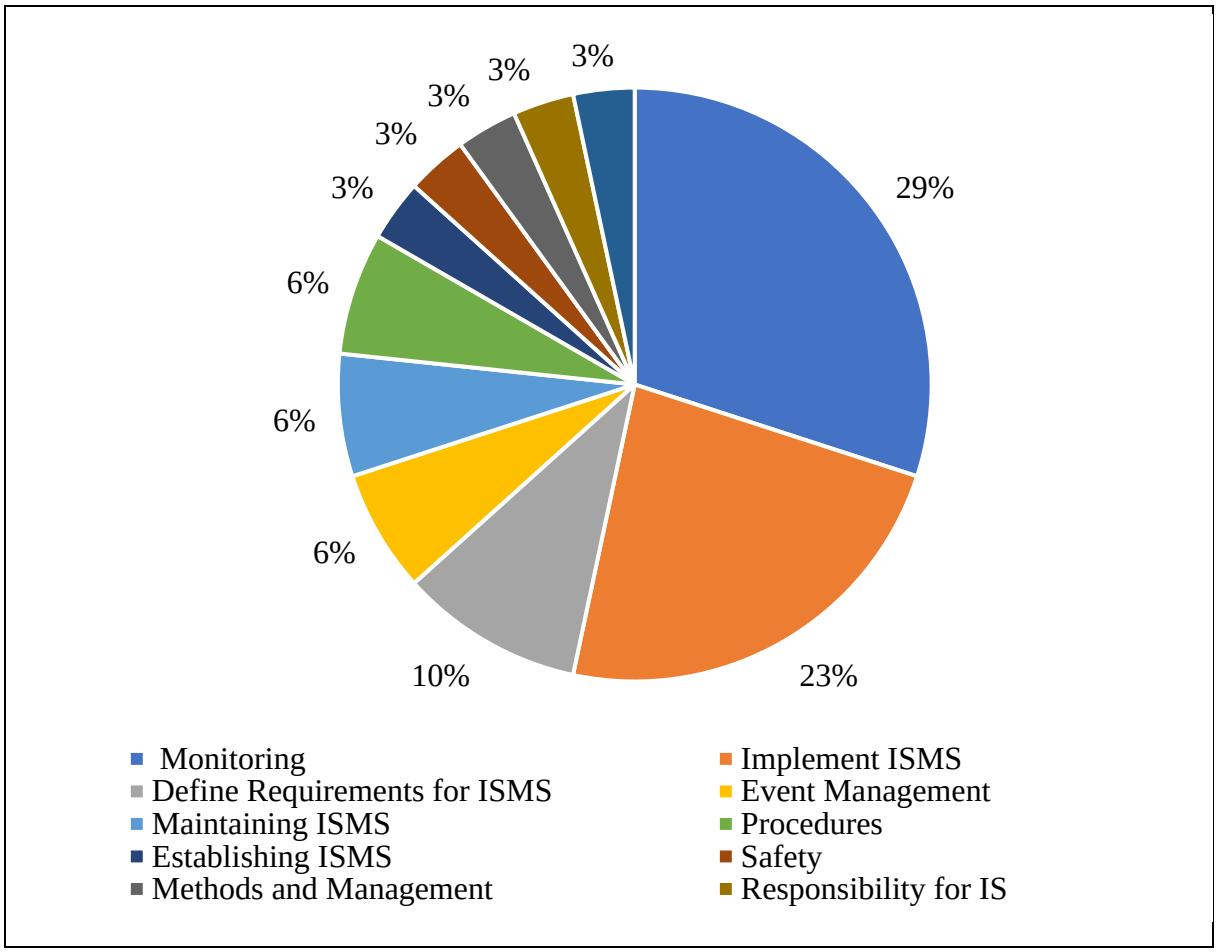

Figure 11. Information Security Management System

Complacence management	Education and training	Process management	Information Security Management System(ISMS)
Establish guideline/policies (42%)	Education and training (92%)	Process Definition (26%)	Monitoring (29%)
Compliance activities (19%)	Self-studying (6%)	Process Optimization (22%)	Implement ISMS (23%)
Compliance monitoring (15%)	Gamification (2%)	Process Implementation (22%)	Define requirements for ISMS (10%)
Analysis of regulations (8%)		Process Identification (13%)	Event management (6%)
Creating IS documentation (7%)		Process Assessment (9%)	Maintaining ISMS (6%)
Monitor compliance with the law (3%)		Process Standardization (7%)	Procedures (6%)
Supervision (3%)			Establishing ISMS (3%)
Compliance testing (2%)			Safety (3%)
			Methods and management (3%)
			Responsibility for IS (3%)
			Maintaining IS (3%)

Table 11. Tasks and Activities. Summaries of the most significant subcodes

1.4 Mistakes

This category reflects the most frequently mistakes mentioned by candidates. These are:

No.	Item (Tasks and Activities)	Percentage share
1	human caused mistakes	40%
2	software caused mistakes	29%
3	lack of knowledge	17%
4	structure caused mistake	6%
5	hardware caused mistake	6%
6	collecting information without purpose	3%

Table 12. Mistakes

According to the interviews, most common mistakes are made due to the human factor. The less common mistakes are caused by software. The errors caused by the lack of knowledge are located in third place. The other reasons occur less common.

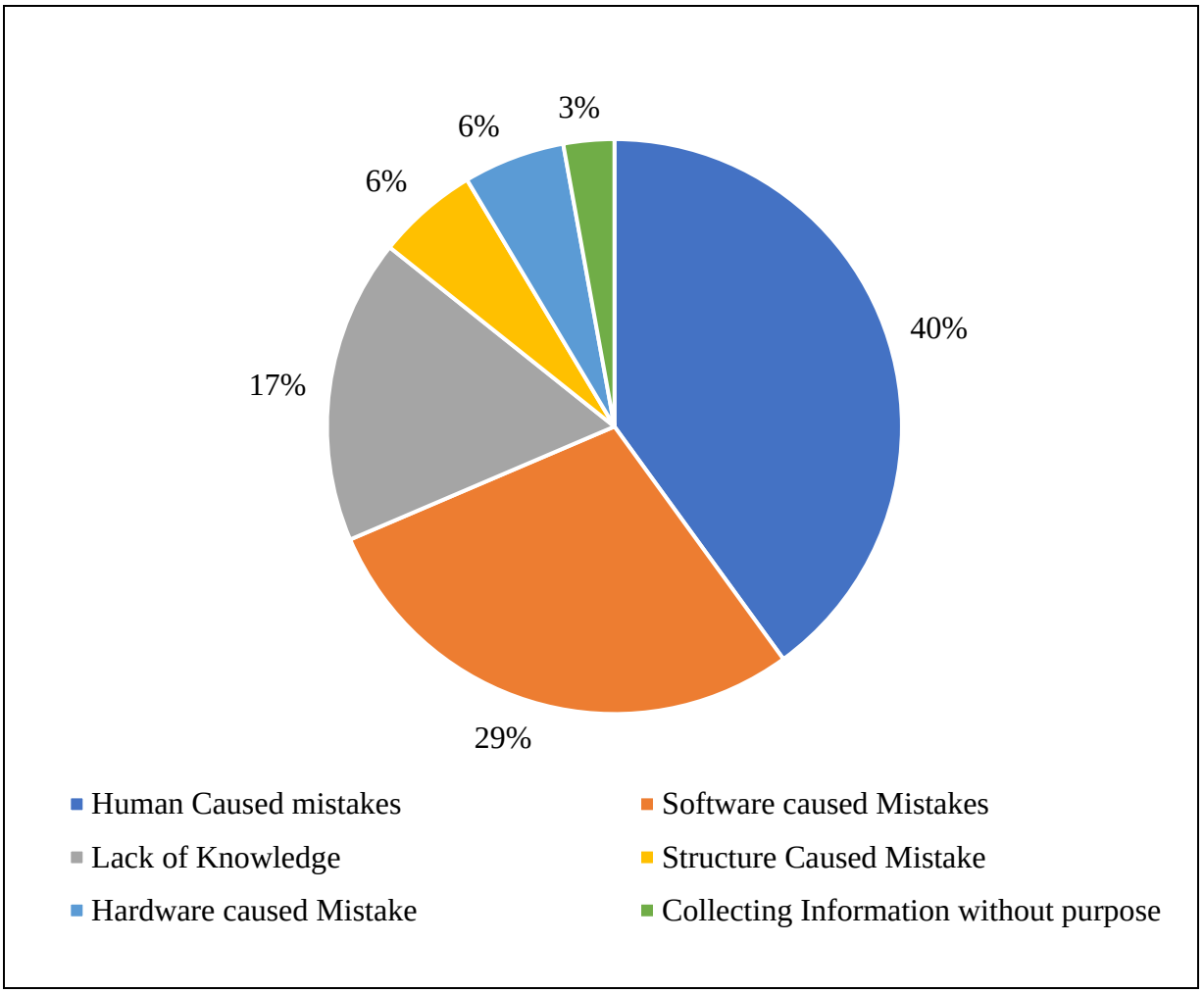

Figure 12. Mistakes

1.4.1 Human Caused mistakes

This group contains the following examples of mistakes:

No.	Item (Tasks and Activities)	Percentage share
1	Employees don't follow the standards	29%
2	Lack in communication	21%
3	Human mistakes	21%
4	Stubborness/ignorance	21%
5	Publication of private data by accident	7%

Table 13. Human Caused mistakes

We can observe almost all types of errors equally. However, we can see that many mistakes are made because of insubordination (employees don't follow the standards and Stubbornness/Ignorance).

Candidate eight from Germany experience from his company as follows:

> *"Young people didn't follow the instructions because of convenience." (DE_8)*

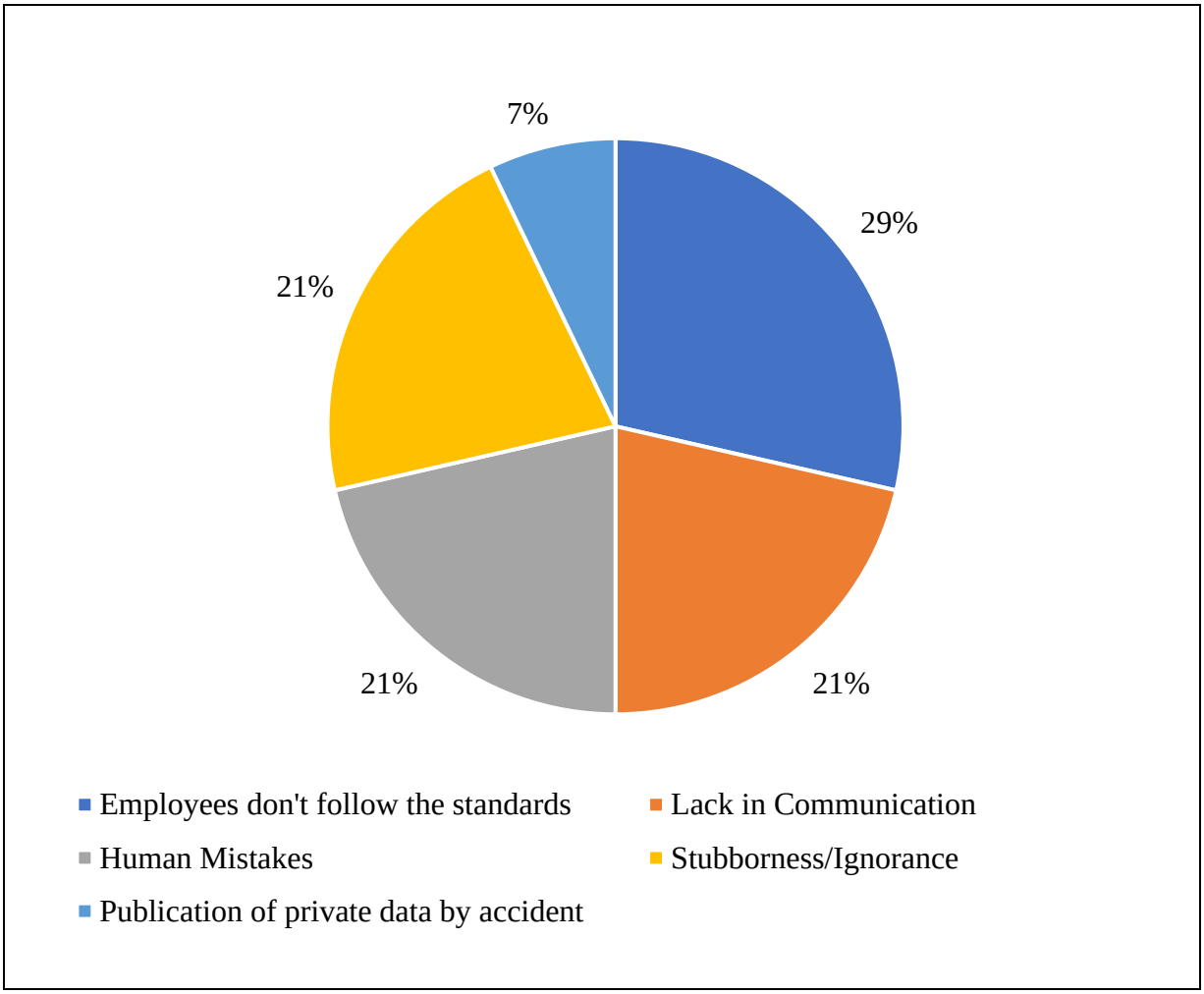

Figure 13. Human caused mistakes

1.4.2 Other types of mistake

Unfortunately, we don't have a well-detailed elaboration of other types of mistakes. However, a description of these mistakes is possible, and examples are available.

As a software caused error, candidate eight from Germany mentioned the installation of private programs. According to Candidate seven from Poland, not only private programs can be the source of mistakes, but also the usage of PC for personal purposes. Candidate two from Poland give another example, which is

> *"insignificant protection of confident data in doctors and nurses duty rooms." (POL_2)*

Candidate three from Poland think that such mistakes are caused due to many employees' access to secured data.

Mistakes caused by lack of knowledge are connected with information security as well. Candidate four from Lithuania and candidate nine from Poland confirmed this. Candidate five from Lithuania even think that mistakes generally caused because some employees don't have enough general and specialized knowledge

1.5 Attack vectors

This category's primary purpose to show the pathways of breaking through the information security system. So this category contains the following groups:

No.	Item (Tasks and Activities)	Percentage share
1	Human-caused attacks	45%
2	Configuration attacks	29%
3	Technical failure	19%
4	Application threats	6%

Table 14. Attack vectors

Most often, breaks of the information security system are caused by simple human mistakes, for example, due to easy passwords or social engineering per phone or email.

The other way to break the information security system is by using mistakes in configurations or technical failures. Potentially hackers can overload the network to access secured data, which is often happening, according to respondents' answers.

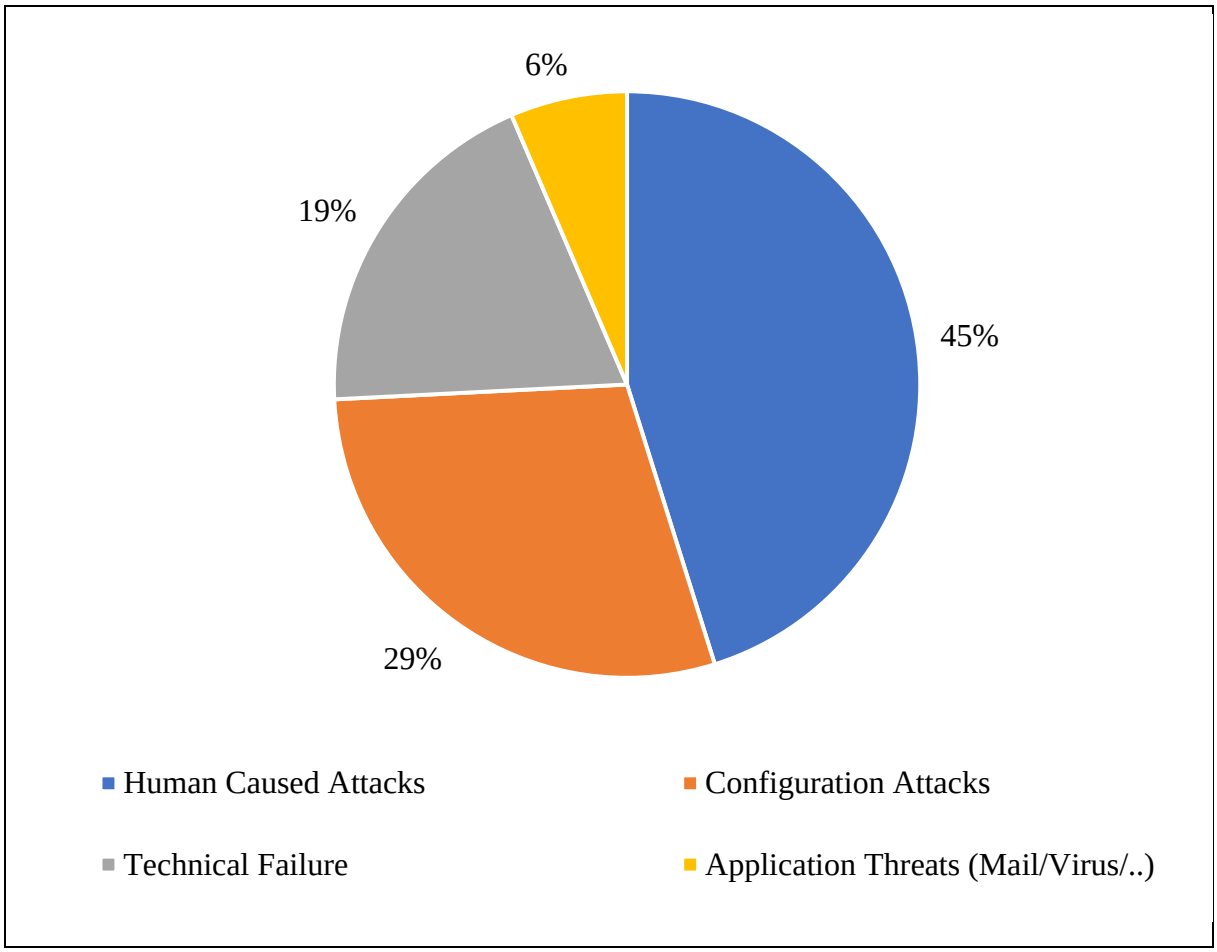

Figure 14. Attack vectors

1.6 Qualification

This category contains answers to the question about a good employee. So basically show which level of education is required for our respondents' companies. Groups in this category don't have any subcodes. We can observe here the following groups:

No.	Item (Tasks and Activities)	Percentage share
1	Higher education	48%
2	Formal education	15%
3	IT education	12%
4	Informal education	9%
5	Certificates conforming skills	6%
6	Legal education	3%
7	Language skills	3%

8	Training in data and information security	3%

Table 15. Qualification

The most requirable level of qualification, according to our interviewees, is higher education (48%). Formal education, IT education, Informal education etc., are significantly less required.

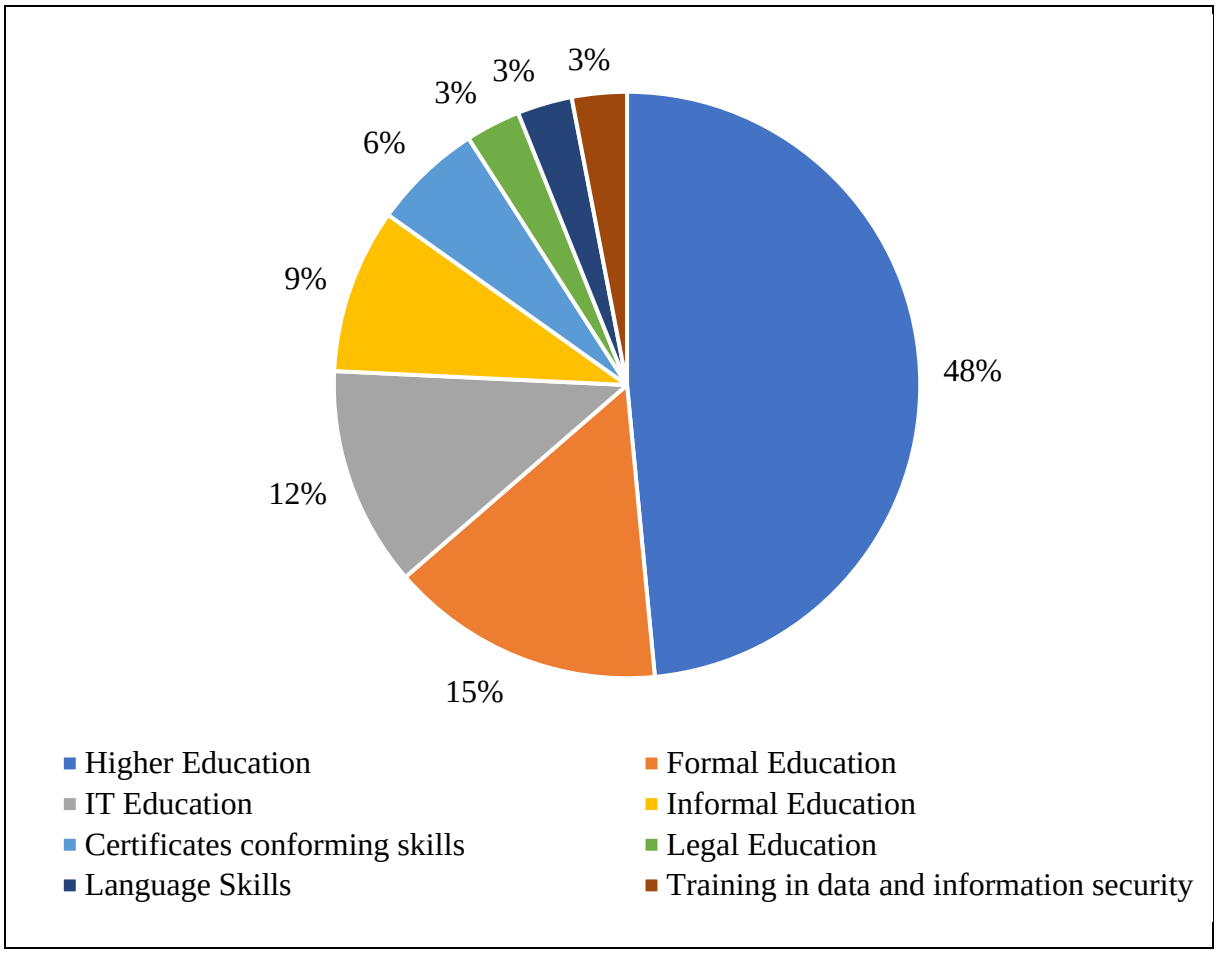

Figure 15. Qualification

2 Conclusion

At this stage of work with interviews, we can conclude that usage of MAXQDA is beneficial in this case. The elaborated code system helps to subtract non-trivial information from the massive amount of text. We can already see that most of all respondents mentioned two groups "competences critical for success" and "tasks and activities".

Among critical for success issues, candidates are usually looking for team-minded persons with good communication skills. These employees should be open-minded and independent people with analytical thinking, ready to take responsibility, and learn more. At the same time, we can observe significant demands for workers that can interact with complex equipment. Moreover, for respondents, data security issues are critical. That is why they want their employees to be familiar with data protection regulations and different ISO standards.

When we speak about possible tasks and activities, most of all, interviewees want their workers to create complacence policies for the company. They should also dedicate time to education and training. Respondents mostly want their employees to develop a plan of work, optimize it, and then implement it. Identification of the process, together with assessment and standardization, for example, are infrequently required. Nevertheless, it is crucial to examine ISMS status, implicate ISMS and create requirements for ISMS.

During interviews, candidates have been asked about potential mistakes. Most commonly, mistakes are made due to the human factor. Thus, many mistakes are made because of insubordination. The less common are mistakes caused by software. The less popular mistakes are initiated by software. They are usually connected with information security. Some candidates mentioned the installation of private programs and PC usage for personal purposes as a problem. The errors caused by the lack of knowledge are located in third place and connect with ISMS as well.

Another topic close to the ISMS is attack vectors, e.g. the pathways of breaking through the information security system. Most often, breaks of the information security system are caused by simple human mistakes, for example, due to easy passwords or social engineering per phone or email.

The other way to break the information security system occurs by using mistakes in configurations or technical failures. According to respondents' answers, potentially, hackers can overload the network to access secured data, which is often happening.

Last but not least is the required qualification level. The most requirable level of qualification, according to our interviewees, is higher education. Formal education, IT education, Informal education etc., are significantly less required.

Information Security Competences

Partner Institutions

Funded by

the Erasmus+ Programme of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

TeBeISI:

Partial Certification in the Occupational Field of Information Security

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