Co-funded by the European Union

AID project

“Exploring the AI Frontier: AI-Driven Cyber Risk Management for SMEs”
KA210-VET

International report on SMEs Digital Competence Gap Survey Results in Italy, Latvia, and Türkiye

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Name of the Project: Exploring the AI Frontier: AI-Driven Cyber Risk Management for SMEs

Acronym: AID

Proposal Number: KA210-VET-7949181B

Project Duration and start date: 15 months, 01 March 2025

Lead partner/coordinator: Baltijas Datoru akademija (BDA), Latvia

Partners:

Training 2000 psc, Italy

Muğla Sıtkı Koçman (MSKU), Türkiye

Activity: 2.2 Data Collection

Title of Deliverable: National Report on SME Digital Competence Gap Survey Results

Authors: Kylene De Angelis, Sara Caboni (Training 2000)

Reviewers: BDA, MSKU

Version 2.0

Date: September, 2025

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of contents

1. Introduction

The "Exploring the AI Frontier: AI-Driven Cyber Risk Management for SMEs" (AID) project is an Erasmus+ initiative designed to enhance the digital readiness and resilience of SMEs. By leveraging AI-driven risk assessments, the project aims to help SMEs identify, manage, and mitigate cyber threats more effectively. The project consortium includes partners from three key European countries: Italy (Training 2000 psc), Latvia (Baltijas Datoru akademija - BDA), and Türkiye (Muğla Sıtkı Koçman University - MSKU).

To achieve its objectives, the project's first step was to conduct a methodical needs analysis. A standardized survey was developed in the three partner countries to identify which digital and AI-related cybersecurity skills are most relevant to SMEs. The survey instrument asked respondents to rate the importance of various competences across cybersecurity, cyber risk management, and data analysis using a 5-point Likert scale, where 1 represented "Not important at all" and 5 represented "Critically important."

A total of 41 responses were collected in Latvia, 31 in Italy and 37 in Türkiye for a total of 109 SMEs across the three countries responded to the AID surveys.

This report synthesizes the findings from national surveys carried out in Latvia, Italy and Türkiye for each section of the surveys described below and will draw overarching conclusions to guide the development of the AID Competence Map and training materials.

The report is structured as follows:

Section 1: Demographics

This section provides an overview of the participating Small and Medium-sized Enterprises (SMEs), summarising responses related to company size and sector distribution.

Section 2: Identification of high-priority competences

This section compares the most important competences across three competences areas: cybersecurity, risk management, and data analysis.

Section 3: **Perceived barriers**

This section compares the importance and presence of priority competences across the three partner countries.

Section 4: Conclusion and recommendation

This final section presents the main conclusions drawn from the survey findings and provides recommendations on the development of the AID Competence Map

2. Section 1 - Demographics

This section summarizes the company size (micro, small, medium and other) and sector distribution of the SMEs participating to the AID surveys in partner countries.

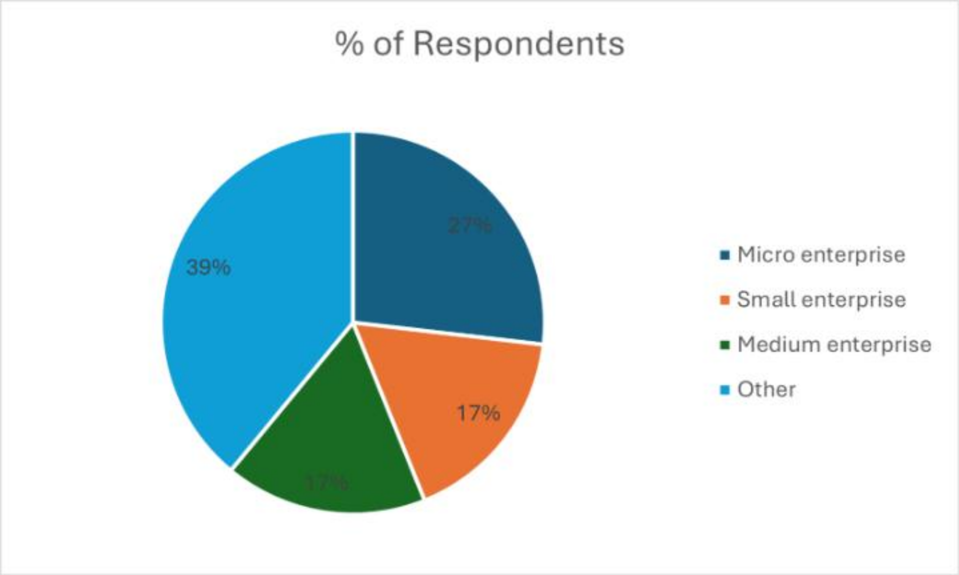
A total of 41 responses were gathered in Latvia, of which 25 were identified as SMEs. This group consisted of 11 micro, 7 small, and 7 medium-sized enterprises. A significant portion of respondents (13) came from the ICT and Digital Services sector. As reported, this portion may influence the overall perspective on digital competence.

The Italian sample (31 responses) was predominantly composed of very small businesses, with micro-enterprises (fewer than 10 employees) accounting for 61% of respondents and small enterprises (fewer than 50 employees) making up another 26%. The main industry sectors represented were Commerce/Retail/Hospitality, ICT and Digital Services, Manufacturing, and Professional Services, providing a diverse cross-section of the Italian SME economy.

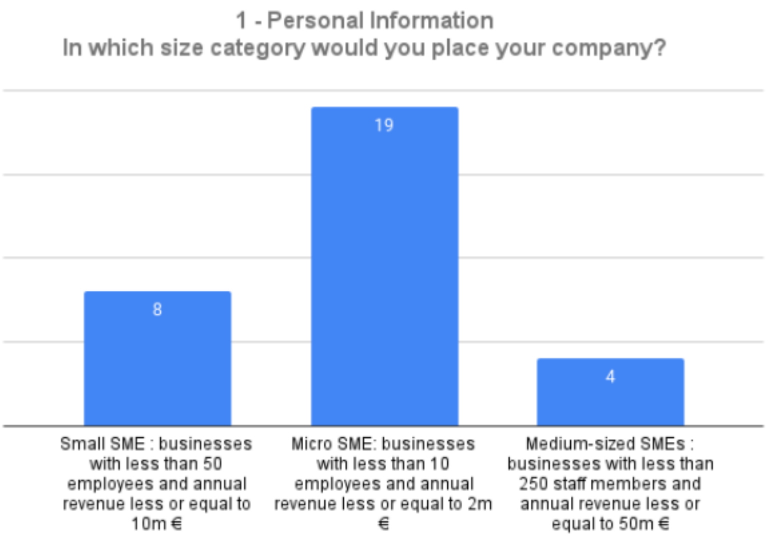
The Turkish sample (37 responses) was dominated by micro-enterprises (51.4%) and small enterprises (35.1%), reflecting a business landscape of smaller organizations. The core concentration of respondents came from the Manufacturing/Industry and ICT/Digital Services sectors. The following section presents the main findings by survey topic.

2.1 Company size distribution in partner countries

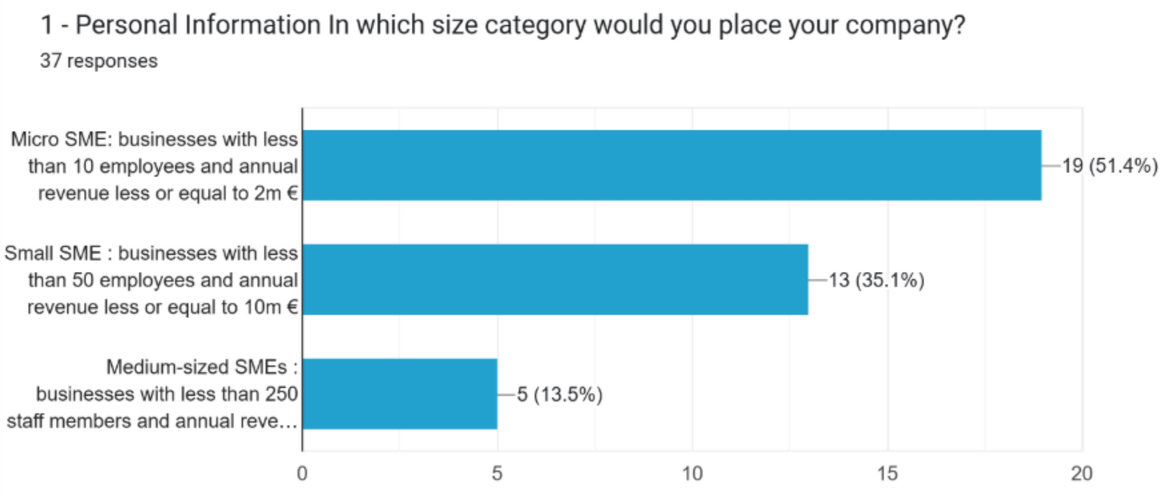
Latvia



Italy



Turkey



2.2 Sector Distribution

Latvia

Enterprises identified themselves as representing various business activities, namely:

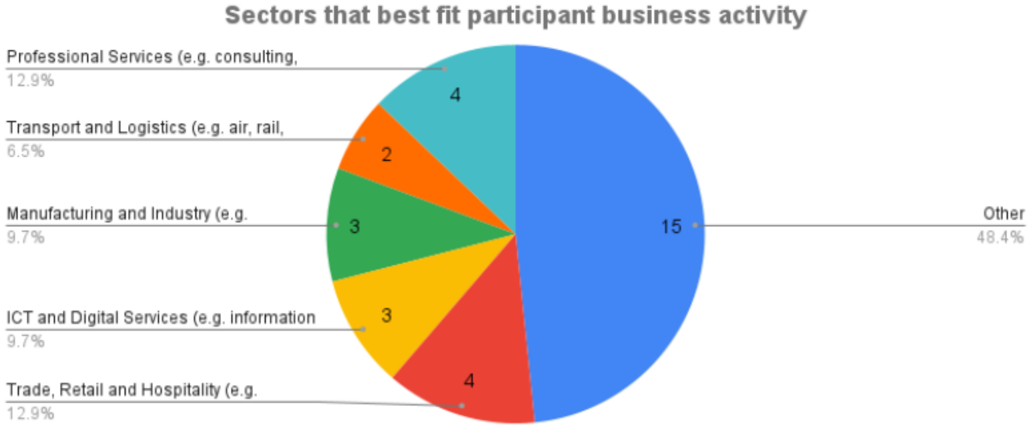
- Manufacturing and Industry - 3,
- Energy and Utilities - 0,
- Transport and Logistics - 1,
- Finance and Insurance - 2,
- Health and Life Sciences - 0,
- ICT and Digital Services - 13,
- Professional Services - 5,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

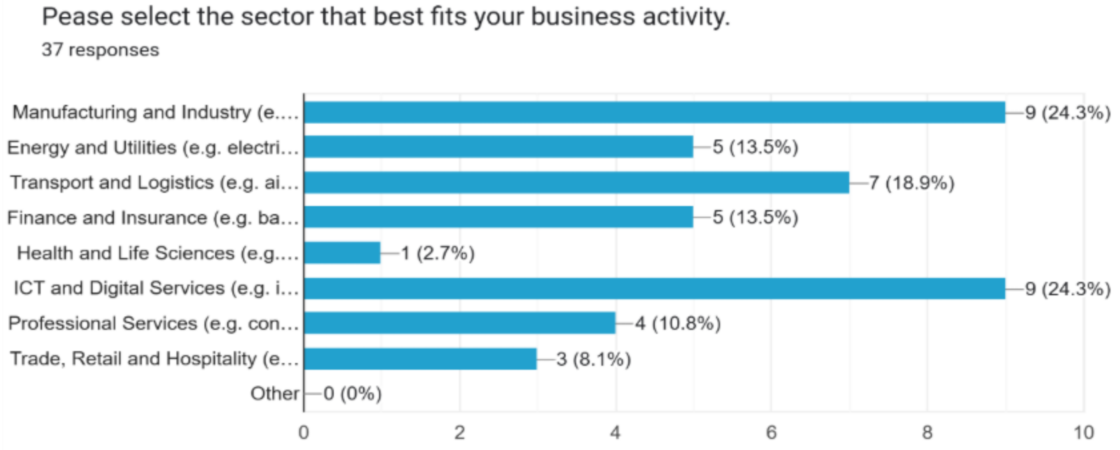
- Trade, Retail and Hospitality - 3,
- Other - 14.

Of the respondents that chose “Other” 2 were education and 6 were public service organizations.

Italy



Turkey



3. Section 2 - Identification of high-priority competences

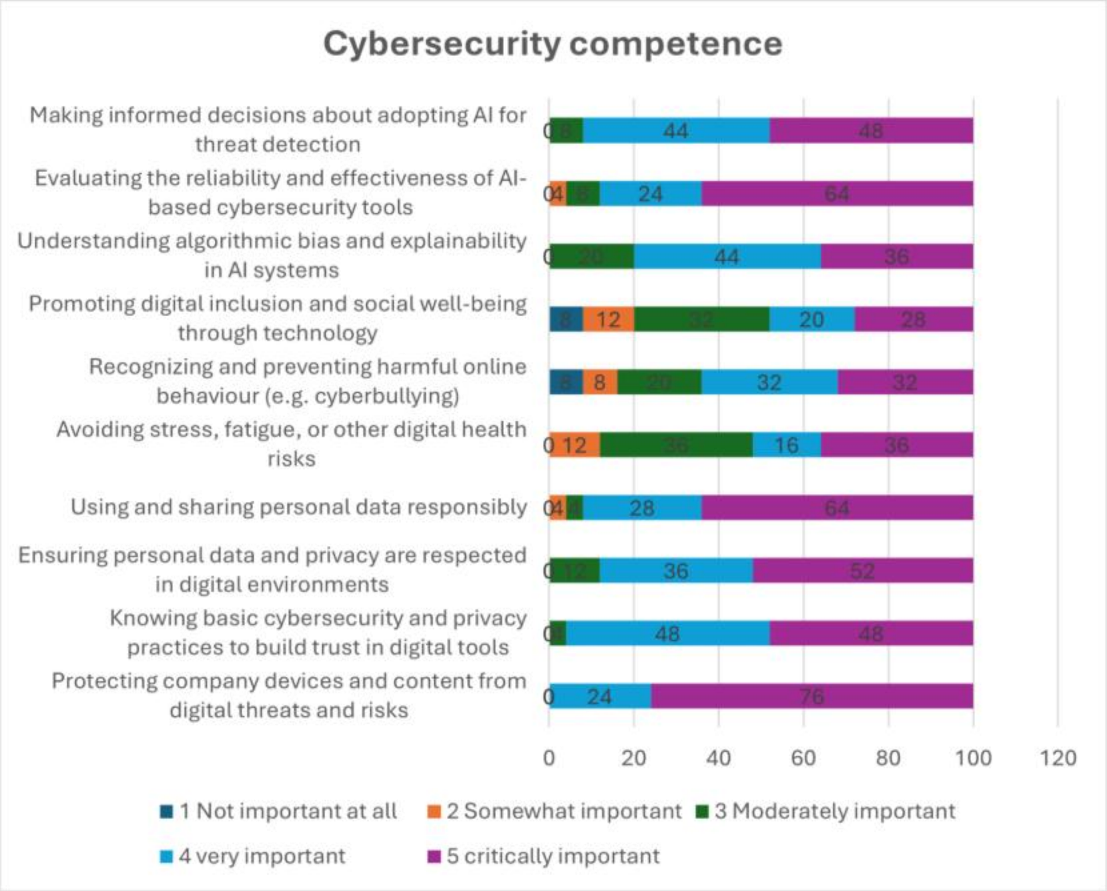
This section presents the survey data from Italy, Latvia, and Türkiye to pinpoint a core set of digital competences that are universally rated as "Very important" (a rating of 4) or "Critically important" (a rating of 5).

The following competences emerged as top priorities in the national surveys:

3.1 Area 1 - Cybersecurity Competences

Latvia

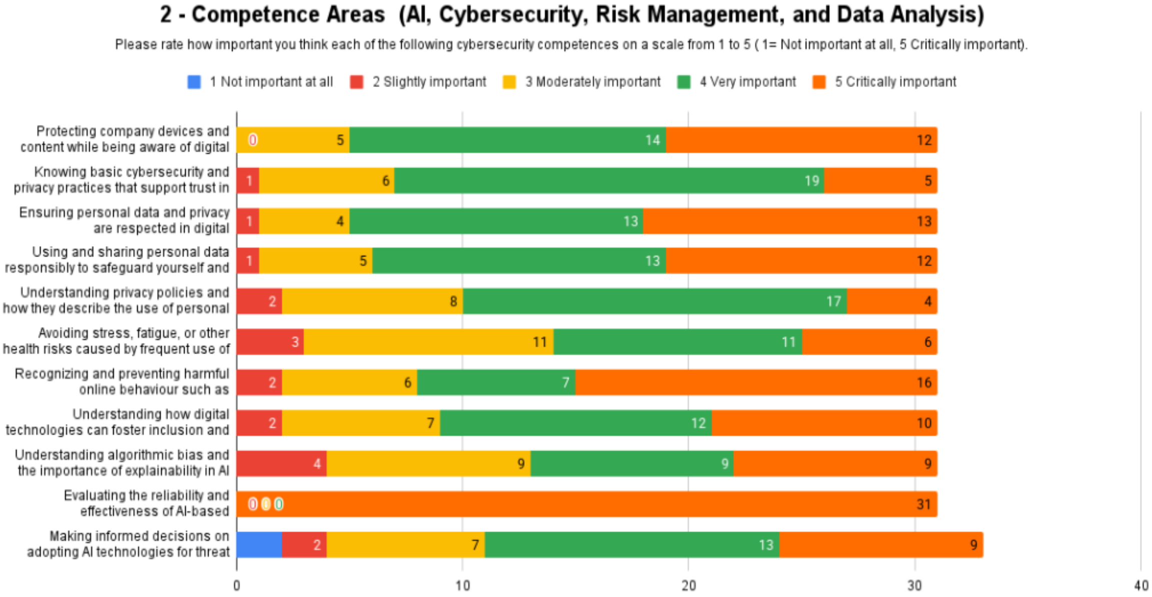
Foundational skills like protecting company devices and content (rated critically important by 76% of respondents) and using and sharing personal data responsibly (64%) were paramount. Notably, evaluating the reliability and effectiveness of AI-based cybersecurity tools was also rated as critically important by 64% of SMEs.



Italy

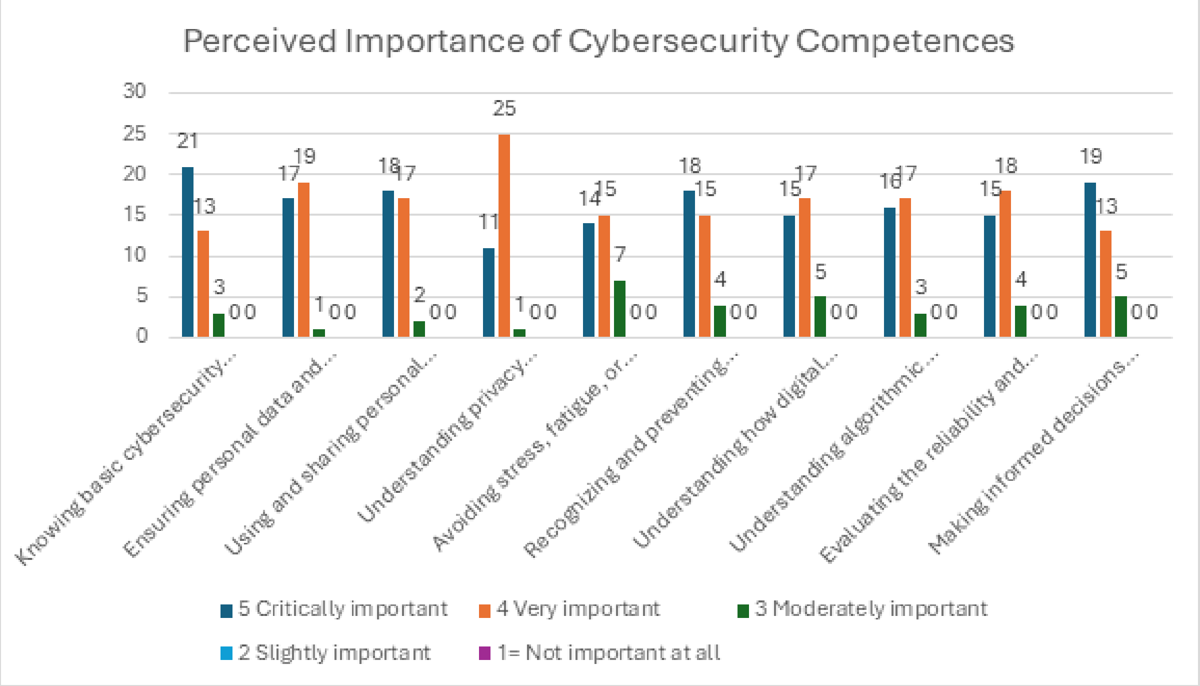
SMEs view cybersecurity as critically important. A standout finding was the unanimous consensus regarding emerging technologies: all 31 Italian respondents rated the competence of evaluating the reliability and effectiveness of AI-based systems at the highest possible level of importance.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Turkey

In the domain of cybersecurity competences (Area 1), Turkish respondents placed highest priorities (5- Critically important) on knowing the basics of cybersecurity (21 responses) and making strategic decisions for their businesses (19 responses). They also highlighted the need for protecting company devices and content and ensuring personal data and privacy are respected.

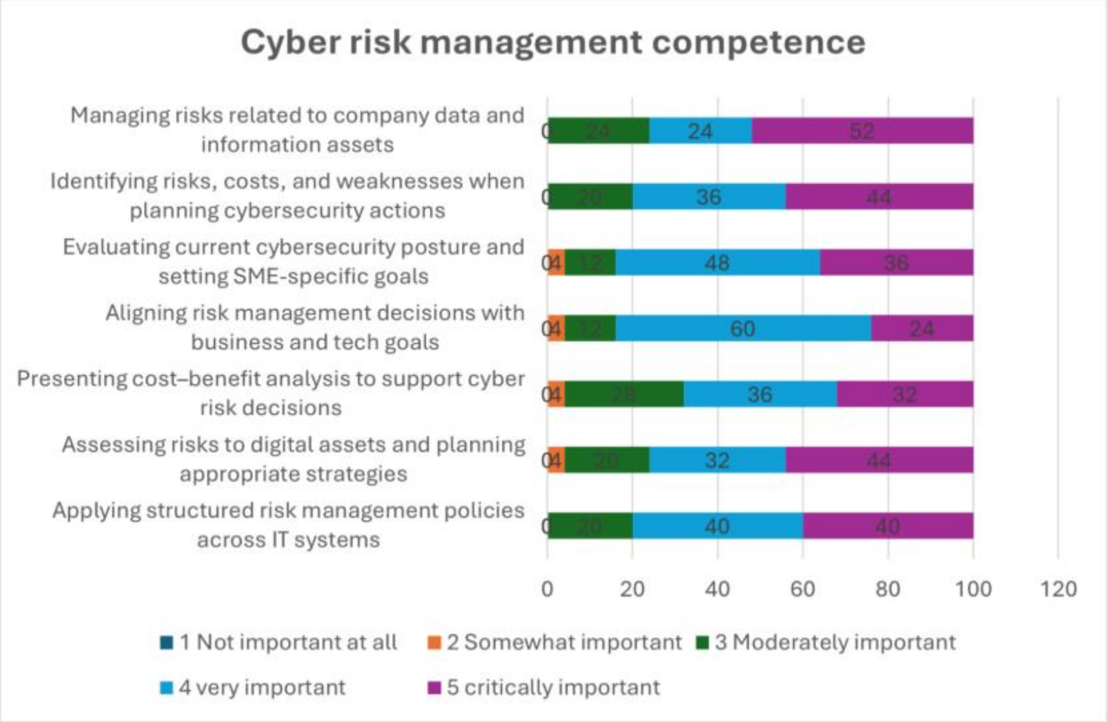


3.2 Area 2 - Cyber Risk Management Competences

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

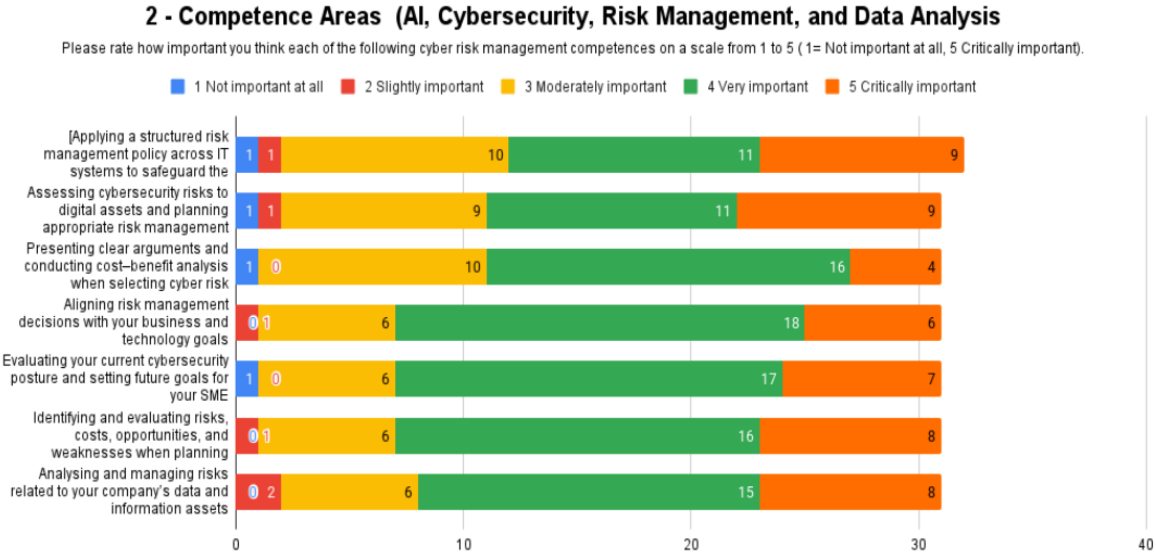
Latvia

While all skills in this domain were deemed important, respondents rated them as "moderately important" more frequently than the skills in the cybersecurity category, suggesting a slightly lower perceived urgency.



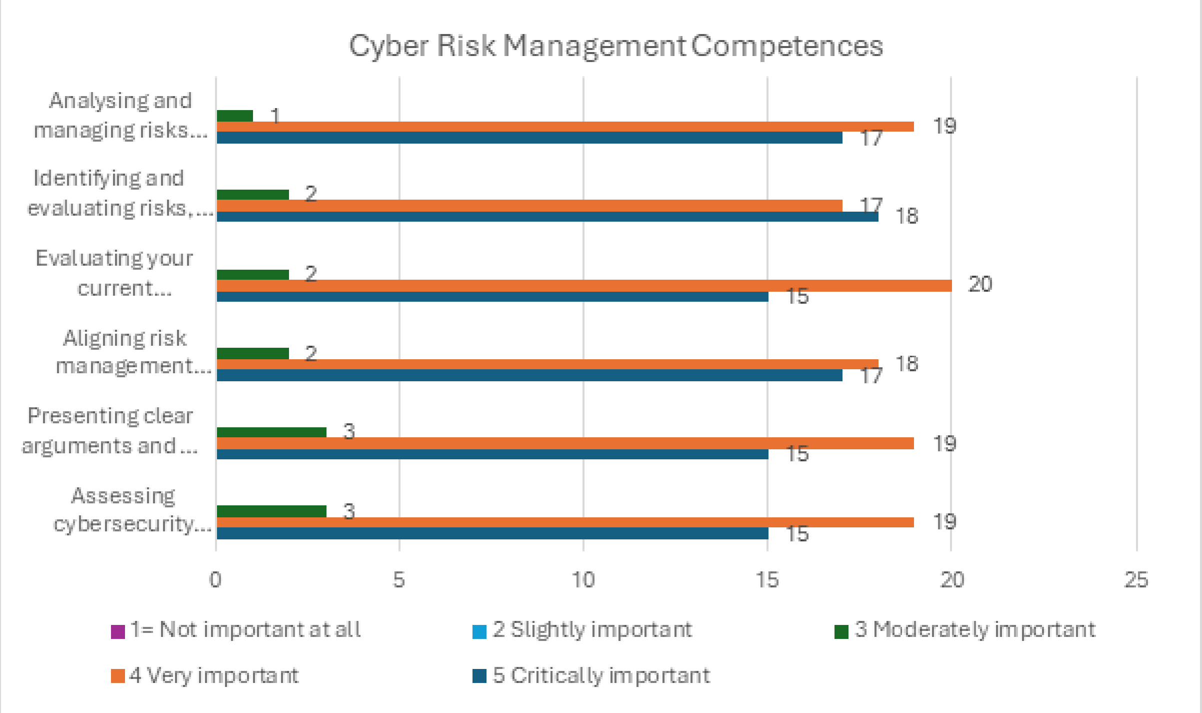
Italy

The most valued skills in this area were aligning risk management decisions with business and technology goals and evaluating the current cybersecurity posture to set future objectives.



Turkey

The skills rated as most critically important were identifying and evaluating risks, costs, opportunities, and weaknesses (20 responses); aligning risk management with business and technology goals (19 responses); and analysing and managing risks related to company data.

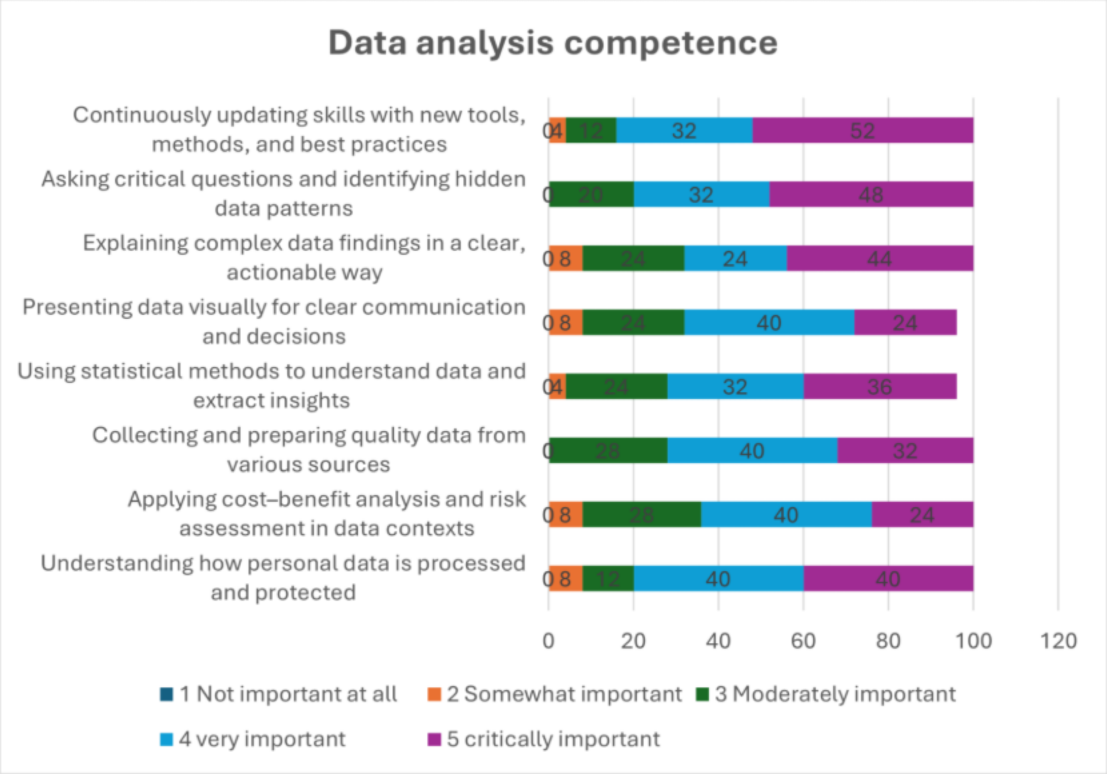


3.3 Area 3 - Data Analysis Competences

Latvia

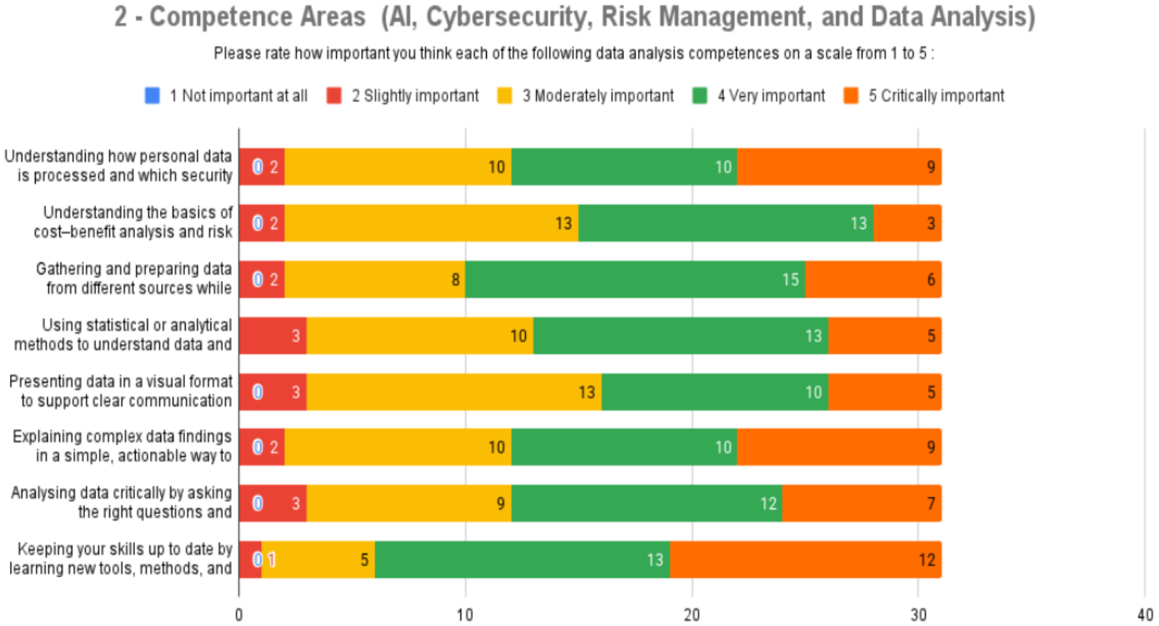
The most valued competencies were continuously updating skills (84%) and understanding how personal data is processed and protected (80%)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



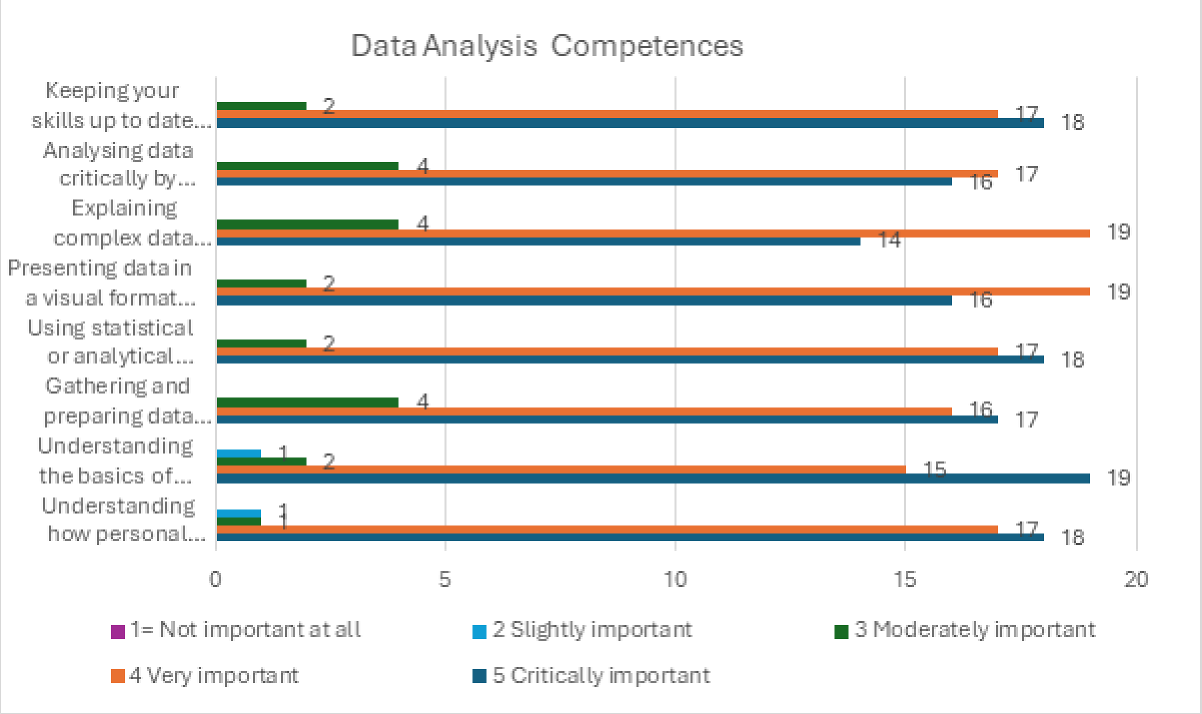
Italy

Respondents showed a strong emphasis on the need for continuous professional development, with keeping skills up to date with new tools and methods identified as a top-rated competence. Moreover, being able to explain complex data finding was also considered very important.



Turkey

Keeping skills up to date by learning new tools, methods, and techniques was the top-rated competence, reflecting a universal agreement on the central role of continuous learning in data analysis.



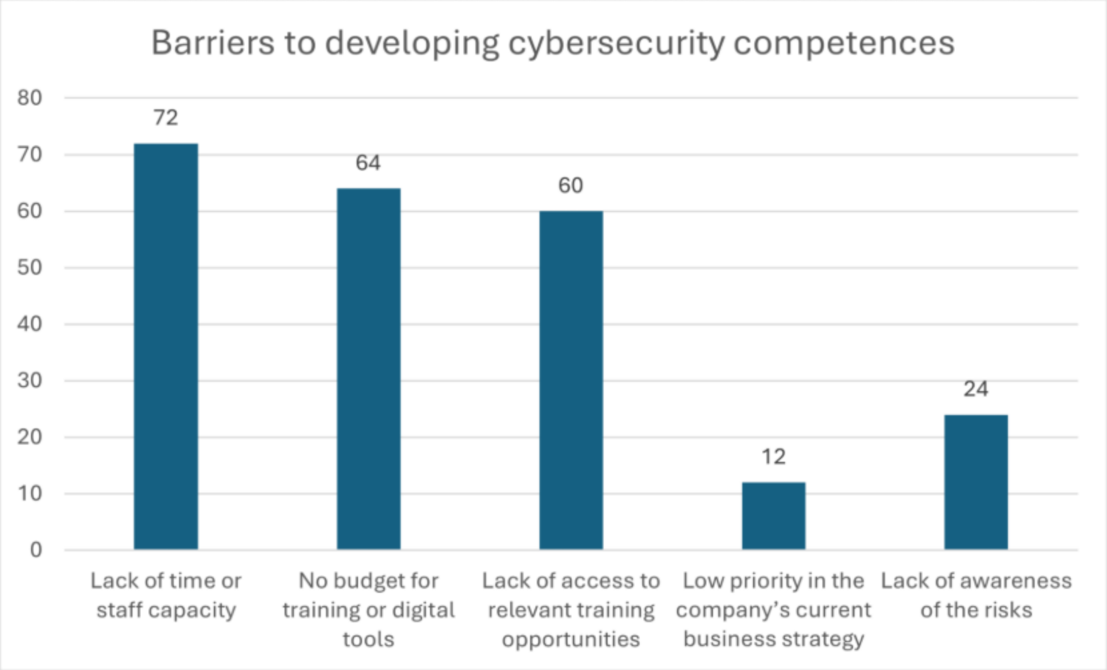
4. Section 3 - Perceived barriers

Latvia

Latvian SMEs identified resource-based constraints as the main obstacles to improving their cybersecurity posture:

- Lack of time or staff capacity (72% of respondents)
- No budget for training or digital tools (64%)
- Lack of access to relevant training opportunities (60%)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Italy

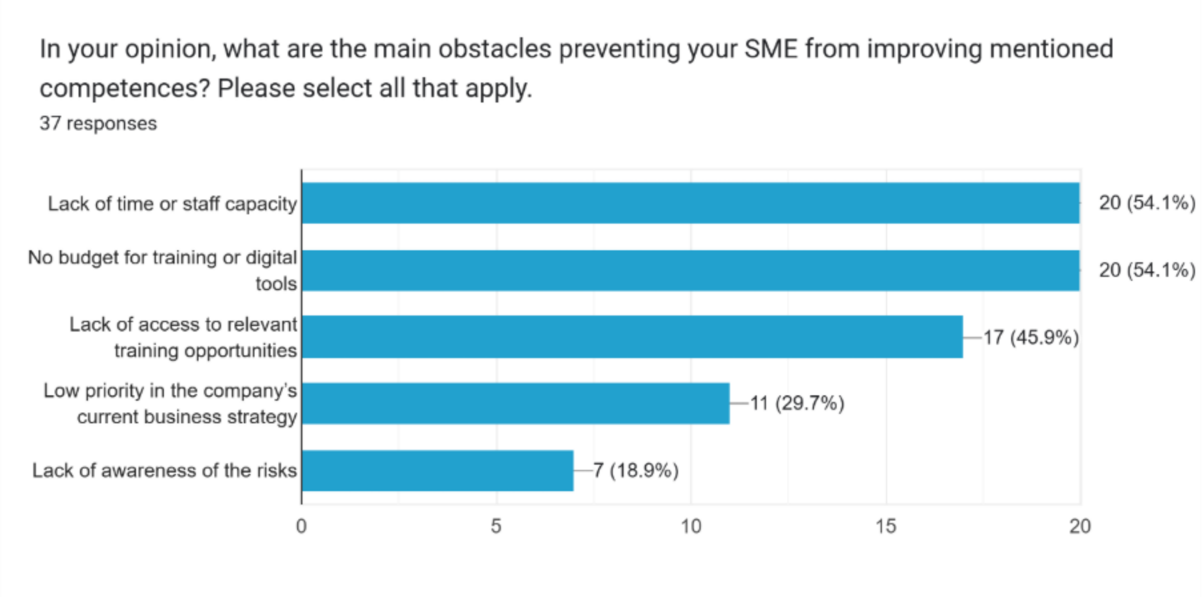
The top reported barriers for Italian SMEs were:

- Lack of time or staff capacity (72%)
- Insufficient funding for training or digital tools (64%)
- Lack of access to relevant training opportunities (60%)

Turkey

The primary obstacles reported by Turkish SMEs were:

- Lack of Time or staff capacity (54.1%)
- No budget for training or digital tools (54.1%)
- Lack of access to relevant training opportunities (45.9%)
- Low priority in the company's current business strategy (29.7%)



In your opinion, what are the main obstacles preventing your SME from improving mentioned competences? Please select all that apply.
37 responses

5. Section 4 - General comments and preferred topics

5.1 Latvia

The Latvian report concludes that SMEs recognize the importance of all three competence areas but place the highest priority on cybersecurity fundamentals and AI reliability. The primary barriers to progress are overwhelmingly resource-based, stemming from a lack of time, budget, and access to training, rather than a lack of awareness of the risks.

The respondents were also asked if they had any specific topics for the future training of cybersecurity and AI topics. The answers were free-form and very individual. Some of the topics mentioned were the following:

- Recognizing the cybersecurity risks,
- Recognizing the limitations of AI tools,
- Risks specific to the use of AI tools,
- Data security and confidentiality.

5.2 Italy

The findings from Italy conclude that while SMEs are aware of the critical importance of digital skills, their ability to act is severely hampered by internal resource constraints. There is a clear and expressed need for practical, application-focused training that accommodates these limitations. Moreover, the following preferred topics were identified by SMEs are:

- Fundamentals of Artificial Intelligence

- Ethics, responsibility, and awareness in AI usage
- Prevention and protection
- Strategies for Digital Innovation
- Sector-Specific and Industry Applications

5.3 Turkey

The Turkish report concludes that while there is a high level of awareness regarding the importance of digital skills, SMEs are constrained by internal barriers. They require practical, affordable, and action-oriented training focused on business continuity and employee awareness to translate this awareness into capability. The preferred topics were:

- Business continuity planning,
- Cyber hygiene and employee awareness,
- Privacy, compliance and governance practices
- AI- strategies in business operations

6. Conclusion and recommendations

This report has provided a comprehensive analysis of the digital competence needs of SMEs in Italy, Latvia, and Türkiye. Despite geographical and market differences, there is a strong international consensus on the digital competences required by SMEs to enhance digital resilience. This shared prioritization of foundational cybersecurity, strategic risk management, and practical, ethics-driven data analysis provides an evidence-based foundation for the AID Competence Map and the development of the training material.

In fact, based on the survey results, SMEs are aware of the digital risks they face and the importance of developing new competences to address them. However, a significant gap exists between this high level of awareness and their internal capacity to act. This "awareness-capability gap" points to a critical need for accessible, practical, and resource-sensitive support. To be effective, training programs and policy initiatives must be tailored to the operational realities of small enterprises, helping them bridge the divide between knowing what to do and having the resources to do it.

The following recommendations are proposed to guide the development of the AID Competence map and training materials:

1. **Prioritize foundational competences**: The focus must be on fundamental cybersecurity practices (e.g., device protection, data privacy), strategic risk management (e.g., alignment with business goals), and practical data analysis (e.g., upskilling, secure data processing).

2. **Critical thinking skills of AI-based systems:** Beyond foundational skills, SMEs identified the evaluation of AI-based systems as a top-tier critical competence. This finding was especially pronounced in Italy, where there was unanimous agreement on its importance. This shared priority demonstrates that European SMEs are not just reacting to current threats but are actively grappling with the reliability and effectiveness of next-generation technologies
3. **Integrate practical learning**: The focus must be on competence that support cost-effective, practical strategies in SMEs, such as developing simple, non-technical incident response checklists as requested by survey respondents, and highlight accessible tools that SMEs can implement immediately to achieve tangible improvements.
4. **Integrate case studies**: The AID Competence map should be designed to explicitly link technical skills with strategic business functions. This can be achieved by developing case studies where implementing multi-factor authentication (a technical skill) directly prevents a business-crippling ransomware attack (a strategic outcome). This approach will help foster an integrated culture of cybersecurity that permeates the entire organization, rather than remaining isolated within an IT department.

By adopting these evidence-based recommendations, the AID project will create relevant, and highly valued resources for SMEs of different sectors. This will not only meet the expressed needs of its direct beneficiaries but also contribute significantly to strengthening the overall digital resilience of the SME ecosystem across Europe.

7. References

1. AID-National Report on SME Digital Competence Gap Survey Results - Latvia
2. AID-National Report on SME Digital Competence Gap Survey Results - Italy
3. AID-National Report on SME Digital Competence Gap Survey Results - Turkiye