



AID project

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

KA210-VET

Competency Research for Digital Adaptation
and Growth in SMEs

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 akadēmija (BDA), Latvia

Partners:

Training 2000 psc, Italy

Muğla Sıtkı Koçman (MSKU), Türkiye

Activity Number: 2.1 Competency Research and Analysis

Title of Deliverable: Competency Research for Digital Adaptation and Growth in SMEs

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

Reviewers: BDA, MSKU

Version 4v_Final

Date:07/09/2025

Table of contents

Sommario

| | |
|--|----|
| Table of contents..... | 3 |
| Introduction:..... | 4 |
| 1.1 General Description..... | 4 |
| 1.2 Target Groups..... | 4 |
| 1.3 Scope..... | 5 |
| 2 Research Methodology..... | 5 |
| 2.1 Literature Review..... | 6 |
| Sources..... | 6 |
| 2.2 Market Analysis..... | 9 |
| Latvia..... | 9 |
| Italy..... | 11 |
| Turkiye..... | 15 |
| 2.3 National Policy framework supporting AI integration into SMEs..... | 16 |
| Latvia..... | 16 |
| Data protection and trustworthy AI..... | 17 |
| Italy..... | 19 |
| Turkiye..... | 20 |
| 2.4 Challenges Faced by SMEs in Adopting AI Technologies in Our Countries..... | 24 |
| Latvia..... | 24 |
| Italy..... | 26 |
| Turkiye..... | 27 |
| Conclusion..... | 27 |
| Annex..... | 29 |
| SME Digital Competence Gap Survey..... | 29 |
| References..... | 32 |

Introduction:

1.1 General Description

The Erasmus+ “Exploring the AI Frontier: Artificial Intelligence Driven Cyber Risk Management for SMEs” (AID) project aims to enhance the digital readiness, resilience, and capabilities of Small and Medium Enterprises (SMEs) by leveraging AI-driven risk assessments. The goal is to help SMEs identify and mitigate cyber threats effectively, fostering a resilient and adaptable cybersecurity environment.

The AID project focuses on the evolving and complex landscape of cyber threats confronting businesses in today’s digital world. As organizations increasingly rely on digital technologies, their exposure to cyber-attacks intensifies, putting both their data and operations at risk. This initiative seeks to deliver a practical, AI-powered solution designed to help companies proactively identify, manage, and adapt to these threats, thereby safeguarding their security and ensuring operational continuity in the digital age.

Securing funding for this project is essential because AI enables superior threat detection, quicker response times, and deeper insights into cyber risks. The AI system will continuously learn and evolve, empowering businesses to stay one step ahead of cybercriminals. Built with adaptability in mind, this solution is suitable for organizations of all sizes, granting access to advanced cybersecurity capabilities that were once out of reach for smaller players.

In addition, the project supports wider goals such as boosting trust in digital technologies and creating a safer online environment for enterprises. Strengthening cyber resilience not only protects individual companies but also reinforces the overall digital economy. Investment in this project will play a vital role in building a secure digital future, fostering economic growth, and enhancing stability across the digital landscape.

1.2 Target Groups

Small and Medium-Sized Enterprises (SMEs) are the principal beneficiaries of the project. The project adapts its competence mapping, training programs, and toolkit to meet the specific cybersecurity requirements of SMEs in the participating countries.

The list of target groups is presented below:

1. **SME Employees:** Employees in SMEs across different industries obtain benefits from the project's training and competency initiatives. These programs improve their cybersecurity skills and competencies.
2. **SME Owners and Managers:** The owners and managers of SMEs are key to cybersecurity-related decision-making. The project provides them with the necessary understanding to make informed cybersecurity decisions and represent leadership.
3. **Vocational Educational and Training Institutions:** Institutions providing cybersecurity courses and training programs may use the project's resources to strengthen their curriculum and provide students with practical, current knowledge.



4. Policymakers and Regulators: Policymakers and regulatory bodies in the partner countries benefit from the project's results and best practices, which may help the development of cybersecurity policies and regulations.
5. Community and Industry Networks: Networks dedicated to community engagement and teamwork, focused on SMEs and cybersecurity, may use the project's platform for knowledge dissemination and promoting a culture of cybersecurity awareness.
6. Professional Associations and NGOs: Associations relevant to IT, cybersecurity, and SMEs may use the project's materials into their member development and campaigns for change

The purpose of this research is present the current digital landscape and SME needs in Latvia, Italy and Turkey.

In a second phase, a survey will be used to identify which digital and AI-related cybersecurity skills are most relevant to European SMEs across different sectors.

Together with a survey, the aim is to offer a clear understanding of areas requiring enhancement. This ensures that the AID Competence map is customized to the distinct requirements of SMEs, facilitating the development of essential skills for efficient digital adaptation and growth.

1.3 Scope

The AID project focuses on the development of a Competence Map and a tailored toolkit for SMEs, specifically targeting AI-driven cybersecurity competencies. The scope of this research is identifying and classifying critical AI-driven cybersecurity skills and knowledge necessary for SMEs.

The project is designed to be customised to the common needs of SMEs across various sectors, ensuring practical applicability and effectiveness in enhancing cybersecurity measures.

The following are the 2 main project objectives:

- **Objective 1:** Define Key AI-Driven Cybersecurity Competencies for SMEs

To identify and structure the core AI-based cybersecurity skills and knowledge areas essential for SMEs to effectively detect, prevent, and respond to cyber threats.

- **Objective 2:** Develop and Pilot a Practical Support Toolkit for SMEs

To create a tailored, user-friendly toolkit that supports SMEs in strengthening their AI-driven cybersecurity capabilities, and to deliver pilot training sessions that demonstrate its effective use.

2 Research Methodology

This section outlines the methodological approach adopted to identify and analyze the digital and AI competencies crucial for Small and Medium-sized Enterprises (SMEs).

The methodological approach started from a research that utilized a quantitative, cross-sectional survey design to gather data from small and medium-sized enterprises (SMEs) across various industries in Italy, Turkey and Latvia. The same survey instrument was developed around key themes including digital competencies, readiness for artificial intelligence integration, cybersecurity awareness, risk management practices, and perceived obstacles to digital skills development.

Data collection was carried out through an online questionnaire distributed via multiple channels such as partner organization mailing lists, SME networks, professional associations, and social media platforms like LinkedIn. Participation was voluntary and anonymous, targeting SME representatives such as owners, managers, or relevant employees.

A purposive, non-probability sampling method was adopted to specifically engage SMEs that met the European Union's SME classification criteria and were willing to share insights related to their digital and cybersecurity competencies. Although no strict quotas were imposed, efforts were made to ensure representation across different sectors and company sizes.

The quantitative data collected were analyzed using descriptive statistics to identify patterns and trends based on company size, industry sector, self-reported skill levels, and perceived barriers to skill development. In addition, qualitative responses from open-ended survey questions were examined thematically to uncover recurring issues and deeper insights, thereby enriching the understanding of the challenges SMEs face in enhancing their digital capabilities.

The methodology also encompasses a literature review and market analysis to gather primary data.

2.1 Literature Review

The objective of this literature review is to establish a comprehensive theoretical foundation for understanding the current state of digital and AI competencies among Small and Medium-sized Enterprises (SMEs). This review aims to identify existing knowledge, gaps, and best practices in the field, with a focus on the DigComp 2.2 framework as the main source. The review also incorporates insights from past projects of the partnership on cybersecurity and practical experiences.

Sources

The literature review draws from a diverse range of sources, categorized as follows:

1. The Digital Competence Framework for Citizen (DigComp)

The Digital Competence Framework for Citizens¹ is primary reference for understanding digital competencies, including specific competencies related to the use of artificial intelligence. The DigComp2.2 framework serves as a compass for digital competencies, providing a structured approach to understanding and developing these skills across various domains.

- **Information and Data Literacy:** The ability to identify, locate, retrieve, store, organize, and analyze digital information, and to evaluate its relevance and purpose. With AI, this includes understanding how AI can process and analyze large datasets, and the ethical considerations involved.
- **Communication and Collaboration:** The ability to communicate in digital environments, share resources through online tools, and collaborate effectively using digital tools. AI integration involves using AI-driven communication tools and understanding their impact on collaboration.
- **Digital Content Creation:** The ability to create and edit digital content in different formats, and to understand how copyright and licenses apply. AI tools can assist in content generation, and understanding their ethical use is crucial.
- **Safety:** The ability to protect devices, content, personal data, and privacy in digital environments. This includes cybersecurity practices and understanding the ethical implications and safety concerns related to AI.
- **Problem Solving:** The ability to identify digital needs and resources, solve conceptual problems through digital means, and use digital tools to innovate processes. AI can be applied to solve complex business problems and enhance decision-making processes

In this case, DigComp2.2 guidance was particularly significant in the realm of cybersecurity, which falls under the "Safety" competence area (Area 4).

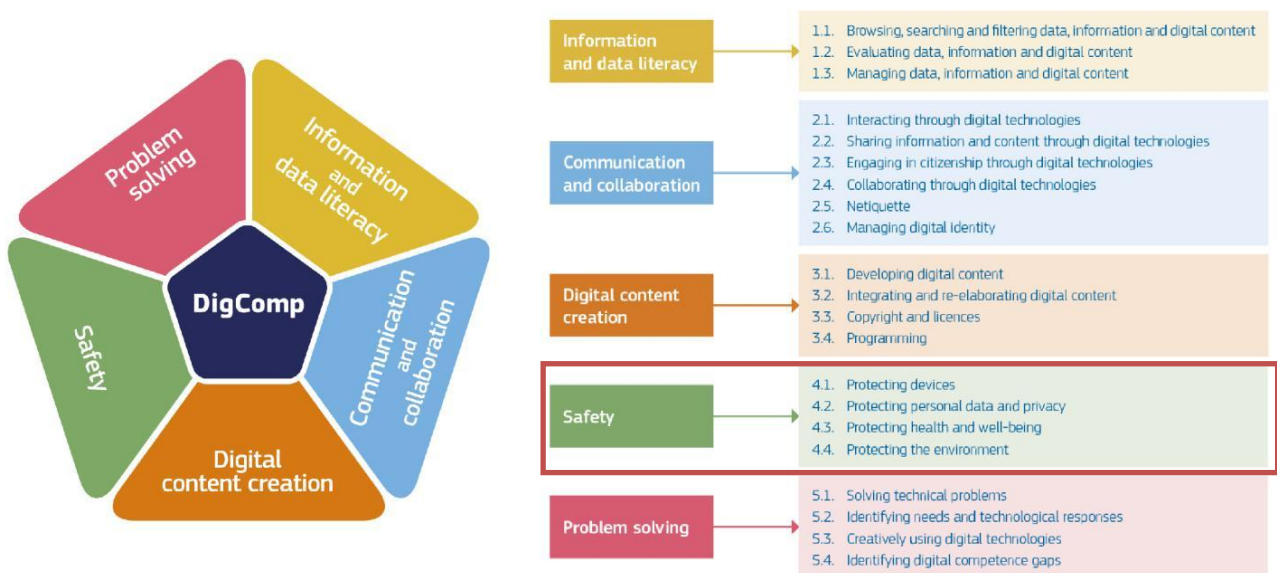


Figure 1 DigComp2.2 overview. Adapted from the Digital Competence Framework for Citizens. Publications Office of the European Union.

¹ Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens—With New Examples of Knowledge, Skills and Attitudes (EUR 31006 EN). Publications Office of the European Union. <https://doi.org/10.2760/115376>



Co-funded by
the European Union



2. Past European Projects

The Erasmus + Project – REDucing the CYBERsecurity Management Skills Gap in SMEs (No. 2018-1-LV01-KA202-046987).

The REDucing the CYBERsecurity Management Skills Gap in SMEs² Erasmus+ project aimed to address the cybersecurity skills gap in SMEs by providing targeted training and resources. Key findings, best practices, case studies, and tools developed from this project are reviewed. In particular, the consortium analyzed and considered the definition of the Risk Manager profile as outlined in the project.

The Cybersecurity Risk Manager plays a key role in shaping and maintaining cybersecurity strategies, policies, and plans to ensure alignment with organizational goals and regulatory requirements. This role leads risk management efforts, advising senior leadership on risk levels and security posture, while supporting decision-making through cost-benefit and risk analyses.

The Cybersecurity Risk Manager collaborates closely with cybersecurity and IT teams to assess, quantify, and mitigate cyber risks, develop threat criteria and metrics, and guide risk treatment strategies. They also contribute to supplier risk evaluations, challenge existing risk assessments, and support cybersecurity awareness initiatives across the organization. Key competencies include information security strategy, risk management, process improvement, and ICT quality and security management.

² <https://edu.unibit.bg/course/index.php?categoryid=103&lang=en>

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.



REDucing the CYBERsecurity Management Skills Gap in SMEs
(No. 2018-1-LV01-KA202-046987)

Security roles

Cybersecurity Risk Manager

Work Role Description

Participate in cybersecurity plans, strategy and policy development and maintenance to support and align with organizational cybersecurity initiatives and regulatory compliance. Leads risk management activities.

Main Responsibilities:

1. Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture
2. Evaluate cost/benefit, economic, and risk analysis in decision-making process
3. Collaborate with cybersecurity personnel on the security risk assessment process to address compliance and risk mitigation
4. Research internal and external cybersecurity risks to develop quantification models and impact values.
5. Work effectively with IT operational teams and business units to facilitate cyber risk assessment and risk management processes, and provides guidance on risk treatment strategies
6. Establish threats criteria and risk metrics to be applied in cybersecurity risk prioritization processes.
7. Contributes to monitoring, testing as well as review and constructively challenges IT operational teams and business units on their assessment of cyber risks, including challenging on risk mitigation and management responses
8. Evaluate, analyze and establish suppliers' monitoring service and set cybersecurity risk criteria for appropriate use.
9. Participate in development and implementation of cybersecurity awareness program in enterprise

Key competences (6): D.1. Information Security Strategy Development, D.2. ICT Quality Strategy Development, D.11. Needs Identification, E.3. Risk Management, E.5. Process Improvement, E.8. Information Security Management

Figure 2 Competence profile of the Risk manager from the REDCyber Erasmus+ project 2018-1-LV01-KA202-046987

2.2 Market Analysis

Latvia

Cabinet of Ministers of Republic of Latvia has approved an important policy planning document on the development of the strategy of cybersecurity in Latvia in form of “Guidelines for Digital Transformation for 2021-2027” approved by Cabinet of Ministers Order No. 490 of 7 July 2021.”³

³ Cabinet of Ministers Order No. 490 of 7 July 2021 “On Guidelines for Digital Transformation for 2021-2027”.
<https://likumi.lv/ta/id/324715>

which is a response to a NIS2 directive of European Union on high common level of cybersecurity across EU⁴.

As a result “The Cybersecurity Strategy of Latvia 2023 – 2026” has been developed⁵. This document has 5 main directions of action listen with regards to improving the cybersecurity at enterprises in Latvia:

- Enhancing Cybersecurity Management,
- Promoting Cybersecurity and Strengthening Resilience,
- Public Understanding, Education, and Research,
- International Cooperation and Rule of Law in Cyberspace,
- Prevention and Combating Cybercrime.

The risks of cybersecurity have become more relevant because of geopolitical situation and the ties of Latvia to EU and NATO.

According to Cyber Incident Response Institution (Cert.LV) which prepares regular reports of the situation in cyberspace in Latvia, country’s cyberspace experiences an increased threat of cyber incidents that happen because of human factor, dependency on digital technologies, device vulnerability and the rising popularity of AI driven solutions⁶. The report of Latvian cyberspace for Q2 2025 indicates that there are several important risks experienced by companies:

- Fraud, in particular phishing campaigns pretending to represent government agencies,
- Human factor (not using 2FA and being vulnerable to phishing attacks),
- Threats of ransomware attacks and business e-mail compromise (BEC) attacks,
- Targeted DDOS attacks against critical infrastructure,
- Raise of AI in cyber threats and disinformation,
- Vulnerabilities associated with Internet of Things (IoT).

Recent fraudulent activities in Latvia have been related to scammer impersonating government institutions, fake investment and cryptocurrency schemes, using seasonal or public events as a background for phishing attempts.

In recent research conducted in Latvia to measure the cybersecurity levels of companies in Latvia some conclusions have been summarized:

- 38% of companies think that ICT solutions are important for the growth of the company but 46% of companies believe that the digital skills of their employees are good enough.
- 34% of companies are worried about loses in business due to the increasing number of cyber security threats.

⁴ NIS2 directive, available <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555>

⁵ The Cybersecurity Strategy of Latvia 2023 – 2026, <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/latvia-cybersecurity-strategy-2023-2026>

⁶ <https://cert.lv/en/2025/08/cert-lv-activity-review-q2-2025>



- 52% of companies are not even sure if the law of National Cyber Security is relevant to their companies⁷. As part of the strategy small, medium and large companies in the Republic of Latvia are planned to be involved in targeted training on the topics of digital, robotic and automation skills, digital transformation and innovation. These programs are implemented with the involvement of Latvia's European Digital Innovation Hubs (EDIHs)⁸.

This leads to a conclusion that although there is an initiative in reducing the cybersecurity risks in enterprises in Latvia, the companies would benefit from a systematic approach to develop a description of cybersecurity competences fit for the employees of the small and medium enterprises.

Italy

Drawing on insights from the "Sistema Informativo Excelsior - Le competenze digitali 2024"⁹ report, below is a comprehensive analysis of the demand for digital skills within Italian enterprises in 2024.

1. Digital Transition and Enterprise Investments

- About 66.8% of Italian companies invested in at least one digital transition area in 2024, a slight increase from the previous year.
- Larger companies (500+ employees) and medium-large companies (50-499 employees) show the highest investment rates (around 88-89%).
- Investments focus mainly on high-speed connectivity, cloud solutions, big data analytics (42.6%), cybersecurity (42.5%), and data management tools (38.2%).
- Integration of technologies within business models and organizational processes is a growing trend.

2. Adoption of Artificial Intelligence (AI)

- AI adoption varies by company size: 35.2% of firms with 500+ employees and 9.8% of micro enterprises use AI.
- AI is predominantly used in economic and financial management (over 50% of AI-using firms) and marketing/e-commerce (35.4%).
- Main AI applications include cybersecurity (22.1%), document analysis (18.3%), CRM customer assistance (14.9%), and language processing (13.5%).

3. Demand for Digital Skills

- For 2024, companies plan to hire 5.5 million new employees with digital skill requirements.
- Digital skill requirements include:
 - Internet technologies and digital communication tools (62.6% of new hires).

⁷ <https://dih.lv/lv/jaunumi-un-pasakumi/jaunumi/10-svarigakas-atzinas-par-ikt-un-kiberdrosibu-no-uznemumu-vaditajiem>

⁸ <https://www.digitallatvia.lv/digital-skills-development>

⁹ https://excelsior.unioncamere.net/sites/default/files/pubblicazioni/2024/Competenze_Digitali_2024.pdf

- Use of mathematical/informatics languages and methods (49.3%).
- Application of digital technologies to innovate and automate processes (37.5%).
- High-level digital skills are mostly requested for managerial and highly specialized roles.
- Even lower qualification levels require basic digital skills, notably in the use of communication tools.

4. Skill Mix Requirements

- About 767,000 planned entries (around 14% of total digital-skilled hires) require a mix of digital skills ('e-skill mix'), combining two or more of the three key digital skill areas.
- The highest demand for multi-skill digital profiles is among executives and highly specialized professions.
- IT, research & development, and finance/accounting areas show the highest incidences of e-skill mix demand.

5. Recruitment Difficulties and Skill Mismatch

- 60.1% of companies investing in digital transformation experience difficulties in recruiting professionals with needed digital skills, up from 58.1% in 2023.
- Manufacturing shows the highest recruitment difficulties (62%), followed by the services and construction sectors.
- Difficulty increases with enterprise size; companies with 500+ employees report the highest hiring challenges.
- Main reasons for recruitment challenges include lack of suitable candidates (36.9%) and inadequate skill levels (23.3%).
- Geographically, recruitment difficulties are higher in Northern and Central Italy, especially in regions like Trento, Bolzano, and Friuli-Venezia Giulia.

6. Education and Training Pathways

- Proficiency in digital skills correlates strongly with education level. Graduates, especially in STEM (math, informatics, engineering), are in higher demand.
- ITS Academies, emerging post-diploma technical institutes, play a crucial role in providing advanced technical digital skills aligned with labor market demand.
- Secondary education diplomas in ICT and telecommunications are highly valued, but demand varies by field.
- Professional qualifications show diverse digital skill demand, with high expectations in electronics and graphic/cartotecnics sectors.

7. Professional Roles Most in Demand

- The most requested digital profiles for digital investments include Digital Marketing specialists, Business Analysts, ICT Account Managers, Social Media Managers, Database Administrators, Application Developers, ICT Consultants, and Data Scientists.
- Difficulty in recruiting is highest for profiles such as Information Engineers, Mathematicians, Statisticians, Construction Technicians, Industrial Designers, and Programmers.

Despite being one of Europe's largest economies, Italy is lagging behind its neighbors when it comes to the adoption of artificial intelligence (AI) in business. According to a recent report from

ISTAT (2025), the country's national statistics bureau, only 8% of Italian companies utilized AI technology last year—a figure noticeably lower than that of France, Spain, and especially Germany, where nearly one in five enterprises have embraced AI.

This limited adoption reflects broader challenges in Italy's digital landscape. Digital literacy remains insufficient across the population, with less than half (45.8%) of Italians aged 16 to 74 possessing basic digital skills. This is significantly below the EU average of 55.5% and far from the ambitious European goal of 80% digital proficiency by 2030. The situation is particularly stark in the Mezzogiorno region, encompassing Italy's southern areas and islands, where only about a third of residents demonstrate even basic digital competencies.

These technological shortcomings are compounded by a wider economic and demographic crisis. Italy's growth has long been sluggish, and in recent years, many young, educated Italians have chosen to seek opportunities abroad rather than stay in their home country. ISTAT data shows a significant rise in the number of graduates aged 25 to 34 leaving Italy in 2023, with 21,000 departures marking a 21.2% increase compared to the previous year. Over the past decade, the net loss of qualified young workers has reached nearly 100,000.

The economic outlook remains uncertain. Italy's government, led by Prime Minister Giorgia Meloni, recently downgraded its growth forecast for 2025 from 1.2% to a mere 0.6%, citing global trade tensions and economic headwinds. Meanwhile, preliminary figures indicate modest economic expansion in the first quarter, with growth of 0.3% compared to the prior quarter.

In this context, Italy faces a critical crossroads. Bridging the digital skills gap and fostering wider AI adoption could be key to revitalizing its economy. Yet, without concerted efforts to improve education, infrastructure, and retain talent, Italy risks falling further behind its European peers in the technological race.

Italy's economy is deeply rooted in its small and medium-sized enterprises (SMEs). With over 4 million SMEs—more than any other EU country—they collectively employ around 13 million people and contribute over 65% of the nation's added value. Beyond their economic role, these businesses are vital cultural and industrial stewards. They preserve the craftsmanship and identity of the "Made in Italy" brand, and their success in sectors such as advanced manufacturing is evident in their significant share of national exports, standing at 53%, well above the European average of 40%.

Despite their diversity in size, sector, and regional location, Italian SMEs face similar challenges as they attempt to navigate digital transformation. These include a lack of digitally skilled workers, difficulty in accessing investment capital, and uncertainty about the legal and operational implications of adopting new technologies. Addressing these shared obstacles is critical to avoiding a widening gap between large and small firms and between different regions of the country.

Encouragingly, many SMEs are already moving forward. According to data from the SMEs Digital Innovation Observatory of the Politecnico di Milano, more than 60% of Italian SMEs are investing

in digitalisation. One-third of them increased their investment between 2022 and 2023, focusing on areas such as digital systems, ICT software and services, and digital content.

The Ministry of Enterprises and Made in Italy is actively supporting this transition. Through the National Recovery and Resilience Plan, public funds have been directed toward strategic supply chains, technology transfer initiatives, clean technology adoption, and the financing of startups. This strategy is complemented by a network of 50 innovation and technology transfer centres across Italy. These hubs offer experimental labs, tailored training, and mentoring to guide businesses - particularly SMEs - through the digitalisation process.

Financial tools like the 'Transition 5.0' programme also play a key role. It provides tax credits to companies investing in digitalising their industrial processes, linking both digital and green objectives to foster a more productive and sustainable business model. At the same time, efforts are underway to build stronger connections with local communities and business associations, ensuring that information about available resources and technologies is widespread and accessible. Site visits and ongoing dialogue with entrepreneurs allow the government to better understand and respond to real business needs.

On the international front, the challenges facing Italian SMEs mirror those encountered by their global peers. Digitalisation, if not approached inclusively, risks becoming a barrier instead of a bridge. That is why international collaboration is essential. As Chair of the OECD D4SME Global Initiative, Italy is pushing for the democratisation of digital tools - making them not only available but usable by all SMEs, regardless of size or sector.

Italian SMEs continue to lag behind large companies in adopting artificial intelligence, despite a surge in national investment. In 2024, AI spending in Italy rose by 58%, reaching €1.2 billion. Yet among small businesses, only 7% have initiated AI projects, and just 15% of medium-sized ones have done the same, according to the Politecnico di Milano. Most of these efforts focus narrowly on operational efficiency, suggesting a cautious and limited approach.

A survey by Confalpi and the Labour Consultants Foundation reinforces this picture. While 47.6% of SMEs report being curious about AI and 29.1% show strong interest, only 11% have implemented AI-based solutions. If companies involved in pilot projects or training are included, the number rises to 29.7%, still well below the level needed to drive real transformation.

The reasons go beyond budget limitations. Many SMEs lack mature data management practices, relying on fragmented or ad hoc analysis that makes it difficult to build effective AI models. A well-organized, continuously updated data infrastructure is essential, but remains uncommon. Compounding this is a significant skills gap: nearly 48% of SMEs cite a lack of technical expertise as the main obstacle to adoption. Recruiting AI specialists is challenging, and internal training initiatives are rare.

Cultural resistance also plays a role. Employees often view AI as a threat, creating internal friction. Without leadership committed to change and clear communication, new technologies are unlikely to be embraced. *Technical infrastructure adds another hurdle.* Many SMEs still operate with legacy systems unsuited for AI workloads, while cloud solutions - though more accessible - are underused

due to perceived complexity or cost. Legal uncertainty adds to the hesitation. About 12% of SMEs cite unclear regulation as a deterrent, particularly in the context of evolving European frameworks like the AI Act.

Despite these challenges, more than half of SMEs say they plan to invest in AI over the next three years. To do so effectively, companies need to start with training - both for key technical roles and the broader workforce. This helps build internal capability and fosters a company-wide data culture. Early efforts should focus on narrow, well-defined use cases where AI can deliver immediate value.

Turkiye

The Turkish artificial intelligence market is undergoing swift expansion, bolstered by governmental efforts and rising private sector demand. Current forecasts indicate that the whole market would attain roughly USD 2.2 billion by 2029, exhibiting an annual growth rate of about 13%. In this context, the generative AI sector is emerging as an exceptionally dynamic domain. Projected to be valued at over USD 128 million in 2024, it is anticipated to increase to over USD 540 million by 2033, indicating an annual growth rate of nearly 17%.

Although this growing potential, adoption rates among companies remain low. According to data from the Turkish Statistical Institute (TÜİK), just 4–5% of enterprises indicate the utilisation of AI technologies. Companies with over 250 employees are significantly more likely to implement AI, exceeding 20%, whereas micro and small organisations have limited adoption rates, between 3–6%. Among enterprises not already utilising AI, the main obstacle stated is the absence of internal expertise, followed by higher costs and limited access to infrastructure.

Adoption is predominantly focused in the manufacturing, finance, healthcare, and retail sectors. Manufacturing firms are starting experiments with predictive maintenance and process automation, whereas financial institutions are employing AI for fraud detection, customer analytics, and risk modelling. Healthcare providers are experimenting with AI technologies for diagnostics and hospital administration, while retail organisations are showing growing interest in recommendation systems and chatbots. An additional domain of swift advancement is generative AI for Turkish-language content, wherein local entrepreneurs and academic institutes are developing models tailored to the nation's linguistic and cultural framework.

A variety of factors are driving this industry forward. The National Artificial Intelligence Strategy (2021–2025) and accompanying 2024–2025 Action Plan prioritise the establishment of an optimal environment for AI, especially for SMEs. Wider challenges associated with Industry 4.0, digitalisation, and the expansion of e-commerce are compelling enterprises to investigate AI solutions. The expansion of cloud computing infrastructure is simultaneously reducing entry barriers for SMEs, while the demand for localised language tools presents distinct potential for domestic companies.

Nonetheless, difficulties persist substantially. Elevated implementation expenses, particularly for smaller enterprises, constrain adoption. The deficiency of proficient AI engineers and data

scientists hinders the advancement of internal solutions, while infrastructural and connectivity discrepancies between urban centres and rural areas increase regional inequalities. Regulatory uncertainty presents a further obstacle: despite the introduction of a Draft Artificial Intelligence Law in 2024, the definitions of risk categories, certification processes, and liability obligations remain inadequately defined. Cultural barriers, notably the limited awareness of AI's business advantages among SME owners, limit experimentation and investment.

The future prospects for Türkiye's AI market are favourable. Growth will be propelled by strategic public assistance, global partnerships, and the swift advancement of generative AI. Small and medium-sized enterprises that can utilise government initiatives (KOSGEB, TÜBİTAK), engage in employee skill enhancement, and partner with universities and research institutions have the capacity to lead this change.

2.3 National Policy framework supporting AI integration into SMEs

Latvia

Latvia's policy framework for AI adoption in SMEs is anchored in overarching digital and innovation strategies (Digital Transformation Guidelines 2021–2027, National Industrial Policy Guidelines 2021–2027, and RIS3), complemented by targeted funding (RRF/ERDF instruments via ALTUM and LIAA), capability-building infrastructure (European Digital Innovation Hub Latvia, AI Centre Lab, and the forthcoming National Artificial Intelligence Center), and regulatory guardianship aligned with the EU AI Act (market-surveillance authorities and the Data State Inspectorate). Together these elements create an enabling environment that lowers adoption risks and costs, expands access to expertise and testbeds, and links AI uptake to Latvia's broader productivity, export, and innovation goals.¹⁰

Strategic and policy foundations

1. Digital Transformation Guidelines 2021–2027 (DTG)

Latvia's DTG is the country's umbrella strategy for digitalisation. It sets directions across five pillars (skills and education; security and trust; telecom access; digital transformation of the economy and public administration; and ICT innovation and research), positioning AI as a lever for public- and private-sector productivity. For SMEs, the document signals a long-term commitment to digital uptake and provides the policy basis for complementary programmes and investments.

2. National Industrial Policy Guidelines 2021–2027 (NIP)

The NIP frames industrial competitiveness and innovation, reinforcing RIS3 priority domains (incl. ICT) and calling for a coherent legal and financial environment that accelerates business R&D and technology

¹⁰ Latvian Digital Transformation Guidelines for 2021-2027 – Accellation of Digital Capacities for Future Society and Economy

diffusion. It explicitly links horizontal enablers - skills, research, IP, and finance - to firm-level technology adoption, which includes data analytics and AI. ¹¹

3. Research and Innovation Strategy for Smart Specialisation (RIS3)

RIS3 guides public support toward Latvia's competitive strengths, including "Information and Communication Technologies," with cross-cutting relevance for AI. Its goal is to "enhance innovation capacity and establish an innovation system that promotes and supports technological progress," thereby creating pathways (grants, competence centers, cluster initiatives) that SMEs can use to co-develop or adopt AI solutions with universities and labs.¹²

4. National AI strategy and public-sector AI leadership

Latvia released a national AI strategy framework in 2020 to "promote the uptake and growth of AI in the whole economy," highlighting actions on skills, adoption in public and private sectors, legal/ethical frameworks, data ecosystems, and infrastructure. This policy emphasis is visible in practical roll-outs such as state-backed language technologies (machine translation, speech tools) and virtual assistants used across government - capabilities that spill over to SMEs through APIs, ecosystems, and talent flows. ¹³

Regulatory and governance environment

EU AI Act implementation and market surveillance

Latvia's implementation of the EU AI Act is progressing with designated market-surveillance authorities, including the Data State Inspectorate (DVI), the Consumer Rights Protection Centre, the Health Inspectorate, and the Bank of Latvia/Ministry of Economics for sectoral oversight. This clarifies supervisory lines for AI risk classes, conformity assessment, and post-market monitoring - reducing legal uncertainty for SMEs planning to deploy or develop AI systems for EU markets.

Data protection and trustworthy AI

DVI actively shapes national practice on data protection in AI contexts and participates in European forums on AI's privacy implications. SMEs benefit from clear regulatory guidance and supervisory engagement on topics such as use of synthetic/AI-generated data and DPIAs for automated processing.

Open data, interoperability, and data governance

Latvia's "Open by default" agenda (National Open Data Strategy, 2019) and ongoing OGP commitments foster reusable public data - with machine-readable publication mandated by regulation - supporting data-driven SME services and AI training/validation. Interoperability reviews further align public data infrastructure with EU data-space initiatives, bolstering trustworthy data access for SMEs.

¹¹ GUIDELINES ON NATIONAL INDUSTRIAL POLICY OF LATVIA 2021-2027

¹² Research and Innovation Strategy for Smart Specialization (RIS3)

¹³ Minister Inga Bērziņa discusses the introduction of AI-based innovations in Latvia at the German Digital Summit , Latvia AI Strategy Report

Public programmes and funding instruments for AI and digitalisation

Recovery and Resilience Facility (RRF) and Cohesion Policy 2021–2027

Latvia channels RRF and ERDF funds into private-sector digitalisation and innovation, including SME-focused measures administered by the Ministry of Economics and finance institutions. Government budgetary plans emphasise investment-led growth with EU funds for digitisation of the state and private sector.

ALTUM: Digital Transformation Loans (with capital discounts)

ALTUM (the national development finance institution) provides sizable loans (€100k–€7m) for enterprise digitalisation projects with capital discounts up to 35% (max €1m), funded under the RRF. Use cases include automated production, data analytics, and AI-enabled process optimisation. As of 2024, approved digitalisation projects totalled €31m across 51 firms.¹⁴

LIAA: Innovation Vouchers and SME support

The Investment and Development Agency of Latvia (LIAA) operates innovation vouchers (co-financed by ERDF) for R&D collaboration with research organisations, prototyping, and technology development - frequent precursors to AI pilots in SMEs. Latvia is also launching new SME loan/grant instruments for innovative products and productivity upgrades (~€98.4m total envelope), further easing access to AI and advanced digital tools.¹⁵

Additional SME instruments and ecosystem services

Forthcoming grant schemes for digital maturity assessments and acquisition of digital solutions help smaller firms begin AI adoption journeys. Business incubators, cluster initiatives, and competence centers (e.g., ICT competence center involving LU, RTU, Ventspils University and companies like Tet, Tilde) provide technical and sector expertise relevant to AI.^{16, 17}

National infrastructure and capability-building

European Digital Innovation Hub Latvia (EDIH Latvia / “EDIC/EDIHlv”)

Latvia’s EDIH serves as a one-stop support hub for SME digital transformation - offering test-before-invest services, training, and access to AI expertise (e.g., demonstrations, modelling of AI in production processes). The hub is positioned as the national contact point for digitalisation initiatives, providing digital maturity assessment and road-mapping that de-risks AI investments for SMEs.

AI Centre Lab and the National Artificial Intelligence Center

¹⁴ ALTUM has approved support for business digitalization projects amounting to 31 million euros.

¹⁵ €98.4 million available for development of innovative products in Latvia,

¹⁶ New support instrument for business digitalization to be launched later this year,

¹⁷ Contribution by Latvia to the CSTD 2024-2025 priority theme on “Diversifying economies in a world of accelerated digitalization”,

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 is scaling AI infrastructure and matchmaking platforms. The AI Centre Lab aims to demonstrate AI's business advantages and connect scientists with companies; the government is also launching a National AI Center as the leading national platform for AI development and deployment - supporting research-industry collaboration and attracting investment. These centres will expand SME access to facilities, datasets, and applied expertise across priority domains (e.g., cybersecurity, language and culture, industrial automation).

State language technology platform (Hugo.lv) - an applied AI exemplar

Hugo.lv is a state-owned platform offering machine translation, speech recognition, and speech synthesis, widely used across public administration and available to citizens and businesses. It demonstrates secure, Latvian-tailored AI at scale and provides reusable components (including virtual assistant catalogues and APIs) that SMEs can leverage in multilingual services, accessibility features, and conversational interfaces.

Public–private collaborations and international partnerships

Strategic partnerships (e.g., Microsoft–Latvia)

A memorandum between Latvia and Microsoft (Dec 2024) focuses on AI adoption for public administration and on strengthening the innovation ecosystem - indirectly benefiting SMEs through upgraded national cloud/AI capacity, skills initiatives, and improved digital services that anchor demand and standards.

Research institutes, DIHs, and clusters

The Electronics and Computer Science Institute (EDI) leads an established Digital Innovation Hub; ICT clusters coordinate SME support for digitalisation and AI skills; and universities (LU, RTU, Ventspils) and firms (Tilde, Tet, RIX Technologies) partner in competence centers that co-develop data/AI solutions. These collaborations give SMEs structured pathways to pilots, talent, and co-funded R&D projects.

Alignment with Latvia's economic and innovation goals

Latvia's AI-for-SME approach supports national aims to raise productivity, diversify exports, and move toward higher-value manufacturing and services. Policy documents and EU-funded instruments are coordinated to spur investment, strengthen research-industry links, and embed digital trust - key recommendations echoed by OECD reviews of Latvia's digital transformation. The combined effect is to mainstream AI within a broader growth model rather than treat it as a stand-alone niche.

Italy

Below is a summary of Italy's national strategies and initiatives aimed at supporting SMEs in the adoption and integration of Artificial Intelligence (AI):

1. National Strategic Program for AI (2022–2024)

Approved in November 2021, this program outlines 24 policies across three key areas: skills, research, and applications. Specific SME-related measures include:

- incentives for hiring qualified staff for Industry 4.0 and AI integration;

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.



Co-funded by
the European Union



- promoting AI technology adoption to boost SME competitiveness;
- supporting start-ups and spin-offs in market access and exports;
- enabling controlled experimentation and future certification of AI products, in line with EU regulations.

SMEs are explicitly mentioned as key beneficiaries, with special focus on disadvantaged or peripheral areas.

2. Italian AI Strategy 2024–2026

Released in July 2024, this updated roadmap builds on the previous strategy. It includes the following SME-focused initiatives:

- support for developing AI applications in production processes and business models;
- public-private research projects (funded by the NRRP and national science funds);
- promotion of Italy’s unique AI contexts to reduce reliance on foreign tech providers.

3. AI Solution Certification

Aimed at increasing EU-compliant certified AI products and services by 30%, this includes:

- national support for SMEs seeking certification aligned with the EU AI Act;
- regulatory harmonization with EU safety and health directives.

4. Digital Innovation Hubs (DIHs) and EDIHs (European Digital Innovation Hubs)

Launched under the 2018 “Industry 4.0” Plan and recapitalized in 2023, these networks offer:

- AI training, technical assistance, and access to cutting-edge technologies;
- specialized support for digital transformation tailored to SMEs

5. NRRP Funds

Leveraging NRRP (Piano Nazionale di Ripresa e Resilienza) and national science funding, these programs finance:

- research fellowships, PhDs, and applied AI projects;
- incentives for Italian researchers abroad to return;
- stronger links between SMEs, academia, and research centers.

These initiatives reflect Italy’s broader commitment to responsible innovation, research application, and accessible AI infrastructure, in line with the EU AI strategy. The strategies aim to make SMEs more competitive while ensuring ethical and sustainable AI development.

Turkiye

Türkiye has been formulating a comprehensive legislative and regulatory framework designed to accelerate AI deployment throughout the economy, with a particular focus on SMEs. The primary components of the framework include strategic plans, legislative and regulatory measures, institutional assistance, and their customisation for SMEs.

1. Strategic Documents and Action Plans

National Artificial Intelligence Strategy (NAIS) 2021-2025

This is Türkiye's first comprehensive national AI strategy, initiated with Presidential Circular No. 2021/18 on 20 August 2021. It is developed by the Digital Transformation Office (Presidency) in collaboration with the Ministry of Industry and Technology. The plan is consistent with the Eleventh Development Plan and the Digital Turkey vision.

It defines six strategic priorities:

1. Educating AI specialists and increasing employment in AI-related fields.
2. Promoting research, entrepreneurship, and innovation in artificial intelligence.
3. Increasing access to better data and improving technical infrastructure.
4. Accelerating legal and regulatory modifications to promote socio-economic adaption.
5. Enhancing global collaboration.
6. Accelerating structural and workforce transformation.

AI Strategy Action Plan for 2024-2025

An update to NAIS, along with the 12th Development Plan, aimed at enhancing previous measures, accommodating technology advancements, and improving the integration of SME-focused initiatives. It reduces the quantity of actions and reorganises them for enhanced agility. Central to these initiatives are strategies designed to: attract AI talent (e.g., TechVisa program), incorporate AI and data science subjects into university and vocational curricula, establish technical and ethical standards for domestically developed generative AI models (such as large language models), and create committees to oversee standardisation and certification.

Strategies for Investment and Innovation Support

The Türkiye International Direct Investment Strategy (2024-2028) and associated action plans prioritise the establishment of a conducive environment for foreign direct investment in technology and artificial intelligence, enhancement of local capabilities, and advancement of infrastructure, including data centres, hosting, and broadband services. These measures enhance the competitiveness of local SMEs, facilitate company operations, and bolster the export potential of technological products and services.

2. Regulatory / Legal Measures

- Draft of the Artificial Intelligence Law (submitted June 2024)
This is likely the primary regulatory instrument in preparation. The proposed legislation aims to govern providers, users, importers, distributors of AI systems, and anyone impacted by their utilisation. Essential characteristics encompass:

- Principles of safety, openness, justice, responsibility, and privacy.
- Mandate for risk assessments of AI systems throughout their development and utilisation; specific duties for high-risk systems (e.g., registration with pertinent supervisory authority, conformance evaluations)

- Measures for oversight and compliance monitoring, including possible sanctions (e.g. substantial fines in relation to revenue or for unauthorised usage) for non-compliance.
- Existing gaps: definitions of high-risk and low-risk remain ambiguous; enforcement mechanisms and the institutions responsible for oversight and audits are inadequately specified.

Data Protection Legislation (KVKK, Law No. 6698) and Associated Guidelines

Although not exclusively pertaining to AI, KVKK is fundamental, as numerous AI applications entail the use of personal data. The Personal Data Protection Authority has issued Recommendations for the Safeguarding of Personal Data in the Domain of Artificial Intelligence, along with other sector-specific and technology-specific rules, such as those pertaining to mobile applications and banking. These provide standards for transparency, data minimisation, informed consent, and other principles, beneficial for SMEs to adhere to in the absence of comprehensive regulation.

Additional Existing Laws & Regulations

Until the new AI legislation is implemented, SMEs must adhere to current legal frameworks that intersect with AI, including consumer protection laws, electronic commerce regulations, industrial property and copyright rules, and cybersecurity regulations. These delineate obligations pertaining to equity, accountability, confidentiality, and intellectual property.

3. Institutional & Financial Support

Government Agencies & Bodies

- Digital Transformation Office (Presidency): the principal coordinating entity for digital and AI policy, strategy, execution, and supervision.
- The Ministry of Industry and Technology (MoIT) plays an essential part in executing innovation, industrial policy, infrastructure development (including data centres and hosting), and facilitating the modernisation of small and medium-sized enterprises (SMEs).
- TÜBİTAK, along with several R&D institutions and university centres, provides assistance for research, innovation, and applied AI, frequently participating in grant programs. Although sources did not consistently specify SME-targeted subsidies, the policy references assistance for entrepreneurship and innovation, which is relevant.

SME-Focused Support Measures

- Financial incentives and grants: The action plan encompasses initiatives that provide financial assistance to SMEs for the adoption of AI generated through local research and development. This encompasses financial support, subsidies, or incentives that decrease the cost burden associated with AI tools and integration.
- Education, Training & Talent Development: Integrating AI and data science into higher education; promoting initiatives to enhance workforce competencies in AI; recruiting AI professionals (e.g., through TechVisa) to mitigate skill shortages. These assist SMEs by increasing accessible talent and decreasing reliance on external consultancy.



- **Standardisation, Certification, and Local Model Development:** In accordance with the AI Action Plan, the creation of local large language models, the creation of ethical standards, and the establishment of technical and ethical standards together with certification or compliance processes. Certified and standardised tools assist SMEs by fostering confidence, facilitating public procurement, enhancing export capabilities, and ensuring scalability.

Infrastructure & Data Access

- **Expansion of data infrastructure:** focus on establishing data centres and hosting services within Türkiye to reduce reliance on foreign suppliers, enhance speed, and ensure data integrity.
- **Public data initiatives:** establishing a Central Public Data Space to catalogue publicly held datasets for utilisation by researchers, developers, and SMEs. This facilitates a reduction in data collecting expenses for SMEs and fosters innovation.

4. Tailoring to SMEs: What Policies Specifically Help / Are Needed

Many of the above measures are beneficial in general, but SMEs have specific needs. Here are how current policies support SMEs or could be improved, based on what is in the strategy / draft law, plus observed gaps.

- **Lowering the Cost of Entry**

Financial support, subsidies or grants aimed specifically at small-/medium-scale deployments (e.g. adopting off-the-shelf AI tools, proving out pilots) are needed. The action plan mentions providing financial support for SMEs, but precise programmes need detailing.

- **Skills & Awareness**

SMEs often lack internal AI expertise. The strategy's inclusion of educational programmes, AI curricula at universities, and talent attraction help, but more support is needed for continuing education (short courses, certifications targeted at SME management / staff). Awareness campaigns (national AI literacy), incubators, mentorship help. The roadmap mentions AI literacy campaign, national AI competitions.

- **Regulatory Clarity / Reduced Uncertainty**

SMEs are risk-averse: uncertainty about liability, compliance, certification, risk categories harms adoption. The draft AI law addresses many of these, but gaps remain in definitions, oversight, enforcement. For SMEs, having clear, proportionate regulation (lighter burdens for low-risk AI / tools) is crucial.

- **Standards, Certification & Trust**

SMEs benefit when there are recognised standards / certification, which can support trust, particularly if they are supplying to larger companies or bidding for public contracts. The strategy's moves toward standardisation, local model certification, conformity assessments are positive.

- **Access to Infrastructure & Data**



Building local data infrastructure (hosting, data centres) lowers costs and raises trust. Public data spaces, open datasets reduce proprietary data acquisition cost for SMEs. These features are present in recent policy proposals.

5. Key Remaining Gaps / Recommendations

While the framework is evolving and many supportive policies are in place or under development, for AI integration into SMEs to be successful, these gaps should be addressed:

- Define **risk categories** (e.g. high-risk, limited risk, low-risk) clearly in the law, with associated differential obligations so that SMEs using low-risk AI tools are not overburdened.
- Establish which institution(s) will oversee supervision, conformity assessment, and certification, and clarify their mandates and incentives.
- Simplify access to grants / financial support: ensure SMEs are aware of programs, reduce administrative burdens, ensure that grant sizes are large enough for meaningful AI deployment.
- Expand educational/training opportunities particularly oriented toward SMEs: short courses, vocational, online certifications, mentoring programs.
- Ensure that public procurement rules encourage use of certified AI tools, especially from domestic SMEs. This can create predictable demand and raise trust.
- Promote open data and shared public datasets/infrastructures to lower data / computing costs for SMEs.

2.4 Challenges Faced by SMEs in Adopting AI Technologies in Our Countries

This section compiles and analyzes the various challenges that Small and Medium-sized Enterprises (SMEs) encounter across our countries SMEs in Adopting AI Technologies. It covers a broad spectrum of issues, including financial constraints, regulatory hurdles, limited access to technology and markets, workforce skill gaps, and infrastructural weaknesses. The aim is to provide a comprehensive overview that highlights both common and country-specific obstacles affecting SME growth and sustainability, supported by data and case studies gathered during our research.

By addressing these issues, we strive to empower smaller businesses to harness AI's potential, improving their competitiveness, resilience, and innovation capacity in the digital economy.

Latvia

Limited Awareness of Cybersecurity Needs

Many Latvian SMEs do not prioritise cybersecurity: a recent survey found that only 6% of SMEs allocate a dedicated IT security budget, fewer than 10% maintain a business-continuity plan for crises, and only about 24% consider cybersecurity to be relevant to their company. This low level of awareness and perceived urgency often prevents SMEs from investing in robust cyber-risk management solutions, including AI-driven tools.

Financial Constraints and High Costs

SMEs often cite high costs and lack of resources as significant barriers to adopting new digital or AI technologies. Smaller firms are less likely than large companies to invest in ICT solutions. Given limited budgets, SMEs may prioritise other business needs over cybersecurity investments or advanced digital transformation.

Lack of Skilled Personnel and Digital Competences

A 2023 EU report shows that only about 45.3 % of the Latvian population has at least basic digital skills, which remains below the EU average.¹⁸ For enterprises, the shortage of ICT specialists is a persistent obstacle: almost 60 % of Latvian companies report difficulty filling vacancies for ICT professionals. 19

This limits SMEs' ability to develop, deploy and maintain advanced digital or AI-based cybersecurity systems internally.

Infrastructure Gaps and Uneven Digital Readiness

Despite progress in digitalisation, Latvia still faces challenges in fully upgrading its ICT infrastructure. Connectivity issues and underdeveloped digital infrastructure slow down adoption of cloud services, AI solutions, and digital communication tools - especially for SMEs outside major urban areas.²⁰

Perceived Complexity and Lack of Internal Capacity to Manage Change

Many SMEs express concerns over the organizational burden of digital transformation. According to a 2021 study, Latvian SMEs report risks associated with digital change: cyber threats, regulatory requirements, digital overload, and dependence on technology.²¹ As SMEs often lack internal capacity for change management, training, and long-term maintenance of digital systems, they may avoid adopting complex solutions like AI-driven cybersecurity.

Insufficient Incentives and Public Support for SMEs' Digital Transition

Research shows that many SMEs depend on public support - subsidies, mentoring, training - for successful digital transformation.²² The lack of tailored financial or regulatory incentives makes SMEs hesitant to invest in digital transformation or AI cybersecurity solutions independently.

¹⁸ <https://digital-strategy.ec.europa.eu/en/factpages/latvia-2024-digital-decade-country-report>

¹⁹ <https://digital-strategy.ec.europa.eu/en/factpages/latvia-2024-digital-decade-country-report>

²⁰ <https://www.varam.gov.lv/lv/media/42912/download?attachment>

²¹ https://eszf.lu.lv/fileadmin/user_upload/LU.LV/Apaksvietnes/Fakultates/www.bvef.lu.lv/Report.pdf

²²

https://www.researchgate.net/publication/367816825_Digital_Transformation_of_Small_and_Medium_Enterprises_Aspects_of_Public_Support

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

Small and Medium-sized Enterprises (SMEs) in Italy represent a backbone of the national economy, but their adoption of Artificial Intelligence (AI) technologies remains limited and uneven. Analysis of data from Eurostat, ISTAT, and the Excelsior report reveals several critical challenges hindering AI integration in Italian SMEs.

1. Financial Constraints

According to ISTAT's 2023 report on "Imprese e Innovazione Digitale", many Italian SMEs face significant budget limitations that restrict investments in new technologies. The upfront costs of AI tools, including software acquisition, system integration, and specialized staff recruitment, often exceed the financial capacities of smaller firms, particularly micro-enterprises. This financial barrier remains one of the foremost hurdles limiting widespread AI adoption.

2. Digital Skills Shortage

Data from Eurostat's 2024 statistics on ICT specialists highlights Italy's below-average share of workers with digital and AI-related skills within SMEs compared to the EU. The Excelsior report (2023) further underscores the difficulty Italian SMEs face in recruiting personnel with the necessary digital expertise. This shortage of qualified professionals constrains SMEs' ability to develop, implement, and maintain AI solutions effectively.

3. Low Awareness and Understanding of AI

ISTAT's 2023 survey on the use of digital technologies reveals a widespread knowledge gap among SMEs regarding AI benefits and practical applications. Many SMEs are unaware of how AI can improve their processes or remain uncertain about the complexity and risks involved. This hesitance slows adoption and reduces incentives for investing in AI-driven innovation.

4. Regulatory and Data Privacy Challenges

Compliance with data protection regulations, especially the EU's General Data Protection Regulation (GDPR), presents significant challenges. ISTAT's recent findings indicate that SMEs often lack the legal and technical resources to navigate these complex frameworks, which is crucial when dealing with data-intensive AI applications. The European Commission's reports reinforce that data privacy concerns remain a key obstacle for SME AI adoption across Europe, including Italy.

5. Digital Infrastructure Disparities

Eurostat regional data (2024) points to notable differences in digital infrastructure quality across Italian regions. SMEs in southern Italy and rural areas are disproportionately affected by slower internet speeds and limited broadband coverage. These infrastructural gaps limit SMEs' access to cloud-based AI services and reduce their competitiveness in the digital economy.

6. Organizational and Cultural Barriers

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.

Traditional SME organizational cultures, particularly family-owned businesses, exhibit cautious attitudes towards innovation. The Excelsior report (2023) and ISTAT's studies on innovation adoption emphasize resistance to change as a major internal barrier. A lack of strategic vision for digital transformation and risk aversion slow down AI uptake despite potential competitive advantages.

Türkiye

SMEs in Türkiye face multiple interlocking challenges when it comes to adopting AI technologies. Many of these are common across countries, but some are specific to the Turkish context. Below are the main obstacles, with explanations and supporting data.

- **Low Adoption & Awareness:** Only 10% of SMEs use AI and there is limited understanding of AI's benefits; low visibility of success stories.
- **Financial Constraints:** High upfront/recurring costs (tools, cloud, licensing, maintenance). Besides there is limited access to funding and complex grant procedures.
- **Skill Shortages:**
 - Few in-house AI/data experts; reliance on general IT staff.
 - Lack of tailored training and certifications for SME staff.
 - Difficulty retaining talent due to competition with larger firms.
- **Data Challenges:** Poor access to quality datasets; fragmented/unstructured records.
- **Regulatory Uncertainty:** Draft AI Law still vague (risk categories, certification, liability).
- **Organisational & Cultural Barriers:** Weak digital/data culture; lack of data-driven decision-making.
- **Unclear ROI (return of investment):** Difficulty measuring short-term benefits. Besides there is a risk of insufficient returns, especially for small firms.
- **Security & Ethical Concerns:** Rising cybersecurity threats and data risks and there are concerns about bias, fairness, and transparency in AI systems.

Conclusion

The research conducted in Latvia, Italy, and Turkey highlights that SMEs across these countries focus primarily on key competency areas essential for their digital transformation and cybersecurity readiness. These areas include general AI adoption, core cybersecurity practices, risk management strategies, and data analysis capabilities. This document establishes the foundation for the survey (Annex 1), which will be launched in partner countries to capture SME perspectives across diverse sectors. The survey will ask SMEs to rate the importance of various competencies within these broad domains, helping to identify critical skill gaps and training needs.

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.

Research in the three countries reveals significant barriers to AI adoption, including financial constraints, skill shortages, outdated infrastructure, and low awareness. Although interest is growing - particularly in Italy - SMEs encounter challenges such as regulatory complexity and organizational resistance.

The project addresses these issues by pinpointing essential AI-driven cybersecurity skills and developing practical tools and training programs to empower SMEs. This ensures that SMEs can build the competencies necessary to manage cyber risks effectively and leverage AI technology for growth.

Annex

SME Digital Competence Gap Survey

Welcome to the Erasmus+ project “Exploring the AI Frontier: AI-Driven Cyber Risk Management for SMEs” (AID) Competence Survey, coordinated by the Baltijas Datoru Akadēmija (BDA) - Latvia, in collaboration with Training 2000 (Italy) and Muğla Sıtkı Koçman University (MSKU) - Türkiye . The project focuses on helping small and medium-sized enterprises (SMEs) strengthen their ability to understand, manage, and reduce cyber risks - with the support of emerging technologies like Artificial Intelligence (AI).

This survey aims to identify which digital and AI-related cybersecurity skills are most relevant to European SMEs across different sectors. It is divided in 4 main sections:

1. Personal information
2. Competence Areas (AI, Cybersecurity, Risk Management, and Data Analysis)
3. Perceived Barriers to developing cybersecurity competences
4. General comments

Thank you for your participation.

The AID project team

Section 1 - Personal Information

1. In which size category would you place your company? (Tick all that apply.)

- Micro SME (fewer than 10 employees and annual revenue ≤ €2 million)
- Small SME (fewer than 50 employees and annual revenue ≤ €10 million)
- Medium-sized SME (fewer than 250 employees and annual revenue ≤ €50 million)

2. Please select the sector that best fits your business activity.

- Manufacturing and Industry (e.g. chemicals, pharmaceuticals, food production, waste management)
- Energy and Utilities (e.g. electricity, gas, water, heating, wastewater)
- Transport and Logistics (e.g. air, rail, road, water transport, postal, courier services)
- Finance and Insurance (e.g. banking, financial markets, insurance)
- Health and Life Sciences (e.g. healthcare, pharmaceuticals, research)

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.

- ICT and Digital Services (e.g. IT, communications, space)
- Professional Services (e.g. consulting, legal, advertising)
- Trade, Retail and Hospitality (e.g. wholesale, accommodation)
- Other (please specify): _____

Section 2 - Competence Areas (AI, Cybersecurity, Risk Management, and Data Analysis)

1. Please rate **how important** you think each of the following **cybersecurity competences** on a scale from 1 to 5 (1= Not important at all, 5 Critically important).

| Cybersecurity Competence | 1 | 2 | 3 | 4 | 5 |
|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Protecting company devices and content from digital threats and risks | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Knowing basic cybersecurity and privacy practices to build trust in digital tools | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Ensuring personal data and privacy are respected in digital environments | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Using and sharing personal data responsibly | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Understanding privacy policies and their implications | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Avoiding stress, fatigue, or other digital health risks | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Recognizing and preventing harmful online behaviour (e.g. cyberbullying) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Promoting digital inclusion and social well-being through technology | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Understanding algorithmic bias and explainability in AI systems | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Evaluating the reliability and effectiveness of AI-based cybersecurity tools | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Making informed decisions about adopting AI for threat detection | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

2. Please rate **how important** you think each of the following **cyber risk management competences** on a scale from 1 to 5 (1= Not important at all, 5 Critically important).

| Cyber Risk Management Competence | 1 | 2 | 3 | 4 | 5 |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Applying structured risk management policies across IT systems | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Assessing risks to digital assets and planning appropriate strategies | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Presenting cost–benefit analysis to support cyber risk decisions | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Aligning risk management decisions with business and tech goals | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Evaluating current cybersecurity posture and setting SME-specific goals | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Identifying risks, costs, and weaknesses when planning cybersecurity actions | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Managing risks related to company data and information assets | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

3. Please rate **how important** you think each of the following **data analysis competences** on a scale from 1 to 5 (1= Not important at all, 5 Critically important)

| Data Analysis Competence | 1 | 2 | 3 | 4 | 5 |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Understanding how personal data is processed and protected | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Applying cost–benefit analysis and risk assessment in data contexts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Collecting and preparing quality data from various sources | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Using statistical methods to understand data and extract insights | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Presenting data visually for clear communication and decisions | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Explaining complex data findings in a clear, actionable way | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Asking critical questions and identifying hidden data patterns | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Continuously updating skills with new tools, methods, and best practices | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Section 3 - Perceived barriers to developing cybersecurity competences

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

- Lack of time or staff capacity
- No budget for training or digital tools
- Lack of access to relevant training opportunities
- Low priority in the company’s current business strategy
- Lack of awareness of the risks
- Other (please specify): _____

Section 4 – General comments

1. What specific topics related to cybersecurity or AI would you consider essential for future SME-focused training or resources?

Open-ended answer:

2. Any other comments or ideas you would like to share?

Open-ended answer:

References

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens- With New Examples of Knowledge, Skills and Attitudes (EUR 31006 EN). Publications Office of the European Union. <https://doi.org/10.2760/115376>

<https://edu.unibit.bg/course/index.php?categoryid=103&lang=en>

Cabinet of Ministers of the Republic of Latvia. (2021, July 7). Guidelines for Digital Transformation for 2021-2027 (Order No. 490). <https://likumi.lv/ta/id/324715>

European Union. (2022). NIS2 Directive on security of network and information systems (Directive (EU) 2022/2555). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555>

Republic of Latvia. (2023). The Cybersecurity Strategy of Latvia 2023–2026. <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/latvia-cybersecurity-strategy-2023-2026>

CERT.LV. (2025, August). CERT.LV activity review Q2 2025. <https://cert.lv/en/2025/08/cert-lv-activity-review-q2-2025>

Digital Innovation Hub Latvia. (n.d.). 10 svarīgākās atziņas par IKT un kibersdrošību no uzņēmumu vadītājiem. <https://dih.lv/lv/jaunumi-un-pasakumi/jaunumi/10-svarigakas-atzinas-par-ikt-un-kiberdrosibu-no-uznemumu-vaditajiem>

Digital Latvia. (n.d.). Digital skills development. <https://www.digitallatvia.lv/digital-skills-development>

Online Article, “Just 8% of Italian enterprises using AI, many people lack digital know-how”, Reuters, May 2025 <https://www.motilaloswal.com/news/global/4197#:~:text=Yahoo!-Just%208%25%20of%20Italian%20enterprises%20using%20AI%2C%20many%20people%20lack,just%2045.8%25%20having%20basic%20skills>. ISTAT DATA

EUROSTAT DATA

Online Article, “Empowering SMEs for digital transformation and innovation: The Italian way “, OECD, March 2024.

SISTEMA INFORMATIVO EXCELSIOR 2024, “LE COMPETENZE DIGITALI ANALISI DELLA DOMANDA DI COMPETENZE DIGITALI NELLE IMPRESE, INDAGINE 2024”.