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

KA210-VET

Competence Map

Introduction

The AID Competence Map is a structured framework designed to identify and classify the critical competencies necessary for SMEs to effectively navigate digital transformation and manage AI-driven risks. Aligned to the European Qualifications Framework (EQF) levels, the map ensures that digital readiness and resilience are measurable and standardised across different European contexts. The structure of the map is specifically organized into three high-priority areas: Cybersecurity, Cyber Risk Management, and Data Analysis. For each area, the framework provides a comprehensive breakdown divided into behaviours, skills, knowledge, and attitudes.

- **Behaviours**: These describe observable actions and decision-making processes, such as applying structured risk management policies, understanding algorithmic bias, and using personal data responsibly.
- **Skills**: This dimension focuses on practical application, including the configuration of security settings, the identification and prioritization of cyber risks, and the collection and cleaning of data from various sources.
- **Knowledge**: This represents the theoretical foundation required, such as understanding fundamental cybersecurity concepts, popular cyberattacks, risk management standards, and the ethics of AI.
- **Attitudes**: The map highlights essential mindsets, including proactivity towards risk prevention, an analytical mindset for evidence-based decisions, and a commitment to upholding data integrity.

To have an overview of the competence map creation process , we recommend reading the study “Competency Research for Digital Adaptation and Growth in SMEs” (Deliverable 1) and the “International Report on SME Digital Competence Gap Survey Results”(Deliverable 2), covering Italy, Latvia, and Türkiye, available on the project website: https://www.bda.lv/en/ai-driven-cyber-risk-management-for-smes/

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.

Competence area and description	Behaviours	Skills	Knowledge	Attitudes
Cybersecurity **The ability to protect company's digital devices, systems, data, and personal online activities from threats and risks by applying secure practices, respecting privacy, and making informed decisions about the use of existing and emerging technologies, including artificial intelligence, to ensure a safe and trustworthy digital environment.**	1. Protecting company devices and content from digital threats and risks 2. Knowing basic cybersecurity and privacy practices to build trust in digital tools Ensuring personal data and privacy are respected in digital environments 3. Using and sharing personal data responsibly 4. Understanding privacy policies and their implications 5. Avoiding stress, fatigue, or other digital health risks 6. Recognizing and preventing harmful online behaviour (e.g. cyberbullying) 7. 8Promoting digital inclusion and social well-being through technology 8. Understanding algorithmic bias and explainability in AI systems 9. Evaluating the reliability and effectiveness of AI-based cybersecurity tools 10. Making informed decisions about adopting AI for threat detection	1. Identification and response to security risks for devices and data 2. Configuration of security settings of devices 3. Use of multi-factor authentication and safe passwords 4. Safe storage and backing up of data 5. Assessment of credibility and reliability of AI tools	1. Knowledge of fundamental cybersecurity concepts (authentification, encryption, data backup) 2. Knowledge of popular cyberattacks (malware, phishing, ransomware etc.) 3. Safe digital practices for work and personal use 4. Common laws and regulations affecting digital data (GDPR, national laws etc.) 5. Basics of machine learning and safe use of AI 6 Ethics and legal aspects of using A	1. Proactivity towards cybersecurity and risk prevention 2. Responsible handling of company and personal data 3. Openness to learning new technologies 4. Healthy skepticism towards communications and use of digital tools and environments

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.

Competence area and description	Behaviours	Skills	Knowledge	Attitudes
Cyber risk management **The ability to identify, analyze, and prioritize risks to digital assets, information systems and data, and to make informed, business-aligned decisions that balance security, cost, and operational needs in order to protect oneself and the organization, and support strategic goals.**	1. Applying structured risk management policies across IT systems 2. Assessing risks to digital assets and planning appropriate strategies 3. Presenting cost–benefit analysis to support cyber risk decisions 4. Aligning risk management decisions with business and tech goals 5. Evaluating current cybersecurity posture and setting SME-specific goals 6. dentifying risks, costs, and weaknesses when planning cybersecurity actions 7. Managing risks related to company data and information assets	1. Identifying, classifying, and prioritizing cyber risks 2. Performing qualitative and quantitative risk assessments 3. Translating technical risks into business-relevant insights 4. Creating realistic risk mitigation strategies and action plans 5. Communicating cyberrisks and releveant strategies to technical and non-technical stakeholders	1. Knowledge of relevant risk management frameworks and quality standards 2. Knowledge of cybersecurity landscape and relevant cyberrisks for the company 3. Importance of analyzing, communication and responding to risk incidents 4. Cost-benefit and risk-based decision-making models 5. Regulatory, legal and compliance requirements for data and systems	1. Balanced judgment between security, cost, and usability 2. Accountability for protecting business value, not just technology 3. Analytical mindset with attention to detail and evidence-based decisions 4. Collaboration across security, IT, and business functions 5. Forward-looking approach to anticipating emerging risks

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.

Competence area and description	Behaviours	Skills	Knowledge	Attitudes
Data analysis **The ability to collect, process, interpret, and communicate data by applying analytical methods, protecting data integrity and privacy, and transforming complex information into meaningful, actionable knowledge that supports informed decision-making.**	1. Understanding how personal data is processed and protected 2. Applying cost–benefit analysis and risk assessment in data contexts 3. Collecting and preparing quality data from various sources 4. Using statistical methods to understand data and extract insights 5. Presenting data visually for clear communication and decisions 6. Explaining complex data findings in a clear, actionable way 7. Asking critical questions and identifying hidden data patterns 8. Continuously updating skills with new tools, methods, and best practices	1. Collecting, cleaning, and structuring data from various sources 2. Using statistical and analytical techniques for data analysis 3. Visualization of data to be used for decision making (charts, graphs, presentations, etc.) 4. Conclusions and decision making based on data 5. Identifying trends and correlations in data using critical thinking	1. Knowledge about data lifecycle, quality, and management principles 2. Statistical and analytical methods for data processing 3. Privacy and ethical use of personal data in data management (GDPR, anonymization of data) 4. Tools and techniques of data visualization 5. Use of cost-benefit and risk analysis models for data-driven decisions	1. Ability and willingness to explore data and question the existing assumptions 2. Commitment to upholding the accuracy and integrity of data 3. Objectivity of the analysis and use of data as opposed to intuition 4. Responsibility in communication and interpretation of data

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.

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

Co-funded by
the European Union

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.