

Competency	Competency description
Behaviours	1 2 3
Skills	1 2 3
Knowledge	1 2 3
Attitudes	1 2 3
Training Focus	1 2 3

<b>Competency</b> <b>Cybersecurity</b>	<b>Competency description</b> 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.
<b>Behaviours</b>	1 Protecting company devices and content from digital threats and risks 2 Knowing basic cybersecurity and privacy practices to build trust in digital tools 3 Ensuring personal data and privacy are respected in digital environments 4 Using and sharing personal data responsibly 5 Understanding privacy policies and their implications 6 Avoiding stress, fatigue, or other digital health risks 7 Recognizing and preventing harmful online behaviour (e.g. cyberbullying) 8 Promoting digital inclusion and social well-being through technology 9 Understanding algorithmic bias and explainability in AI systems 10 Evaluating the reliability and effectiveness of AI-based cybersecurity tools 11 Making informed decisions about adopting AI for threat detection
<b>Skills</b>	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
<b>Knowledge</b>	1 Knowledge of fundamental cybersecurity concepts (authentication, 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 AI
<b>Attitudes</b>	1 Proactivity towards cybersecurity and risk prevention 2 Responsible handling of company and personal data 3 Openness to learning new technologies 4 Healthy scepticism towards communications and use of digital tools and environments

<b>Training Focus</b>	<ol style="list-style-type: none"><li>1 Cybersecurity basics and common digital threats</li><li>2 Data protection and privacy compliance rules</li><li>3 Responsible use of digital and cloud tools and collaboration platforms</li><li>4 Safe and responsible use of AI tools</li><li>5 Implications of human factor on digital safety</li></ol>
-----------------------	---

<b>Competency</b> <b>Cyber Risk Management</b>	<b>Competency description</b> <b>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.</b>
<b>Behaviours</b>	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 Identifying risks, costs, and weaknesses when planning cybersecurity actions 7 Managing risks related to company data and information assets
<b>Skills</b>	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 relevant strategies to technical and non-technical stakeholders
<b>Knowledge</b>	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
<b>Attitudes</b>	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
<b>Training Focus</b>	1 Basics of cyber risks and popular risk management standards 2 Risks assesment and risk mitigation techniques 3 Economic principles of cyber risks and decision making on protection 4 Alignment of cyber risk management with general business management strategy

<b>Competency</b> <b>Data Analysis</b>	<b>Competency description</b> 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.
<b>Behaviours</b>	<ul style="list-style-type: none"> <li>1 Understanding how personal data is processed and protected</li> <li>2 Applying cost–benefit analysis and risk assessment in data contexts</li> <li>3 Collecting and preparing quality data from various sources</li> <li>4 Using statistical methods to understand data and extract insights</li> <li>5 Presenting data visually for clear communication and decisions</li> <li>6 Explaining complex data findings in a clear, actionable way</li> <li>7 Asking critical questions and identifying hidden data patterns</li> <li>8 Continuously updating skills with new tools, methods, and best practices</li> </ul>
<b>Skills</b>	<ul style="list-style-type: none"> <li>1 Collecting, cleaning, and structuring data from various sources</li> <li>2 Using statistical and analytical techniques for data analysis</li> <li>3 Visualization of data to be used for decision making (charts, graphs, presentations etc.)</li> <li>4 Conclusions and decision making based on data</li> <li>5 Identifying trends and correlations in data using critical thinking</li> </ul>
<b>Knowledge</b>	<ul style="list-style-type: none"> <li>1 Knowledge about data lifecycle, quality, and management principles</li> <li>2 Statistical and analytical methods for data processing</li> <li>3 Privacy and ethical use of personal data in data management (GDPR, anonymization of data)</li> <li>4 Tools and techniques of data visualization</li> <li>5 Use of cost-benefit and risk analysis models for data-driven decisions</li> </ul>
<b>Attitudes</b>	<ul style="list-style-type: none"> <li>1 Ability and willingness to explore data and question the existing assumptions</li> <li>2 Commitment to upholding the accuracy and integrity of data</li> <li>3 Objectivity of the analysis and use of data as opposed to intuition</li> <li>4 Responsibility in communication and interpretation of data</li> </ul>
<b>Training Focus</b>	<ul style="list-style-type: none"> <li>1 Data governance and responsible handling of data</li> <li>2 Techniques and tools for collecting and processing data</li> <li>3 Use of the appropriate tools for data analytics, statistics, data modelling and visualisation</li> <li>4 Validation of data and use in cyber risk management</li> </ul>