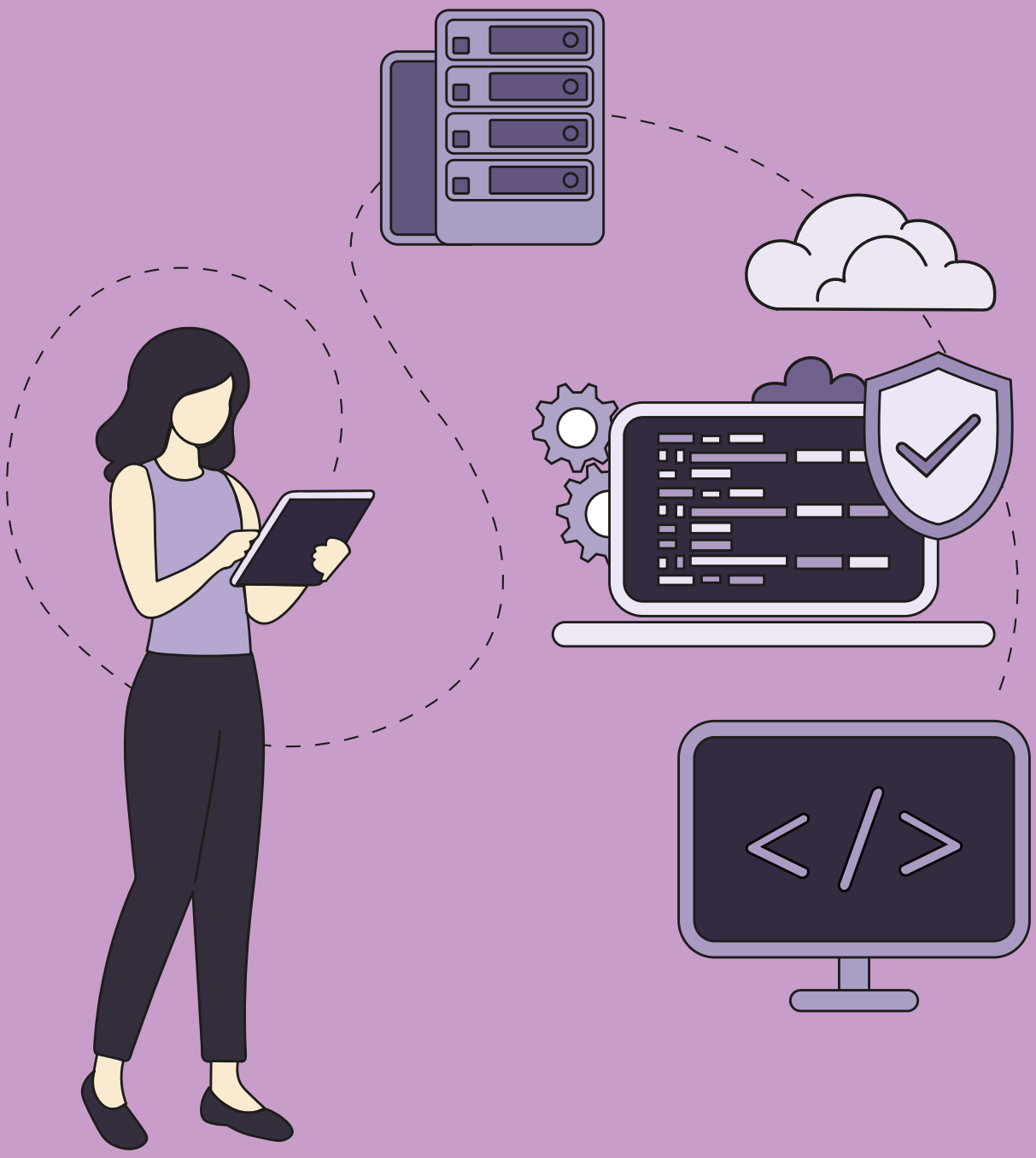
INTEGRATED QUALIFICATIONS SYSTEM



UPDATED SECTORAL QUALIFICATIONS FRAMEWORK FOR INFORMATION TECHNOLOGY (IT)

European Funds for Social Development
Republic of Poland
Co-funded by the European Union
EDUCATIONAL RESEARCH INSTITUTE
National Research Institute

Authors of the introductory chapters: Edyta Cieszkowska, Dawid Dymkowski, Michał Królikowski, Monika Lentacz, Mateusz Przywara, Urszula Wrońska

Authors of the updated SQF IT: Adam Białek, Edyta Cieszkowska, Witold Dobrzyński, Dawid Dymkowski, Rafał Kołodziejczyk, Monika Lentacz, Tadeusz Osowski, Damian Parol, Janusz Popielewski, Bartłomiej Przybyciel, Maciej Rakowski, Agnieszka Rogowska, Dominik Strzałka, Kamil Szostak, Urszula Wrońska, Jerzy Żemła

Polish language editor: Anna Herzog-Grzybowska
Translation: Barbara Przybylska
Cover design: Zuzanna Gułaj
Layout: Wojciech Maciejczyk

ISBN: 978-83-68752-07-6

Publisher:
Educational Research Institute – National Research Institute
ul. Górczewska 8, 01-180 Warsaw, Poland
tel. (+48 22) 241 71 00; www.ibe.edu.pl

Warsaw 2026

Citation: Białek, A., Cieszkowska, E., Dobrzyński, W., Dymkowski, D., Kołodziejczyk, R., Królikowski, M., Lentacz, M., Osowski, T., Parol, D., Popielewski, J., Przybyciel, B., Przywara, M., Rakowski, M., Rogowska, A., Strzałka, D., Szostak, K., Wrońska, U., Żemła, J. (2026). *Updated Sectoral Qualifications Framework for Information Technology (SQF IT)* (B. Przybylska, Trans.). Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy. (Original work published 2026)

This publication was produced as part of the systemic project "Supporting the further development of the Integrated Qualifications System in Poland (IQS 6)", co-financed by the European Union through the European Funds for Social Development 2021–2027 (FERS) programme.

Free copy

Table of Contents

1. Definition of the sector

The information technology sector encompasses all activities relating to the processing, storage, transmission, and management of information using digital technologies. It involves activities of varying degrees of complexity, such as: requirements analysis, design, development, testing, security, and software deployment, as well as the administration of IT systems, digital service configuration, maintenance, and required updating activities. The IT sector also includes the development and application of hardware, software, computer networks, databases, and digital platforms, as well as the provision of a variety of digital services utilising cloud systems and artificial intelligence in conjunction with cybersecurity services that protect IT (ICT) systems against threats and cyberattacks.

Sectoral determinants:

I. IT infrastructure
II. Network technologies
III. Software engineering
IV. Digital applications and services
V. Cloud solutions
VI. IT support
VII. Data management and AI
VIII. IT solutions architecture
IX. IT management
X. Groundbreaking IT technologies
XI. Green IT
XII. Communication, collaboration, leadership
XIII. User-centred approach
XIV. Responsibility and ethics
XV. Development and innovation

2. Practical application of the Sectoral Qualifications Framework for Information Technology

The Sectoral Qualifications Framework for Information Technology (SQF IT) is a universal tool for managing the competences in the information technology sector. Due to the fact that the structure of SQF IT does not impose specific business solutions, it can be used in any number of ways by many different audiences.

Employers

With the help of SQF IT, employers can take a broader view of the industry competences present in their business environment, enabling them to manage their human resources more efficiently and compete more effectively in the labour market. The main advantages of using this tool include support in analysing competence gaps in the industry or company, planning human resource development and the salary grid of job positions, as well as gaining help with recruitment and the selection of personnel.

The table of competences allowed me to determine the criteria for recruiting staff based on the key competences in the industry, as well as to prepare job descriptions.

Schools and educational institutions

After identifying the main competence gaps in the industry, we launched an apprenticeship programme to prepare our students to successfully enter the labour market.

On the basis of SQF IT, schools and educational institutions can adapt the curricula they offer to the current and real needs of the labour market. This means that the table of competences supports these institutions in expanding and modifying their teaching programmes as well as filling in the competence gaps of students, such as those relating to practical or soft skills. Additionally, it can be a useful tool in career counselling for students and in monitoring the success of school leavers.

Higher education institutions

SQF IT is a tool that supports higher education in aligning their study programmes with current trends in industry development. As a result, students are better prepared to enter the labour market and achieve career success. The table of competences also makes it possible to monitor students' progress and evaluate the effectiveness of study programmes.

We use SQF IT to analyse students' level of skills against those needed by the IT sector and the effectiveness of our study programmes.

By better matching the needs of our customers, we have become more competitive in the training market.

Training companies

Using SQF IT allows training companies to effectively design specialised courses, enabling them to prepare a tailor-made offer for a specific sub-sector, and to meet the expectations of their clients. With the help of the sectoral qualifications framework, they can select individual competences and match them to the outcomes of a given training programme. They can also prepare exams to assess knowledge, skills, and social competence. In addition, the gradation of the complexity of competences in SQF IT makes it easier to prepare training offers at various levels of proficiency.

IQS stakeholders

Among the broad audience of the Integrated Qualifications System (IQS), the groups most likely to benefit from the SQF IT are primarily industry organisations and those describing market or sectoral qualifications. Among others, industry organisations are tasked with establishing educational agreements that strengthen cooperation between schools and employers, as well as providing information on the demand for sectoral competences to educational institutions and

labour market institutions. In turn, persons describing market or sectoral qualifications can use the framework to more easily define sets of learning outcomes.

Other entities

SQF IT can be used for many other purposes depending on the current needs of the industry. In the information technology sector, it can be used as a supplementary tool to prepare methods for assessing the knowledge of a company's employees.

Moreover, the IT sector is currently facing a shortage of skilled workers. The Sectoral Qualifications Framework for Information Technology can be us at specific levelsed to retrain and launch the professional careers of people from related sectors.

As an IT expert, I strive to keep up with the latest technical developments in the industry. Analyzing the "Groundbreaking IT Technologies" determinant allows me to focus on the most important areas that are relevant not only within the sector but also in the job market.

3. Instructions for using the Sectoral Qualifications Framework for Information Technology

1 Familiarise yourself with the sectoral determinants, as they indicate the main areas of the sector's activities.

2 Familiarise yourself with the competence series, as they further describe each sectoral determinant.

3 Familiarise yourself with the competences in a given series at specific levels.

The competences in the SQF at particular levels correspond to second stage Polish Qualifications Framework levels for vocational education and training

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
SECTORAL DETERMINANT I.	knows and understands...								
	is able to...								
SECTORAL DETERMINANT II.	knows and under-								
	is able to...								
SECTORAL DETERMINANT III.	knows and under-								
	is able to...								
SECTORAL DETERMINANT IV.	is ready to....								

Competences are grouped into their appropriate categories by colour:

knowledge (knows and understands...),

skills (is able to...),

social competence (is ready to...).

Remember!
Green competences are designated in bold and indicated as **(GC)** in front of the description.

Important!
A specific process can often be fully described only by combining competence series from the categories of **knowledge** and **skills**.

4. Updated Sectoral Qualifications Framework for Information Technology, indicating the green competences identified in the sector

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	knows and understands…	**Server environments**	basic issues relating to computer networks and operating systems; the structure of server environments	the specifications and architecture of physical servers, including multi-core processors; network interface parameters and their significance; the principles of administering Windows Server and/or Linux and/or UNIX server operating systems (e.g., Windows Server, Debian/Ubuntu/RHEL, HP-UX/ AIX/Solaris); the environmental conditions affecting the operation of servers (e.g., temperature, humidity)	the principles of server and service configuration (including web, file, email, and database services); clustering issues (creation, management); scripting languages and command-line shells (e.g., Bash, PowerShell)	the methods of automation and orchestration of server environments (e.g., IaC); high availability (HA) mechanisms; the principles of server network configuration; the principles of managing server environments in hybrid and distributed cloud models	the methods of selecting security solutions for server environments; the methods of designing scalable and redundant server environments; the principles of selecting server technologies from a business and licensing perspective	
	is able to…	**Server environments**	boot operating systems (Linux/ Windows) from pre-built images	select and configure the parameters and architecture of physical servers; assign and configure network interfaces (including the IP address, subnet mask, default gateway); select power supply parameters; select the type and parameters of the emergency power supply; ensure appropriate environmental conditions for server operation	configure server parameters for specific services; configure a server cluster; create/use (automation) scripts and use command-line shells	create and maintain virtual machines and containers; manage the high availability of server environments, including load balancing; automate the management of server environments (e.g., Ansible, Terraform, Puppet)	secure server environments through the continuous application of hardening measures; build, configure, and deploy server environments in a hybrid infrastructure (on-premises data centres and the cloud)	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	knows and…	**Virtualisation**	the basic concepts of virtualisation	the guidelines for selecting the infrastructure for virtual solutions; the lifecycle of a virtual machine; the basics of virtual networks; the difference between a snapshot and a backup	the methods of managing virtualised networks; the principles of backing up and the retention policy of virtual machine backups; the principles of storage virtualisation	the methods of managing clusters and HA mechanisms, as well as live migration	the methods of migrating environments (virtual-to-physical, virtual-to-virtual); the risks associated with P2V/V2V environment migration and rollback methods	
	is able to…	**Virtualisation**	create virtual machines from templates and configure their basic parameters	select infrastructure for virtualisation; create a snapshot for a virtual machine; change the parameters of virtual machines	configure VLANs on a virtual switch and assign port groups; configure virtual machine backup jobs	configure live migration and HA policies for critical virtual machines; create and manage virtual machines in a cluster	develop a virtual architecture design; plan and execute P2V/V2V migrations with a contingency plan (rollback)	
	knows and understands…	**Containerisation**		the principles of containerisation; the basics of how a container works; the basics of container networking (bridge/host) and persistent storage (volume); basic containerisation tools (e.g., Docker, Podman) and OCI standards	the structure of a layered image and how cache works; the methods of creating application health probes and environment variables within a container (e.g., health probe or liveness probe); the role of a private registry and tagging rules	the method of data persistence in a container and its significance; orchestration tools, container platforms (e.g., Kubernetes, OpenShift), and cluster management tools (e.g., Rancher); container lifecycle management (from image build to deployment and monitoring)	the patterns for porting applications to containers (resource migration models: 6R and 7R strategies)	
	is able to…	**Containerisation**		build a container image; start a container from an image; mount a volume; read the logs and status of a container	prepare one's own container image; add a health check and resource limits for a container; prepare a Compose file for a service stack with persistent storage; log in to a private registry and push and pull images	implement a local image registry with a retention policy; design a multi-service environment with a segregated network, secrets, and persistent storage	develop a plan for migrating applications to containers; design a phased update with health checks and rollback criteria	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	knows and understands...	**Monitoring IT infrastructure**	basic system parameters (e.g., availability, CPU load, memory usage, storage space, environmental parameters); basic network parameters (e.g., availability, bandwidth, latency, packet loss, interface load); basic application and service metrics (e.g., service and process status, response time, number of connections)	virtual and cloud environment parameters (e.g., machine load, host and hypervisor status, cloud resource availability)	the rules for analysing alerts from monitoring tools; the impact of monitored parameters on system availability; monitoring tools (e.g., Zabbix, Grafana, Kibana)	the methods of event correlation	the impact of incidents on SLAs and KPIs; IT infrastructure maintenance strategies	the ability to create and utilise new AI/ML algorithms for fault prediction and automated response
	is able to...	**Monitoring IT infrastructure**	read data from IT infrastructure monitoring tools; log incidents relating to monitored parameters	configure basic parameters for monitoring IT infrastructure	configure advanced parameters for monitoring IT infrastructure; respond to incidents relating to monitored parameters; analyse system event logs; assess the impact of monitored parameters on system performance and availability	integrate monitoring with notifications; create dashboards; propose improvements to the IT infrastructure	design IT infrastructure monitoring systems; report on the effectiveness of monitored system parameters; support decision-making regarding the monitored components of the IT infrastructure; be responsible for SLAs and KPIs; develop IT infrastructure monitoring policies; oversee compliance and operational efficiency	use innovative AI/ML algorithms to predict failures and automate the initiation of preventive actions
	knows and understands...	**Authentication and authorisation technologies**	the basics of authentication; the basics of authorisation	various identity and access management technologies and systems (e.g., biometrics)	a wide range of identity and access management technologies and mechanisms within an organisation (e.g., MFA, SSO, PAM, PIM); access control methods (e.g., DAC, MAC, RBAC, ABAC, PBAC, Rule-Based Access Control); organisational procedures and policies relating to identity and access management	complex identity and access management methods characterised by enhanced security and improved efficiency; identity and access management systems; identity federation; specialised identity and access management methods utilising automation	the methods of auditing security policies relating to identity and access management; the principles of identity and access strategy management	research into trends in the development of Zero Trust and SASE technologies

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	is able to…	**Authentication and authorisation technologies**	verify the user's identity using basic methods; implement and maintain authentication and authorisation technologies	report incidents relating to identity and access; apply various identity and access management technologies and systems (e.g., Active Directory, Microsoft Azure AD, SSO)	select a scheme for granting and verifying permissions within an organisation; determine optimal methods of identity and access management	administer user accounts, roles, and access rights, applying the principles of least privilege and compliance with security policies; design complex identity and access management methods; automate access management (AD/IAM) processes and integrate permissions	implement and maintain solutions for authentication, authorisation, and access auditing using tools and scripts that automate identity and access management	
	knows and understands…	**Storage and file systems**	the types of storage and file systems	the principles of selecting storage and file systems; the principles of configuring NAS servers	the principles of checking and restoring file system integrity; the principles of data protection; the principles of configuring arrays using RAID technology	the principles of verifying the accuracy of collected data; an organisation's backup policies (including issues relating to the retention of media/copies, backup strategies, and rules for storing copies/media); the principles of allocating array resources to operating systems	the principles of configuring storage arrays and server clusters; data replication principles; storage architecture for organisations	
	is able to…	**Storage and file systems**	use various types of storage and file systems	prepare storage for use (e.g., create partitions, volumes); configure NAS servers	check and restore the integrity of file systems; configure parameters to ensure data stability and security; configure arrays using RAID technology	check data quality; create an organisation's backup policies (taking into account issues relating to media/backup retention, backup strategies, and rules for storing backups/media); manage storage resources allocated to operating systems	configure storage arrays and server clusters; configure data replication; configure the mass storage architecture for an organisation; create virtual mass storage networks (e.g., SDS)	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	knows and understands…	**Managing operating systems**	basic types of operating systems (e.g., server, desktop, and mobile); file structure; basic system services; the structure of user accounts, permissions, and services	the differences between server and desktop systems; the principles of resource management (e.g., RAM, CPU, disk); the principles of user and permission management in a distributed environment; the basic principles of directory services (e.g., LDAP/AD); common system scripts	the principles of managing multiple systems in a distributed environment; virtualisation, containerisation, and backup mechanisms; the structure of domains, OUs, GPOs, and security policies	operating system architecture and its impact on performance and availability; the interdependencies between the operating system layer and applications and hardware	the methods of designing relationships between operating systems in the context of IT architecture, security, compliance, and automation	
	is able to…	**Managing operating systems**	install an operating system; create local user accounts; execute basic operating system commands	configure the operating system; monitor system performance and resolve common problems relating to the functioning of the operating system; manage the attributes and permissions of local users; perform basic administrative tasks and implement basic security configuration	design and implement system security policies, secure the system, and analyse operating system logs; manage system and network services (e.g., DNS, DHCP, NTP); administer user account attributes and groups in LDAP/AD across distributed systems; configure password, permission, and access policies; create system scripts	optimise system configurations in terms of performance and resources; create backup and recovery procedures; manage distributed environments; manage security policies in a distributed environment	design complex system environments; select operating system technologies in accordance with business requirements; audit and assess the compliance of operating systems and services with IT norms and standards; manage security systems and policies in multi-domain environments; integrate AD/LDAP with cloud systems	
	knows and understands…	**Managing system services in an IT environment**	basic system services (e.g., DNS, DHCP, NTP, directory services, printing services)	the role of system services in the IT environment; methods of monitoring system services	advanced system services (e.g., SNMP, RDP, SSH, PKI, VPN, WSUS, syslog); the relationships between system services and IT infrastructure; the basics of service management in a client-server model; the impact of time synchronisation on security and compliance	the architecture of system services in multi-domain environments; the impact of system service configuration on the security and performance of the IT environment; the impact of and interdependencies between system services on an organisation's business continuity	the principles of scaling, redundancy, and high availability of system services; logs collected from individual system services and their significance for the security of the IT environment	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	is able to…	**Managing system services in an IT environment**		start and configure basic system services at the local level; monitor the availability of system services and report related problems	configure and maintain system services (e.g., DNS, DHCP, SNMP, NTP, RDP, SSH, directory services, printing services); diagnose and resolve common problems with the operation of system services; ensure time synchronisation across all servers within an organisation's environment; manage digital certificates; manage secure remote access (e.g., VPN, RDP)	design and implement system services in multi-domain environments; create technical documentation and operating procedures for system services; integrate system services with other infrastructure components; manage updates and system security for the environment (e.g., WSUS, SCCM)	optimise the configuration of system services; design service management policies in line with business and regulatory requirements; audit and improve system service delivery processes; manage centralised log collection; select technologies and service delivery models (on-premises, edge, cloud-native) to meet an organisation's business needs; assess the risk of disruption to system services and their compliance with standards	
	knows and understands…	**Embedded and real-time systems**		the basic concepts and differences between embedded systems and real-time systems; the practical basics of the runtime environment	the differences between general-purpose systems and embedded systems; the concepts of safety, reliability, and resilience in real-time and critical systems; the architecture of embedded systems (e.g., microcontroller, memory, interfaces, sensors); the basic mechanisms of RTOS operation (e.g., tasks, priorities, scheduling)	the principles of designing and implementing real-time systems, taking into account timing requirements; the impact of hardware constraints on software design	standards and norms for critical systems; communication and task synchronisation models in RTOS	the latest methods of designing real-time critical systems and highly reliable embedded systems

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	is able to…	**Embedded and real-time systems**		recognise an embedded system and its main components; recognise a real-time system; run a simple microcontroller control program	develop applications for microcontrollers using basic RTOS functions; implement prioritised tasks and test their concurrent operation; analyse basic synchronisation errors and resource deadlocks; use basic tools for programming and debugging embedded devices	develop software for resource-constrained embedded systems; integrate hardware and software components in real-time systems; analyse system performance, latency, and reliability	conduct risk and functional safety analysis; implement solutions ensuring deterministic operation and compliance with safety standards	design modern real-time critical systems and highly fault-tolerant embedded systems
	knows and understands…	**Business continuity, backups, and disaster recovery**		the types of backups (full, differential, incremental); the principles and procedures for backing up physical and virtual environments; backup tools; the technologies for backing up physical and virtual environments	the principles and procedures for disaster recovery; the tools for disaster recovery; the procedures for ensuring the continuity of an organisation's IT infrastructure; the strategy for ensuring business resilience and the continuity of key business processes during and after a failure, including in hybrid environments	the comprehensive set of principles and standards of business continuity within an IT organisation; the principles of risk analysis within an organisation relating to the business continuity of IT systems	the procedures for developing a strategy for the business continuity of IT infrastructure to maintain key business processes; the trends in building resilience using predictive models; the use of AI, automation, and cloud solutions (e.g., Disaster Recovery as a Service—DRaaS) in building business continuity	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	is able to…	**Business continuity, backups, and disaster recovery**		apply standard procedures to ensure the business continuity of an organisation's IT infrastructure; create backups in accordance with the procedure; document the backups created	develop procedures for restoring and recovering backups; identify and assess the risks of system failure and data loss; select the type of backups; test backups and verify their integrity; restore the IT environment and/or data from backups (in accordance with the procedure); document the backup recovery process; report incidents relating to breaches of business continuity and backups	develop procedures to ensure the continuity of IT infrastructure operations; conduct a risk analysis within an organisation relating to the continuity of IT systems; manage backups using sophisticated security and optimisation tools; implement redundant solutions (e.g., clusters, multi-site setups, cloud solutions); plan and implement remedial actions in crisis situations within an IT organisation; apply optimal solutions to ensure rapid recovery in order to minimise losses; conduct backup recovery tests	use advanced methods and tools for monitoring and preventing (using predictive analysis) failures and attacks that disrupt the continuity of IT systems; use automation for backup creation, restoration, and verification of correct data recovery or environment restoration; develop business continuity and IT system continuity plans	
	knows and understands…	**Integration with cloud solutions**	basic cloud solutions and applications	the difference between an on-premises environment and a cloud environment; the basic methods of service synchronisation; the security methods for cloud environments	the principles of local network integration with the cloud; the methods of resource integration and collaboration with the cloud; basic integration patterns (e.g., point-to-point, shared database, file exchange, API); the methods of synchronising accounts and settings between on-premises and cloud environments	the methods of selecting suitable mobile applications to support cloud solutions; the principles of designing hybrid connections; the mechanisms for synchronising identities and permissions; the methods of periodic and event-driven synchronisation	the methods of testing and implementing appropriate quality standards for the integration of cloud solutions; the integration patterns for hybrid and multi-cloud environments; the methods of ensuring service consistency, including directory services	the trends in new solutions such as cloud bursting, edge computing, and service mesh

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
I. IT infrastructure	is able to…	**Integration with cloud solutions**	use cloud applications	use a pre-configured connection (e.g., VPN) and check basic connectivity; report a lack of access to the service on the cloud side	integrate data with the cloud; describe the network requirements for the cloud service; specify the synchronisation cycle for services communicating with the cloud; launch applications to utilise data from the cloud; implement security measures for small cloud environments	prepare an integration specification, including communication between local and cloud infrastructure components; set up user account synchronisation; implement security measures for large cloud environments	test, analyse, and ensure data security in the cloud; develop a standardised description of a hybrid solution, including for critical systems; determine the minimum acceptable level of downtime for hybrid infrastructure	develop innovative solutions utilising cloud bursting, edge computing, and service mesh
	knows and understands…	**Data centre management**	the basics of IT infrastructure; the types of equipment in a data centre; basic health, safety, and physical security principles	the principles of cabling and the configuration of simple connections; the principles of operating and selecting UPS systems and generators; the basics of server room cooling; the principles relating to fire detection and suppression in a data centre; typical infrastructure risks in a data centre	data centre architecture; redundancy and the high availability (HA) of equipment in a data centre; documentation standards (e.g., TIA-942)	the design of network topologies in data centres (e.g., spine-leaf); the design of redundant power supply systems; energy consumption and efficiency metrics monitoring; energy and environmental standards relating to the operation of data centres; data centre security policies	the design and expansion of data centres in line with business requirements; risk management and data centre business continuity plans; data centre operational standards (e.g., ISO/IEC 22237, Uptime Institute Tier Standard); the principles of cooperation with network operators and service providers	the trends in newly designed data centres (e.g., edge, green IT, DLC—direct liquid cooling); the assessment and implementation technology for innovative, alternative energy sources (e.g., photovoltaics, SMR, energy storage)
	is able to…	**Data centre management**	perform simple maintenance tasks relating to the operation of a data centre; monitor basic performance indicators of the equipment installed in a data centre; report incidents relating to the operation of a data centre	monitor the environment (temperature, humidity); diagnose equipment installed in a data centre; assist with infrastructure deployments	manage servers and networks; plan the maintenance and inspections of a data centre; implement backups (e.g., tape backups, deduplication)	coordinate the work of the technical team assigned to a data centre; design network topologies, power supply systems, and monitoring systems; optimise data centre resources; produce reports (on availability, environmental conditions, security, maintenance and inspections, incidents, changes, compliance with procedures)	plan investments in data centres; select technologies and suppliers for a data centre; oversee a data centre's compliance with norms and standards; implement BCP and DRP procedures in a data centre	develop new strategies for a data centre's development; assess the environmental impact of new technologies used in a state-of-the-art data centre and manage IT innovations

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	knows and understands…	**Local Area Networks (LAN)**	the basic components of local area networks (hubs, switches, network interface cards); the types of cabling (e.g., twisted pair of a specific category, single-mode and multi-mode fibre optic cables); the rules for accessing local area networks within an organisation; the concepts relating to IP addressing; the principles of the physical addressing of network devices (MAC); the basic elements of local area network infrastructure; communication layers (OSI, TCP/IP)	the architecture of local area networks; the basic parameters and limitations of local area networks (e.g., network segment lengths); basic protocols (e.g., Ethernet, ARP, DHCP); the differences between network topologies (e.g., bus, star, ring, mesh, tree); the differences between the types of wired networks; the tools for managing network devices; the tools for updating network devices, including firmware updates; the principles of network segmentation (VLAN) and security; the principles of configuring devices for building local area networks (e.g., switches)	the principles of LAN design; the principles of redundancy in network design and device interconnections; management protocols (SNMP); Quality of Service (QoS) configuration methods; the principles of optimisation, auditing, and the standardisation of configurations in LANs; the tools for monitoring network performance and security	advanced LAN mechanisms (e.g., STP, RSTP, MSTP); the operation of network security tools (e.g., NAC, 802.1X, ACL); the devices for diagnosing network connections; the principles of integrating LANs with WANs and the cloud; IaC tools for network configuration and management	LAN architecture in large organisations; the principles of implementing and managing SDN architecture using control plane centralisation to optimise data flow and automate device configuration; configuration automation mechanisms (e.g., Ansible, NetConf)	
	is able to…	**Local Area Networks (LAN)**	install and configure basic network components; connect devices to a LAN; configure simple IP addressing; set up internet access using various technologies (DSL, cable, fibre optic); check the network connection (ping)	configure network switches; configure basic VLANs; diagnose common network problems; document the local network configuration; use tools for managing network devices; configure and update network devices	design and implement LANs within an organisation; configure VLANs, trunking, and basic ACLs; monitor network performance and respond to incidents; use network monitoring tools to ensure network performance and security	optimise LAN configuration; identify the location of faults in LANs; implement security policies in LANs; implement QoS policies	design a LAN development strategy at an organisational level; use SDN technology; select network technologies and management models in line with business and regulatory requirements	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	knows and understands…	**Wireless networks (WLAN)**	the basic principles of using WLAN networks; WLAN standards (802.11 a/b/g/n/ac/ax); basic WLAN terms (e.g., AP, Wi-Fi, SSID, password); the basics of WLAN security (e.g., WEP, WPA, WPA2, WPA3); basic wireless network devices (e.g., AP, controller, repeater)	differences between wired and wireless networks; use of PoE technology	basic WLAN topologies (e.g., BSS, ESS, IBSS, mesh); the standards and applications of IoT wireless networks (LoRa, Sigfax, NB-IoT)	the principles of WLAN design; radio channels and interference; roaming principles; authentication mechanisms (802.1X, RADIUS)	advanced WLAN management mechanisms (controllers, centralised management, SSID segmentation); the principles of WLAN integration with the cloud and 5G; the regulatory standards for wireless networks (e.g., power limits); global satellite internet systems and mobile versions	the latest technologies using AI in wireless networks for diagnostics and security
	is able to…	**Wireless networks (WLAN)**	connect a device to a WLAN network; configure basic wireless network settings (e.g., SSID, password)	configure network devices using PoE technology; configure simple WLAN access points; set up WLAN security (e.g., WEP, WPA, WPA2, WPA3)	diagnose basic WLAN connection problems; connect and configure a sensor for data transmission in an IoT network (e.g., LoRa or NB-IoT); configure and integrate a satellite system at the service delivery site	design and implement large-scale WLAN networks within an organisation; plan the use of radio channels and avoid interference; configure WLAN controllers and access policies; monitor WLAN performance and respond to incidents	optimise WLAN configurations; implement security and QoS policies for WLANs; audit and improve WLAN management processes	design and implement advanced WLAN networks using the latest technologies, particularly AI
	knows and understands…	**Wide area networks (MAN/WAN)**	the OSI model; the TCP/IP, IPv4/IPv6 protocol suite; basic protocols (e.g., NAT, DHCP, DNS); network infrastructure components (e.g., routers, modems, switches)	WAN, MAN, and LAN architectures and their interdependencies; the security rules for WANs; routing protocols (e.g., OSPF, BGP, RIP, EIGRP); the routing protocols and communication standards used in wide area networks (WANs)	network monitoring tools (e.g., Wireshark, SNMP, SolarWinds, Zabbix); wide area network architecture; network segmentation, clusters, traffic encryption; the automation of the configuration and operation of network devices	WAN/MAN design principles; the methods of diagnosing delays, packet loss, jitter, and routing problems; distributed networks; the use of SD-WAN; advanced networking mechanisms (e.g., MPLS, QoS); the principles of optimising, auditing, and standardising configurations in wide area networks	advanced WAN management mechanisms (routers, UTMs, controllers, WAN segmentation); the policies relating to the security of WAN operations; the integration of wide area networks with the cloud	the directions for developing and using quantum networks in digital communications

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	is able to…	**Wide-area networks (MAN/WAN)**	identify typical problems associated with network operation; use basic diagnostic tools (e.g., ping, traceroute)	use network technologies (e.g., VPN, IPsec, SSL VPN, BGP, OSPF, EIGRP); perform simple configuration tasks	configure advanced router and switch functions, including the automation of their operation; utilise UTM capabilities; monitor network performance and availability;	design and implement wide area networks (WANs); design and implement network migration processes; create technical documentation and network diagrams; configure network components and WAN management policies; monitor WAN network operations in accordance with security and WAN administration policies (e.g., security incidents or business continuity)	optimise and configure WAN/MAN; manage security policies for WAN/MAN; optimise and audit WAN management processes; design wide area network architecture	
	knows and understands…	**Internet services**	the basic types of internet services (e.g., web, email, FTP); the basic relationships between categories of other internet services	how internet services work; the operation of networks and web applications	the principles of load balancing and high application availability; the use of load balancing in the context of L4 vs. L7 layers	the principles of designing the availability of web services; load balancing algorithms (e.g., Round Robin, Least Connections, Weighted RR, IP Hash); session persistence mechanisms; the methods of maintaining the high availability of web services (High Availability); failover mechanisms; distributed content delivery network (CDN) technologies load balancing tools (e.g., HAProxy, NGINX, F5 BIG-IP, Traefik, Envoy)	the advanced mechanisms for reducing the load on the application server and increasing its performance (e.g., TLS/SSL termination or offloading); cloud balancing methods (e.g., AWS, GCP, Azure); strategies for protecting against overload as well as DoS and DDoS attacks; the methods of automatically monitoring system health (health checks)	the latest technologies for optimising network traffic and service availability using AI

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	is able to…	**Internet services**	use basic types of internet services	assess the correct functioning of basic tools for providing internet services	diagnose common problems relating to the availability and performance of internet services	design and implement solutions for load balancing and improving the availability of internet services; apply methods to maintain the high availability of web services; monitor the operation of web services and respond to incidents; use distributed content delivery networks; use load balancing tools	optimise the performance of application servers using advanced mechanisms; apply cloud-based load balancing methods; anticipate and counteract the risks of overload as well as DoS and DDoS attacks; audit the operation and monitoring of web services; design distributed content delivery networks	design and implement fast internet services that have a high degree of reliability and security
	knows and understands…	**Network monitoring and maintenance**		the principles of ensuring IT network business continuity at a basic level; the methods of analysing network traffic (bandwidth, load, latency); the basic tools for monitoring IT networks	common types of IT network failures; the methods of identifying vulnerabilities and performance problems in IT networks; the tools for monitoring network performance and analysing logs (e.g., NetFlow, sFlow, Nagios, Zabbix, PRTG)	the tools for analysing network traffic; the methods of detecting unauthorised activities and potential IT network security threats; the methods of optimising the use of network resources	security policy principles and applicable regulations necessary to ensure network continuity; the trends in network development and modernisation	
	is able to…	**Network monitoring and maintenance**		ensure basic IT network continuity; diagnose basic IT network maintenance problems (loss of connectivity, overloads); perform routine maintenance tasks (e.g., restarting devices, updating)	detect and prevent IT network failures; identify bottlenecks and performance problems in the IT network; monitor IT network performance; configure systems to monitor and provide alerts relating to IT network performance	identify IT security threats (unauthorised activities); optimise the use of network resources; plan the development and modernisation of IT networks; create scripts to manage network devices; select and use tools for analysing network traffic (e.g., Wireshark, Cloudshark)	ensure network continuity in accordance with applicable security policies and regulations	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	knows and understands…	**Network and internet security**	the types of network threats; basic security concepts (e.g., NAT, DMZ, guest networks)	the types of firewalls depending on, among other things, implementation or technology; the role of a firewall in protecting a workstation and a small local area network; the principles of network traffic filtering	the principles of how next-generation firewalls (NGFW) work; the basic functions of IDS and IPS systems; the methods of analysing security incidents; the methods of classifying digital content	network security architecture, including next-generation firewalls; the principles of operating network threat detection engines; the concepts of zero trust, micro-segmentation, and multi-layered protection (defence in depth); the impact of firewall configuration on service availability and network performance; the methods of protecting against DDoS attacks; SIEM and SOAR tools	threat models and attack scenarios that take into account local infrastructure and cloud environments; the methods of assessing the effectiveness of implemented solutions (FW/NGFW/IPS/IDS) based on metrics, tests, and security audits; the impact of new technologies and trends (e.g., SD-WAN, SASE, XDR) on the design of network security architecture; the methods of integrating security tools (e.g., SIEM, SOAR, XDR, AV)	
	is able to…	**Network and internet security**	recognise basic types of network threats	create simple traffic filtering rules on an edge device; interpret entries in network device system logs	configure firewall rules; design simple firewall policies for a small network; implement simple IDS/IPS scenarios; interpret entries in FW/IDS/IPS system logs; apply methods of classifying digital content	design network security policies; configure next-generation firewalls; select and fine-tune IDS/IPS profiles to protect key services; integrate FW/NGFW/IDS/IPS with logging and monitoring systems; apply/create basic access control lists (ACLs); design an architecture resilient to DDoS attacks	design SIEM integrations with security systems; design and implement automation workflows in SOAR for network incidents	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
II. Network technologies	knows and understands…	**Network orchestration**	network infrastructure components (e.g., SDN controllers and control planes); the concept of network virtualisation	the application of SDN architecture (Application Plane, Control Plane, Data Plane); flow tables; how OpenFlow protocols work (at a basic level)	the use of different types of SDN architectures (e.g., hybrid, centralised); the principles of API operation (e.g., REST, NETCONF, gRPC); network functions virtualisation (NFV) architecture; the concept of Service Function Chaining (SFC)	the use of network virtualisation protocols (e.g., details of OpenFlow, NETCONF, RESTCONF); data modelling principles (e.g., YANG)	the impact of the latest solutions in the field of network orchestration (e.g., Intent-Based Networking); the integration of high availability and disaster recovery (HA/DR) models for SDN controller clusters; the methods of creating full service lifecycle management policies	
	is able to…	**Network orchestration**	log in to a simple SDN monitoring interface; identify basic network elements (e.g., ports) in the interface; execute a command (e.g., check the status of the controller service)	set up a simple virtual SDN controller (e.g., in Mininet); monitor the status and basic metrics in the controller interface; implement and verify the operation of simple, static routing	use the controller API to dynamically configure the network; analyse and resolve problems relating to data flow (e.g., errors in flow tables); implement and manage a simple NFV service chain	design and implement a comprehensive SDN/NFV architecture for a small network; develop and implement advanced automation scripts (e.g., for provisioning); integrate SDN solutions with cloud systems	design and evaluate mechanisms ensuring high availability and resilience of SDN controllers; conduct performance and security tests (e.g., penetration tests) on SDN systems; recommend SDN optimisations; develop documentation for SDN implementation standards; develop policies for managing the full lifecycle of a service	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	knows and understands…	**Requirements analysis**		the basic concepts relating to requirements analysis; the basics of the UML standard; the methods of developing use case diagrams	the methodology for requirements analysis and system modelling (UML, BPMN); the methods of developing class diagrams; non-functional requirements (NFR)	the methods of developing behavioural diagrams, including object flow methods	the methods of developing implementation diagrams (component and deployment diagrams)	
	is able to…	**Requirements analysis**		understand the context of the software being developed in accordance with the requirements; define simple diagrams in UML	analyse the relationships between the requirements of individual object classes; determine user and organisational requirements in the context of the software being developed; model class diagrams; interpret BPMN diagrams; describe the behaviours, functions, and operations that the system must perform	create IT system models; model behavioural diagrams; analyse the relationships between software and IT system components; create BPMN diagrams; understand business requirements in the context of the software being developed	create implementation diagrams (component and deployment diagrams)	
	knows and understands…	**Design**	the role of design in the software development lifecycle; the importance of technical documentation in an IT project	basic design patterns; basic data models	IT system architecture (e.g., three-tier, client–server); design methodologies; the relationships between requirements and system design	advanced design patterns (e.g., MVC, Observer); the impact of design decisions on costs, risks, and future software development; API design and system integration	design of distributed and microservice systems; the principles of designing IT systems with high availability, scalability, and security	new trends in system design with the potential for AI integration; novel methods of assessing the innovativeness of solutions

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	is able to…	**Design**	create simple block diagrams; use design documentation	create simple UML diagrams; model simple systems; create simple data models	design system components in accordance with requirements; analyse design risks; produce design documentation in accordance with standards; identify functional and non-functional software requirements	design components and workflows; solve highly complex design problems; conduct reviews of IT system designs	design distributed and microservice systems; design IT systems with high availability, scalability, and security	develop new innovative design patterns with the potential for AI integration; verify the impact of new solutions on availability, scalability, and security
	knows and…	**UX/UI Design**	the role of UX/UI design in software development	the basic concepts and principles of UX (user experience) and UI (user interface)	the user experience design process; the principles of user-centred design (UCD); the principles of interaction design (user flow); the tools and software for interface design	the principles of digital accessibility and interface ergonomics; the tools and software supporting the development of prototype models	UX/UI research methods to improve software usability	
	is able to…	**UX/UI design**		create a static outline of the structure of an application/ website/program/system (wireframe)	create a visual representation of the design (mock-up); ensure the visual and functional consistency of the solutions created	create an interactive prototype using UX/UI tools; conduct a UX usability audit, including a check of accessibility guidelines; conduct usability tests	apply appropriate test methods and types of UX tests	
	knows and understands…	**Programming**	the basics of algorithms; the basics of coding; the types of programming languages; IDE development tools; the importance of the structure and usefulness of technical documentation for hardware and software environments	the basics of structured and object-oriented programming; the types of databases	the GIT-type environment (version control); frameworks and libraries (including open-source) supporting application development; the software development lifecycle	the range of programming languages and tools supporting code and application development; programming tools and methods of distributed and cloud-based solutions; microservice-oriented programming; the potential of AI, no-code, and low-code approaches for software development; REST API and SOAP web technologies; the principle of idempotence	cloud programming methods; cross-platform programming methods	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	is able to…	**Programming**	develop a workflow diagram for a requirement	use IDE programming tools; program a simple process using a database; write code in at least one programming language; create simple code snippets with the support of AI assistants; verify that the code syntax generated by AI is correct	analyse simple code, including identifying logic and syntax errors; use programming libraries and frameworks; use a GIT-type environment (version control); monitor the performance of the code and the changes made to the application; refactor and optimise code as suggested by GenAI tools; apply the principles of clean code; develop and implement software representations of object-oriented models of systems and processes	program in multiple programming languages and their ecosystems; use no-code and low-code platforms; use AI to generate code and automate routine tasks; integrate applications using various network methods and technologies (APIs); ensure the idempotence of operations; conduct security audits of AI-generated code (AI Code Review) for vulnerabilities and business logic; integrate coding assistants into the CI/CD pipeline	program in a hybrid cloud; perform cross-platform programming	
	knows and understands…	**Deployment**		industry-specific deployment terminology; the IT environment relevant to deployment; the type and stages of deployment; the business requirements of deployment	the technologies relating to the subject of the deployment; the principles of planning deployment stages (technical and implementation-related); the functioning of the system being deployed; the methods of managing the deployment project, including change management; deployment security principles	the methods of system analysis and gathering user requirements (pre-deployment analysis); system testing methods; data migration procedures	the principles of planning the deployment schedule; deployment technologies (traditional, CI/CD) the principles of planning data migration and system configuration; the methods of analysing and optimising deployment costs; industry-specific deployment terminology and the legal framework of deployment	modern and innovative deployment methods and trends, e.g., Blue-Green Deployment, Strangler Fig Pattern

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	is able to…	**Deployment**		define the functionality of an IT system; configure basic software functions; install software, transfer and migrate data	plan the stages of system deployment; verify and document the project being deployed in accordance with the methodology, including change management; plan and conduct training on the system being deployed; configure and parameterise the system's functions	manage the deployment project in accordance with the methodology; apply technologies to optimise the deployment process; apply testing methods; plan the data migration process	agree on the details of the deployment as well as the division of work into stages; analyse the client's requirements (pre- deployment analysis); take into account the legal aspects of deployment; plan the deployment and its stages (technical and software-related); manage the migration process and data verification; manage the deployment process in accordance with the agreed approach	apply modern deployment methods
	knows and understands…	**Testing**		testing objectives; the basic concepts relating to testing (e.g., test scenario, types of tests); the classification of test environments; manual testing methodology	the full testing cycle, including the structure of API requests; the boundary values of test cases; the principles of preparing data for testing; acceptance testing methodology; test management tools; autonomous testing	the selection of strategies for test risk; unit, integration, and system tests; the types of non-functional tests; the methodology for defining test metrics; the structure of an automated test; exploratory tests; test isolation techniques	the methodology for combining different types of tests; the principles of integrating the testing process with the development cycle (e.g., DevOps); the potential for using AI in system testing	
	is able to…	**Testing**		define test cases; check a prepared test case; document test results, and in particular, report a bug with the necessary conditions for replicating the case	plan test cases for all requirements, including for the API; verify scenarios for acceptance testing; use test management tools; deploy and monitor autonomous testing agents	design and perform unit tests; design and perform integration tests; design and perform system tests; design automated tests; design exploratory testing sessions; design performance, security, usability, and reliability tests	prepare a report on the solution's readiness for implementation; manage test data and verify the coverage of tests generated automatically by AI; formulate corrective and preventive actions for recurring errors; update CI/CD pipelines by adding automated tests, and use AI to test systems	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	knows and understands…	**Maintenance and development**		the methods of maintaining IT systems; the methods of IT system development; the differences between methods of maintaining and developing IT systems resulting from the way an organisation operates; the methods of handling requests regarding the operation of existing IT systems	the methods of managing changes in operational IT systems; the methods of monitoring operational IT systems	the methods of maintaining the continuity of IT system operations; the methods of developing IT systems; the principles of optimisation and automation in accelerating software development; continuous integration and system development practices (CI/CD, DevOps) in accordance with security policy	the methods of implementing new IT system functionalities; the methods of applying innovative solutions in the maintenance and development of IT systems; the methods of assessing the effectiveness of IT systems, their monitoring and auditing	
	is able to…	**Maintenance and development**		categorise reports concerning operational IT systems; handle requests concerning operational IT systems	update the environment in connection with the change being implemented; use tools to monitor IT systems	maintain and develop systems in the Dev/Sec/Ops environment; develop concepts for system modifications and changes, taking into account corrections, version stabilisations, improvements, and modifications; use automation tools (including AI) for the development and maintenance of IT systems	manage the policy for the maintenance and development of IT systems; integrate applications (including in real time); optimise the costs of maintaining and developing IT systems; adapt IT systems to changes in the environment (including technological, legal, and business changes)	
	knows and understands…	**Documentation**	the basic concepts and principles of documentation	the differences between types of documentation, e.g., functional and technical; team collaboration and knowledge management platforms, such as Confluence, Jira, and Miro	the principles of documentation versioning, including the documentation lifecycle; documentation and knowledge management standards, documentation formats (e.g., Markdown, AsciiDoc); notation methods of diagram modelling and visualisation (UML, BPMN)	tools for automating documentation generation (e.g., Swagger/Open API, Redocly, Doxygen, Sphinx, Javadoc)	trends in the development of IT documentation management strategies; the optimisation of API documentation using AI capabilities	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
III. Software engineering	is able to…	**Documentation**	create a simple user guide, e.g., a README	create user manuals or user documentation; document changes in a changelog	manage versions of IT documentation; create user documentation for a module/component/system (e.g., manual, tutorial); document a list of tasks, requirements, and functionalities (e.g., Dev/Ops, backlog)	create IT system design documentation; generate automated technical documentation; create documentation templates; implement knowledge repositories	set standards for the creation of IT documentation; manage knowledge and documentation using the latest documentation tools	
	knows and understands…	**Organising development and deployment teams**		the basic structures of development and deployment teams; the tasks of development and deployment teams depending on the organisational structure; standard and current system deployment methodologies; design patterns and software development principles	the principles of establishing and operating dev/ops and dev/ops/sec teams (continuous integration/ continuous delivery—CI/CD); the project methodologies appropriate for an organisation and the purpose of the software; the importance of selecting appropriate tools for managing software development and deployment; the tools for managing the development and deployment team and for project communication (e.g., Slack, Teams, Jira)	microservices as a transformation in software development and the decomposition of monolithic systems; the tools for automating software development processes (e.g., Jenkins)	IT's wide range of technological diversity when selecting the working environment for development and deployment teams (e.g., frameworks); the organisation of specialist development and deployment teams	the need to build innovative interdisciplinary teams with developers to deliver digital innovations; the use of various modern design methodologies and innovations, including AI, in software development; the importance of leadership in development and deployment teams
	is able to…	**Organising development and deployment teams**		define the team's operating procedures; define the scope of a programmer's duties within a given organisation; document work in accordance with programming standards; define the stages of system deployment	apply solutions such as test-driven development in practice; apply methodologies for an effective programming process (e.g., Agile, Scrum); use tools for collaborative code editing (e.g., GitHub, GitLab);	implement programming tasks in accordance with the proposed architecture and good programming practices; define the terms of the development and deployment service contract in the dev/ test/prod environment	manage development and deployment teams; organise independent work for a development and deployment project	provide, create, and implement a range of innovative tools and techniques, including AI, that accelerate the software development process; propose innovative solutions tailored to the needs of development and deployment teams; lead the development and deployment team and manage the process of creating innovative solutions

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IV. Digital applications and services	knows and understands…	**Digital service platforms**	the differences between a traditional application and a service platform; the rules for using the solutions offered on the service platform	the basic concepts relating to service platforms; basic security and authorisation principles for platforms; the basic concepts relating to the use of internal service platforms	the types and applications of digital service platforms; the principles of making services available in the form of APIs, modules, or components; typical security mechanisms used in service platforms	the principles of designing new services using available modules; the principles of the monitoring, scalability, availability, and security of platform services; advanced methods of integrating platforms with systems	advanced security and regulatory compliance models for digital services the trends, development directions, and the integration of service platforms with systems in an organisation	modern approaches to developing innovative services on digital platforms
	is able to…	**Digital service platforms**	use the service catalogue; launch individual services	configure a simple service based on known parameters; report problems and platform malfunctions	configure and launch services on the platform; perform basic functional tests of services; manage permissions, roles, and workspaces within applications	design new services or service modules in accordance with platform standards; identify bottlenecks and performance problems to optimise the operation of existing services; conduct functional tests of services and security on the platform	establish standards for the development and maintenance of services, including quality, performance, and security policies; oversee the implementation of digital services within an organisation; manage the digital services portfolio and guide their development within an organisation	set new trends and directions for the development of service platforms within the global digital ecosystem
	knows and understands…	**Accessibility**	the principles of digital accessibility, including WCAG	the role of accessibility in UX/UI design; the tools supporting accessibility	the advanced methods of designing accessible interfaces; national and EU legislation and standards on accessibility; the principles of designing content and media accessible to users	the methods of designing accessible solutions for IT devices and systems; how to integrate accessibility requirements into CI/CD processes; the impact of accessibility on business and the user experience	digital accessibility strategy and quality policies; the trends and innovations in accessibility	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IV. Digital applications and services	is able to…	**Accessibility**	create materials compliant with WCAG	use accessibility testing tools; identify and classify accessibility problems; conduct website accessibility audits	implement measures to improve accessibility in projects; develop accessibility guidelines for project teams; conduct accessibility audits of applications and electronic documents	coordinate accessibility projects across an organisation; incorporate accessibility requirements throughout the software development process, including for devices delivering digital services; assess the effectiveness of implemented accessibility solutions	develop and oversee an organisation's accessibility policy; analyse trends and innovations in the field of accessibility	
	knows and…	**Application and service lifecycle management**		the stages of the application lifecycle (e.g., planning, development, deployment, maintenance, decommissioning); application version management tools	the methods and standards of managing the lifecycle of applications and digital services; the guidelines for managing versions, releases, and decommissioning within an organisation	complex application and digital service lifecycle management processes in a multi-service organisation	the strategic management of the application and service portfolio	
	is able to…	**Application and service lifecycle management**		record and update information on versions of applications and digital services; report and document the need to make changes or retire applications	plan releases and updates of applications and digital services within an agreed schedule; coordinate application maintenance activities and pre-deployment testing with business users (CI/CD practices)	design and deploy automated processes; manage risk and the continuity of digital services; monitor the status of the project throughout the application lifecycle	define and implement a strategy for managing the application and digital service lifecycle across an entire organisation	
	knows and understands…	**Monitoring**	basic application and service metrics; the basics of event logging in applications; basic concepts of web analytics	the tools for monitoring applications and digital services; the process of monitoring user behaviour	the principles of developing and collecting metrics for measuring the performance of digital applications and services with monitoring tools (e.g., Prometheus, Grafana); the principles of application log analysis; the impact of monitored parameters on the availability of applications and services	the relationships between application layers and how errors propagate; the correlation of technical metrics with business metrics	the trends and opportunities for using AI in application data analysis; the relationship between monitoring and the concept of observability for the analysis and optimisation of IT infrastructure and services, and for mitigating vulnerabilities in real time	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IV. Digital applications and services	is able to…	**Monitoring**	read data from tools that monitor applications and digital services; identify the basic symptoms of user problems based on simple error messages and service statuses; record incidents relating to the monitored parameters of applications and digital services	use ready-made dashboards to monitor applications; read basic statistics (e.g., from Google Analytics)	create and analyse basic application dashboards; recognise and describe typical anomalies in the operation of applications and digital services; define metrics and dependencies for all types of applications and technological environments in monitoring tools (e.g., Prometheus, Grafana)	analyse the root causes of problems by correlating statistics from different application components; implement and develop application monitoring standards; collaborate with product teams to define service level indicators and service level objectives (SLI/SLO) as well as alert thresholds		
	knows and…	**Distribution models and monetisation**		the basic models for distributing digital services; basic licensing and subscription terms for applications	the types of licensing and monetisation arrangements; the key differences in the costs, operations, and business risks of distribution models	the impact of application and service architecture on the distribution model and monetisation; the risks associated with the monetisation of digital services	the management of monetisation models across an entire organisation; the regulatory and economic frameworks of subscription models; current market conditions in the context of monetisation	
	is able to…	**Distribution models and monetisation**		distinguish between types of licences and subscriptions; maintain a licensing/ subscription model for a given application/service	analyse basic usage data for the application and the new digital service; compare licensing and subscription offers from different providers; identify opportunities to optimise licence and subscription procurement plans	design a distribution and monetisation model for a new or developing service; propose a monetisation concept for a portfolio of digital services and applications; assess the potential risks associated with proposed solutions for the monetisation of digital services	design and oversee the implementation of complex, multi-channel monetisation models; develop a long-term monetisation strategy for the portfolio of digital services and applications; conduct market analyses in the context of digital service monetisation	
	knows and…	**Systems integration**		the basic methods of system integration; the basics and limitations of REST APIs	advanced API concepts (e.g., authentication, rate limiting); API design principles (e.g., RESTful); the basic principles of ESB as a central integration hub; the use of HTTP/REST and SOAP	error handling mechanisms during system integration; the impact of system integration on application security and performance; advanced methods of system integration	hybrid approaches to systems integration, particularly using APIs; the strategy for integrating systems within an organisation	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IV. Digital applications and services	is able to…	**Systems integration**		use ready-made tools and scripts to communicate with APIs; use existing APIs to retrieve or send data	design, deploy, and document APIs; integrate systems by developing custom API clients with secure authentication; use data bus tools to integrate systems	select the system integration method depending on the architecture; optimise the performance of system integration; design and deploy complex, error-resilient integration architectures between systems	define standards and best practices for system integration; design distributed system architectures, particularly using APIs; forecast trends and future integration challenges	
	knows and understands…	**Security of digital applications and services**	the basic concepts relating to the security of applications and digital services (e.g., vulnerability, threat, incident, confidentiality, service availability, authorisation); the importance of basic 'digital hygiene' (e.g., strong passwords, caution regarding links and attachments)	basic digital security threats (e.g., phishing, malware, account takeover, data breaches, unauthorised access, DDoS); measures to protect against threats (e.g., MFA, communication encryption, software updates); the threats relating to fraud and disinformation, including the generation of fake content (e.g., deepfakes)	the methods of analysing IT incidents; the mechanisms used to compromise the security of digital applications and services; application security testing (e.g., penetration testing, vulnerability scanners, API security testing, social engineering testing, load testing)	the standards of designing and deploying secure applications and services; the methods of securing application APIs	the strategic management of the security of applications and digital services; the use of AI to detect security incidents and breaches in digital applications and services	new global trends in shaping the security of applications and digital services
	is able to…	**Security of digital applications and services**	take into account the basic principles of 'digital hygiene'	use basic security mechanisms in applications and services (e.g., MFA, password policies, roles and permissions, connection encryption, basic event logging); ensure software is kept up to date; recognise the typical symptoms of IT security incidents; report IT security incidents	analyse application security risks; configure security mechanisms in applications and digital services; participate in the security testing of applications and digital services	design and implement security solutions for applications and services; plan and perform security audits of digital applications and services; recommend and implement corrective measures in digital applications and services in response to errors and vulnerabilities detected during testing	implement security policies for applications and services; monitor compliance with established security policies; make strategic decisions regarding security investments	develop and implement innovative methods in the field of application and digital service security

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
V. Cloud solutions	knows and understands…	**Deployment methods**		the basic types and functioning of cloud computing (public, private, hybrid, social)	the characteristics of public, private, and hybrid clouds in the context of application deployment; environment models (dev, test, pre-prod, prod); how to link the CI/CD pipeline to the deployment strategy (e.g., incremental, parallel) and the ability to roll back a deployment; Infrastructure as Code methodology	the key organisational and technical differences in deployments within a hybrid environment; the role of intermediate environments (test, pre-production); deployment methods in public, private, and hybrid cloud environments; the complex problems at the cloud service user level (e.g., lack of service synchronisation)	the impact of the deployment method on system availability and the risk of failure; available advanced cloud solutions (multi-tier architecture); continuous deployment methodology using CI/CD and IaC tools across multiple environments, including multi-cloud	the latest cloud solutions accelerating the implementation of innovations, reducing service delivery times, and enhancing their security
	is able to…	**Deployment methods**		configure and secure access to simple services (e.g., granting access to files) depending on the type of cloud	update cloud application components; document updates made to cloud application components; use prepared scripts or templates (including IaC tools) to launch simple resources; identify the components required to implement a resilient IT service using the cloud	prepare an implementation procedure for the cloud solution; implement an application or service in a public or private cloud; migrate services to a cloud environment and between cloud environments; diagnose and resolve complex problems encountered by cloud service users; conduct a deployment risk assessment as part of the decision to approve a change to the production environment	implement and manage cloud organisation and infrastructure; select an appropriate implementation strategy (e.g., phased implementation, parallel deployment) suited to the nature of the system and business requirements; coordinate the implementation of changes in a hybrid environment; prepare contingency procedures and rollback scenarios, perform recovery and tests for deployments	develop new cloud solutions based on an organisation's current needs

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
V. Cloud solutions	knows and understands…	**Deployment models**		the technical fundamentals of IaaS, PaaS, SaaS, and FaaS models; the basic mechanisms of virtualisation and resource isolation in the IaaS model	the shared responsibility model in IaaS, PaaS, SaaS, and FaaS; the differences in configuration, maintenance, and updates between PaaS, SaaS, and FaaS	the mechanisms for automatic scaling, load balancing, and high availability in different service models (IaaS, PaaS, FaaS); the methodology for integrating monitoring tools into various cloud models; the methodology for managing secrets; the impact of model selection on the scalability, costs, and resilience of applications and services	the methods of designing PaaS applications (e.g., microservices, event-driven architectures); the methods of utilising FaaS in serverless and event-driven architectures	
	is able to…	**Deployment models**		deploy infrastructure components on an IaaS platform (start a virtual machine); configure SaaS options within an organisation	configure a simple application on the PaaS platform; configure basic components in a cloud architecture; optimise the selection of a solution for a specific IT infrastructure	implement a secret management tool; design application components that enable application scaling; implement a tool for monitoring cloud components	design a complex cloud-native application architecture based primarily on PaaS and FaaS; develop technical standards for the use of PaaS/SaaS/FaaS within an organisation; design solutions utilising FaaS as an element for the orchestration of technical and business processes	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
V. Cloud solutions	knows and understands…	**Cost optimisation and management of the cloud**			the concept of billing for cloud service usage (charges for resource usage)	the methods of calculating the costs of individual components of a cloud project; the principles of selecting resource classes (rightsizing), auto-scaling, and scheduling resource shutdowns to optimise costs; the budgeting and cost alert mechanisms offered by cloud providers	the impact of system architecture (monolithic vs. microservices, serverless vs. IaaS, different storage classes, cache) on the solution's cost profile; the methods of optimising costs in large cloud environments (reservations and savings plans, commitments to use, spot/ preemptible resources, selection of regions and zones based on cost); FinOps principles and showback/chargeback concepts; the methods of estimating costs associated with changes or the implementation of new projects in a cloud environment	
	is able to…	**Cost optimisation and management of the cloud**				identify the main cost categories and analyse cloud bills and cost reports; select the appropriate resource classes for the chosen cloud component (e.g., VM size); configure budgets and cost alerts with a cost summary for the cloud project; prepare a cost optimisation plan for a small/medium-sized cloud environment, taking into account traffic fluctuations and automatic scaling	design and implement a cloud cost optimisation process at the level of individual systems within an organisation; define and enforce tagging standards in cloud solutions; document cost optimisations relating to the cloud infrastructure; prepare a cost estimate for changes or the implementation of a new project in the cloud infrastructure	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
V. Cloud solutions	knows and understands…	**Multi-cloud models**			the concepts of multi-cloud and cross-cloud; the relationship between multi-cloud and cross-cloud; the significance of the hybrid cloud	the methods of integration between clouds; the methods of load balancing between clouds	multi-cloud architectural patterns (e.g., system partitioning across clouds, active-active/active-passive across clouds); the methodologies in the service, network, security, and identity models of major cloud providers and their impact on the design of multi-cloud systems; the methods of creating shared service layers; the methods of creating failure and recovery scenarios in multi-cloud and cross-cloud models	
	is able to…	**Multi-cloud models**			select the appropriate cloud solution depending on requirements	identify system components dependent on the cloud provider (vendor lock-in) and determine ways to minimise them; implement simple multi-/ cross-cloud integration scenarios; maintain consistent multi-/ cross-cloud configurations and standards; analyse problems arising from differences between clouds	design multi-cloud and cross-cloud system architectures; implement an approved multi-cloud model; plan and coordinate the expansion of the system to include another cloud and migration between clouds; design cross-cloud integration mechanisms; design common standards and technical templates for all clouds within an organisation; implement shared service layers across clouds	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
V. Cloud solutions	knows and understands…	**Security in the cloud environment**			the difference between the encryption of data at rest and in transit in a cloud environment; the principles of using encrypted protocols when accessing services in a cloud environment	the mechanisms for encrypting data at rest (e.g., provider certificates, client-managed certificates, KMS) and in transit (e.g., TLS, certificates, endpoint configuration) in a cloud environment; cloud environment requirements for data location, retention, and deletion in the context of regulations and organisational policies	end-to-end encryption strategies in a cloud environment; cloud exit model processes; the methods of creating a compliance report in a cloud environment	
	is able to…	**Security in the cloud environment**			configure encryption in transit in a cloud environment; use cloud services with data-at-rest encryption enabled; document the key security aspects of the solution deployed in a cloud environment	design and configure the encryption of data at rest using certificates managed by providers in a cloud environment; verify the correctness of the encryption configuration and assess the impact on service performance; configure the encryption of data in transit between system components in a cloud environment; configure logging and security event auditing in a cloud environment	design and implement an encryption model for the system in a cloud environment; design and document a cloud exit strategy for the system, including a risk analysis and a business continuity plan for the migrated service; plan and implement security and compliance policies in a cloud environment; analyse security and compliance risks in a cloud environment; prepare and present security and compliance documentation for the system in a cloud environment	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VI. IT support	knows and understands…	**User support and ticket management**	basic IT concepts and terminology; ticket management systems; basic concepts relating to tickets; the rules for prioritising tickets	the standard applications used within an organisation; the typical problems reported by users relating to hardware and software; organisational procedures and policies relating to end-user support; the concepts relating to the escalation of tickets to incidents, problems, and changes; the significance of SLAs and the principles of ticket categorisation; the KPIs required by an organisation	the lifecycle of a ticket, incident, problem, and change; the structure of an organisation's IT environment; the specialist applications used within an organisation; the business systems used within an organisation; the hardware and peripheral environment within an organisation	the procedure for handling incidents, problems, and changes within an organisation; handling tickets in DevOps and DevSecOps teams; service management standards, e.g., ITIL	SLA and OLA service levels; the principles of KPI development; IT service management models	
	is able to…	**User support and ticket management**	record tickets; resolve the simplest problems using pre-defined scripts	classify tickets; prioritise the handling of tickets; provide simple instructions to end users; diagnose and resolve common end-user problems; handle incidents in the ticket system; document the problem-solving process	validate tickets; monitor SLAs and OLAs; escalate a ticket to an incident, problem, or change; resolve problems relating to applications and business systems arising from IT infrastructure or network errors	develop processes relating to incident, problem, and change management; analyse complex problems within an organisation concerning IT service management	manage SLA and OLA service levels; monitor performance and define specific KPIs; develop IT service management models	
	knows and…	**Software installation and configuration**	the basic principles of software installation and configuration	the procedures and policies regarding licensing, installation, permissions, and IT security; the principles of software versioning and compatibility; the software commonly used within an organisation and its purpose	the rules for the installation and configuration of software in a distributed environment (e.g., a network); the techniques for diagnosing installation errors and installation logs	the tools for automating software installation and configuration; the principles of configuring user profiles, default settings, and group policies	the technologies enabling the automation of software installation and updates within an organisation (e.g., WSUS)	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VI. IT support	is able to…	**Software installation and configuration**	analyse basic installation logs; use basic diagnostic tools to resolve software configuration errors; install standard software	configure standard software; resolve software version compatibility problems; verify the availability of software licences within an organisation	install and configure distributed software; test to ensure the software is correct; troubleshoot installation errors based on log analysis and system diagnostics	use available tools to update software within an organisation	automate the process of installing and updating software within an organisation; oversee the correct implementation of software update automation	
	knows and…	**IT hardware and resource management**	the basics of IT hardware; the life cycle of IT equipment within an organisation (purchase, use, decommissioning)	the purpose of IT equipment and rules for its use; the procedures for issuing IT equipment within an organisation	the full life cycle of IT equipment; IT technical documentation and the rules for maintaining it	IT asset management policies and guidelines for creating a configuration management database (CMDB); IT equipment security standards (e.g., hard drive disposal, securing equipment)	an organisation's requirements for IT equipment and resources; market trends in IT hardware solutions	
	is able to…	**IT hardware and resource management**	keep a record of equipment; check that computer hardware, basic network equipment, and peripherals (e.g., routers, access points) are functioning correctly	take stock of IT equipment and resources; apply service and warranty procedures	plan the replacement or repair of IT equipment and resources; prepare the specifications for basic IT equipment and resources	assess the costs associated with the IT equipment and resources in use; plan the budget for IT equipment and resources	plan and optimise IT resources; make purchasing decisions regarding managed IT equipment and resources; optimise costs and expenditures relating to the equipment in use and its performance	
	knows and…	**Remote support for computer and virtual hardware**	common hardware and system problems; remote access policy; the basic components of a computer and operating system	the operation of IT systems within an organisation; the guidelines for working with remote users; typical user problems relating to computer hardware; remote support tools (e.g., RDP, VNC, TeamViewer)	virtual solutions (e.g., VDI, terminal)	the principles of managing hardware resources and virtual solutions (e.g., VDI, terminal); integration with AD and the cloud	the end-user infrastructure maintenance strategy; the trends in desktop solutions	
	is able to…	**Remote support for computer and virtual hardware**	connect remotely to a user's computer and perform a simple diagnosis	remotely diagnose and resolve hardware and software problems	plan security measures for remote support; diagnose the problems of virtual machines; configure applications and services in virtual environments	design and implement security measures for remote support; configure central management tools	design and develop a strategy for managing desktop environments within an organisation	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VI. IT support	knows and…	**Remote support for mobile solutions**	the basic functions of smartphones and tablets; the principles of backing up data and migrating data between devices	Android and iOS systems; common user problems relating to mobile devices; the types and functions of basic mobile applications	MDM tools; mobile device policies relating to security and regulations within an organisation	the principles of mobile device management and integration with AD and the cloud	the management strategy for mobile solutions within an organisation; mobile solution policies, including BYOD	
	is able to…	**Remote support for mobile solutions**	help a user configure the device remotely	back up data and applications; support the remote configuration of accounts and connections; migrate data and applications between a user's devices	remotely manage mobile devices (e.g., reset or lock devices); use an MDM system to manage mobile devices	create and implement MDM policies; automate device update processes	design and oversee mobile support processes; develop strategies and security policies for mobile solutions	
	knows…	**Training and educating users of IT solutions**	the principles of preparing simple instructions for using applications	the basics of using common applications and end devices	teaching and communication methods useful in user training	the principles of designing IT training, including e-learning courses and webinars	the trends and needs in IT education	
	is able to…	**Training and educating users of IT solutions**		explain the basic options and examples of how IT solutions are used; develop easy-to-understand instructions on how to use applications and end-user devices	conduct short IT training sessions; update the IT knowledge base; develop comprehensive IT training courses; adapt the language to the audience's level of knowledge	develop educational materials and training programmes in the field of IT	manage an organisation's IT training strategy; assess the effectiveness of IT training	
	knows and understands…	**Identity and access management**	the principles of user data protection; basic concepts: user account, password, login, permission, role; the standard process for creating an account and assigning basic permissions; the principles of secure password management; the basic risks associated with inappropriate permissions	the guidelines for creating accounts and passwords; user role models and permission schemes within an organisation; the procedures for creating, modifying, and deleting accounts	the model for granting and revoking IT permissions within an organisation; the process of verifying an employee's IT permissions within an organisation	the permission matrices within an organisation; the tools for monitoring access and analysing security logs	access policies; how to define and monitor KPIs for access management	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VI. IT support	is able to…	**Identity and access management**	process access requests according to approved workflows	create and delete user accounts	grant, revoke, and verify permissions in accordance with user roles and the organisational structure	monitor access, analyse security logs, and identify anomalies in access and permissions; verify permission matrices and analyse associated risks	oversee access policies and conduct related audits; define KPIs and quality metrics for access management	
	knows and…	**IT support automation**	the basic concepts relating to automation	basic helpdesk tools; typical automation scripts	the methods of writing simple automation scripts (e.g., PowerShell)	the methods of writing advanced automation scripts	RPA and API technologies	the new models of automation solutions for IT tasks, including those using AI
	is able to…	**IT support automation**	use basic, ready-made scripts	use basic automation scripts	create basic automation scripts; automate repetitive helpdesk tasks	create advanced automation scripts	develop new IT task automation solutions	develop new, complex IT task automation models with the potential to utilise AI
VII. Data management and AI	knows and understands…	**Databases and data platforms**		the examples and applications of basic databases (e.g., Access, MySQL, SQL Server); relational and non-relational databases (e.g., SQL, NoSQL); query languages for basic databases (e.g., SQL); the types and examples of data platforms	a wide range of data structures (e.g., tables, indexes, views, procedures); advanced query syntax in database languages; the use of cloud databases and data platforms; the use and examples of data repositories (e.g., data warehouses, big data)	various methods of data analysis; various principles and methods of data normalisation, consistency, and integration (e.g., ETL, ELT); the principles of data modelling and the use of supporting tools (e.g., LLM modules); the operating principles of complex architectures for data warehouse and big data solutions (e.g., Hadoop)	various principles and methods of database tuning and orchestration; advanced principles and methods of database scalability; the complex principles and methods of optimising database volume, speed, and performance; the security principles of operating and using databases; the use of AI and LLM modules for database management	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	is able to…	**Databases and data platforms**		create basic databases; use basic databases; create standard database queries	create complex databases (including those using AI); use advanced database queries to a great extent; select specialised database management tools and use them; use cloud-based data platforms (e.g., Azure, Google Cloud, AWS); monitor activity and access to the database	design complex databases (e.g., Oracle, Hadoop, MS SQL); use data analysis tools (e.g., BI); use data processing tools (e.g., Apache Spark, Airflow, Kafka, Databricks); use data modelling tools; optimise data flows and queries; design data platforms, lakes, streams, and grids (e.g., lakehouse, data lake, data warehouse), as well as their integration	design optimal and scalable data flows; effectively analyse errors and the performance of databases and data platforms; design and orchestrate; automate the administration of databases and data platforms; use AI and LLM tools to manage and utilise databases and data platforms	
	knows and understands…	**Data processing**	the basic principles of digital health and safety when working with data in registers (key protection, phishing); the role of public and private IP addresses in data identification; the basic digital assets and data units in corporate systems	the differences between test and production environments in terms of data reliability; the types of node failures impacting data availability	the legal basis for processing personal data on the blockchain; data types in smart contracts (e.g., mapping, struct) and their capacity limitations	the techniques for optimising digital data storage to reduce transaction costs; the methods of ensuring data consistency during the blockchain-to-traditional-system integration process; data indexing mechanisms in distributed systems and their impact on dApp performance	the risks associated with illegal practices in critical digital business processes; advanced cryptographic methods of protecting the privacy of digital data; the problems of digital data interoperability between different blockchain standards	current research trends in consensus algorithms and the scalability of digital data processing (e.g., sharding); the impact of quantum technologies on the security and durability of digital data in blockchain ledgers
	is able to…	**Data processing**	produce simple transaction history reports from the user interface (wallet or dashboard); read transaction statuses (confirmed, pending, rejected)	verify transaction statuses across public and private block explorers as part of ticket resolution; monitor the synchronisation of the local node with the network and the continuity of data flow	interpret event logs generated by smart contracts to diagnose logic errors; produce analytical reports on the financial flows of digital assets	develop and implement database schemas and distributed file systems (e.g., IPFS + Blockchain); develop big data solutions for the secure delivery of off-chain data to smart contracts	design comprehensive data flow architectures in hybrid enterprise blockchain systems; conduct security audits of data processing logic in smart contracts; develop policies for key management and access to sensitive data in blockchain systems	develop and implement new standards for protocols governing the exchange and verification of digital data; conduct research and development on new consensus algorithms or structures for digital databases

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	knows and understands…	**Data analytics and reporting**	the principles and methods of producing simple reports; the basic functions and tools for producing simple reports (e.g., Excel spreadsheet)	the types of reports (e.g., tabular, graphical); the methods and tools for creating standard reports (e.g., Canva); reporting tools in a cloud environment (e.g., Google Sheets); common data statistics issues; the basic tasks in data analytics and data science	the technologies and tools for searching, exploring, and verifying data; the technologies and tools for data modelling and forecasting; the technologies and tools for data visualisation (e.g., charts, spatial data); the broad scope of the functions and tools as well as the methods of producing complex reports	the specialised methods of data cleaning, profiling, and preparation (ETL); advanced statistical tests and correlations; the complex methods of building a world of objects for reporting purposes (e.g., Digital Twin); the professional tools and their functions for preparing complex reports and data visualisations (e.g., BI systems such as Power BI and Tableau); the tools for managing and analysing large datasets (e.g., big data)	the specialised processes for creating metrics that ensure data consistency, accuracy, and reliability; predictive modelling methodologies (including those using AI) and trends in their development (e.g., Spark, Orange Data Mining); the specialised platforms for data analysis, data quality management, and reporting; the tools for consolidating large datasets from various fields (e.g., IoT, industry, spatial data)	
	is able to…	**Data analytics and reporting**	produce simple reports (e.g., in an Excel spreadsheet)	use standard functions and templates in tools for producing classic reports (e.g., Canva); produce standard reports, including with the use of cloud-based tools; draw basic conclusions from data for analytic purposes	use technologies and tools for searching, exploring, and verifying data; use technologies and tools for data modelling and forecasting; use technologies and tools for data visualisation (including GIS); create comprehensive reports (including using AI); document data analyses	perform efficient data cleansing and preparation (ETL); draw conclusions from the analysed data (effectively interpret reports); convert data into specific recommendations; produce complex, interactive reports and data visualisations (i.e., dashboards), e.g., using BI systems such as Power BI and Tableau; analyse large datasets and simulate real-world phenomena	identify strategic KPIs and develop metrics; support project management through efficient reporting; automate reporting, including in real-time and with the use of AI; use LLM tools for reporting; use analytics and reports to make strategic business decisions and manage data quality	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	knows and understands…	**Data management strategy**	basic definitions: data, information, personal data, unstructured data, and metadata; the basic principles of file and document organisation	data classifications (e.g., public, confidential) within organisations; the procedures relating to data security and confidentiality in organisations	detailed data governance principles, including roles, processes, and technologies within organisations; data modelling methods and the architecture of various databases and data warehouses; data correction procedures; the principles of creating data quality metrics	data architecture models (e.g., data mesh, data lakehouse); strategic approaches to monetising and valuing data assets; the methods of managing data-related risk; implementation principles in accordance with data policy	advanced theories and models of data management; various ethical and philosophical approaches to data and privacy; the research trends in data policy and their potential strategic implications for organisations	current global strategies, legal regulations, and data policies with the potential for AI application
	is able to…	**Data management strategy**	use basic IT tools to implement data policies in practice	verify and validate data for quality and completeness in accordance with an organisation's policy; prepare a report or data summary in accordance with internal reporting standards	help develop data quality metrics; apply corrective procedures to restore data integrity; analyse data models	design and implement a comprehensive data governance architecture within a large organisation; develop a data management strategy for an organisation; make decisions regarding the use of data in unpredictable regulatory contexts	define a long-term data strategy for the entire organisation; conduct audits and provide consultancy on regulatory compliance and the strategic use of data; propose the development of new standards, procedures, and data management models within an organisation; audit and assess the compliance of data collection and processing procedures with an organisation's internal policies	implement and update a long-term data strategy as required; provide effective strategic advice on regulatory compliance and data usage policies, including in relationship to AI

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	knows and understands…	**Data privacy**		the types of permissions for the data being processed (access, creation, modification, deletion); the types of data collected, the purpose of collection, and the retention period; the principles and criteria for classifying sensitive data (particularly identity data) subject to legal protection; the procedures for responding to data privacy breaches; the methods of analysing and visualising protected data; the risks arising from the misuse of AI in relation to data privacy	data privacy regulations (e.g., GDPR, laws and regulations, the Labour Code, data processing agreements, confidentiality clauses); standard methods and tools for managing data access and destruction; standard methods and tools for data privacy protection (including identity, sensitive data, and online activity); standard methods and tools for managing the lifecycle of personal data; the principles of data management documentation	advanced methods and tools for the encryption, access control, anonymisation, and pseudonymisation of data; the principles of 'privacy by design' and 'privacy by default'; the principles of risk analysis in accordance with the GDPR; the principles of securing personal data	the trends in AI development for data privacy protection; the latest methods and tools for data protection using AI	
	is able to…	**Data privacy**		identify basic and particularly sensitive data subject to legal protection; identify users and their access rights to protected data; respond to data privacy breaches in accordance with the relevant procedures	apply data privacy regulations; use tools for managing data access and destruction; use data privacy protection tools; manage data in accordance with its intended purpose and lifecycle; document how data and its access are managed	use complex tools for the encryption, access control, anonymisation, and pseudonymisation of data; ensure the principles of 'privacy by design' and 'privacy by default'; analyse risks in accordance with the GDPR; apply enhanced data access security measures; protect data against AI malfunctions	apply the latest data protection methods and privacy tools using AI; use AI solutions to enhance data security	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	knows and understands…	**Artificial intelligence**	the basic concepts relating to artificial intelligence; the basic applications of AI in everyday life and work; the basic principles of distinguishing tasks performed by artificial intelligence; the basic the principles of security and data protection when using AI tools	the types of machine learning (supervised, unsupervised, reinforcement); the relationship between traditional software and machine learning systems; the concept of AI autonomy and AI agents	the full lifecycle of an ML project; the basic and most popular ML algorithms; the problems relating to bias and AI hallucinations	model scaling, distributed computing, and predictive models; the European regulations (AI Act), risk categories, and safety issues relating to the use of AI/ML; how LLM and DL (deep learning) models work; the methods of configuring and fine-tuning AI models; the RAG technique for expanding LLM models; the principles of human oversight of AI systems in accordance with the AI Act; AI Act requirements on the procedures for assessing the compliance of high-risk AI systems and their technical documentation; AI Act requirements for general-purpose AI (GPAI) models, including provider obligations and systemic risk criteria	the latest scientific research in the field of AI and ML/LLM; the latest trends in AI; explainable AI (XAI) methods and model interpretability; advanced research frameworks and areas of development for new AI/ML algorithms; advanced AI, LLM, and deep learning (DL) architectures, e.g., multi-agent systems; the principles of monitoring AI systems after they have been placed on the market and the obligation to report serious incidents; the role and operating principles of AI regulatory sandboxes in the innovation implementation process	current and dominant global AI strategies; the latest global trends in data science/AI

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	is able to…	**Artificial intelligence**	use ready-made AI-based tools and applications; apply the principles of recognising AI-generated content; apply basic security and data protection principles when using AI tools	select simple datasets for use in AI/ML tools; deploy ready-made ML models in no-code/low-code tools; interpret basic results of AI/ML model evaluations; apply simple AI tools to various tasks; deploy an AI agent	pre-process raw input data into a more effective dataset and select a model; clean and curate datasets for use in AI/ML tools; independently build and train an ML model using publicly available libraries; implement a simple AI/ML model; recognise AI hallucinations and bias; use large language model (LLM) APIs for simple automation tasks; apply techniques such as prompt engineering to achieve reproducible results	design and implement comprehensive AI/ML/RAG solutions; identify and assess bias, drift, and hallucinations in AI/ML models; produce technical documentation for developed AI/ML/RAG solutions; oversee AI systems in accordance with the AI Act; implement and apply procedures for assessing the compliance of AI systems and technical documentation in accordance with the AI Act; apply the requirements of the AI Act to general-purpose AI (GPAI) models	independently conduct experiments and research in the field of AI/ML (including the optimisation of computational costs); design new LLM model architectures or significantly improve existing ones, e.g., multi-agent systems; manage the full optimisation and automation pipeline of MLOps processes; minimise bias, drift, and hallucinations in AI/ML models and ensure compliance with ethical and legal regulations; apply AI explainability (XAI) methods to ensure the transparency of AI systems' operations in accordance with the requirements of the AI Act	identify current trends and directions in AI development; develop, select, and combine modern AI strategies required by business; develop innovative AI strategies for organisations in compliance with the AI Act and other regulations, e.g., AI TRiSM
	knows and understands…	**AI ethics**	the concepts of AI hallucinations and deepfakes; the principles of AI use	the risk categories set forth in the AI Act (unacceptable, high, limited, minimal); the fundamental legal and ethical obligations of IT system providers and users in the context of AI; the risks and liabilities associated with the use of AI agents	the specific requirements of the AI Act for high-risk systems; the methods of detecting and mitigating AI hallucinations; the techniques for making and detecting deepfakes; the criminal and civil liability for the harmful use of generative AI; the mechanisms underlying hallucinations in LLM and generative models	advanced methods of attack and defence in the field of deepfakes and multimedia manipulation; the procedures for assessing compliance with the AI Act in relation to policies for detecting and responding to deepfakes, bias, and hallucinations; the global and European standards for detecting synthetic content; the ethical standards for the deployment of AI (in particular AI agents)	the latest research on the causes and limitations of hallucinations and bias in AI models; advanced methods of attacking AI models and their ethical and legal implications	the latest global scientific publications on the ethical alignment and safety of large-scale AI; the potential long-term risks associated with uncontrolled hallucinations, bias, and disinformation on a global scale

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	is able to…	**AI ethics**	recognise obvious hallucinations and deepfakes in the media; apply the principles of not disseminating suspicious AI-generated content; verify facts provided by AI; report inappropriate AI behaviour (e.g., suspicious content) to the relevant authorities	assess whether a given use of AI falls into the high-risk category; label AI-generated content; verify that the use of tools complies with the AI Act and the GDPR	implement mechanisms to reduce hallucinations in production environments; use tools to detect deepfakes and synthetic media; apply legal requirements and rules for the labelling and registration of high-risk AI systems; detect and counteract hallucinations in everyday work with LLMs	design AI-powered systems (including AI agents) in accordance with ethical principles and social context; implement an AI risk management system; conduct an audit of AI systems for legal and ethical compliance; respond effectively to deepfakes, bias, and hallucinations	test the methods of detecting and preventing hallucinations, bias, and deepfakes; design certification systems and safety standards for generative AI; interpret and verify LLMs and multimodal models in relation to the ethical aspects of AI; develop policies for detecting and responding to deepfakes and hallucinations	advise governments and international institutions on the development and updating of regulatory policies concerning AI risks; develop new methods of detecting and preventing hallucinations, bias, and deepfakes
	knows and understands…	**Open data**	the basic definition of open data and the principles governing its sharing; the concept and examples of metadata; the main public open data portals; licences enabling the reuse of data; the common tools for processing datasets	the key principles and methods of making open data available; the differences between popular data formats; the basic categories of exclusions and restrictions on data sharing	common data structures and formats, including spatial data; key platforms for sharing public data (e.g., CKAN, DKAN, GeoServer); the platforms collaborating on making public and commercial data open (e.g., Socrata, OpenDataSoft); the detailed legal and technical requirements for the publication of open data; the methods of assessing the quality and maturity of the datasets made available; advanced metadata standards	the methods and tools for creating and managing complex open data systems; the role of APIs in accessing data and building applications that operate on real-time data; the policies for sharing data from IoT devices; the technical solutions for automatic and scalable data sharing; the importance of cleaning open data for projects and innovations (e.g., OpenRefine)	the research methodologies for evaluating open data; the trends and technologies in the field of interoperability and open data exchange; the importance of building an ecosystem for the joint opening of public and commercial data	the challenges facing future legal and technical regulations on open data; the ethical principles of open data processing (Data Ethics Canvas); the latest methodologies and trends in the ongoing promotion of directly using open data (e.g., data storytelling) with the potential for AI application

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VII. Data management and AI	is able to…	**Open data**	find and download standard data tables from an official open data portal; use basic tools to open and visualise datasets; recognise whether a given dataset has metadata and be able to read it	search for and combine data from various open sources; use tools to query public datasets; correctly cite licences and attribute them to the open data being shared	develop an internal data publication procedure; de-identify and anonymise data; manage and maintain datasets in an open data platform; ensure that open data is up to date and that metadata is of high quality; assess potential technical, legal, and ethical risks associated with the publication of open data	develop a procedure for publishing open data for an organisation or sector; implement advanced IT mechanisms for the automatic and scalable sharing of data	develop highly complex models for sharing open data; design complex IT mechanisms for the automatic and scalable sharing of data; deploy shared platforms for public and commercial open data	conduct research and develop innovative models for sharing highly complex open data; develop new standards and procedures at the national or international level on making data open, including commercial data; collaborate on building innovation within the ongoing process of making data open and build a community around this
VIII. IT solutions architecture	knows and understands…	**Vision of IT architecture**		the fundamentals of IT architecture and IT analysis	the role of IT solution architecture depending on the organisation; the fundamentals of enterprise architecture and its components (TOGAF, Open Agile Architecture); the relationship between IT architecture and IT solution analysis	the methods and tools for designing IT architecture (based on TOGAF); the principles of developing a target vision of IT architecture (TO-BE); the relationships and principles of creating IT architecture layers (components: business, data, application, technology, and critical systems architecture)	the significance of the AS-IS and TO-BE state descriptions for an organisation's architectural model; the importance and significance of architectural principles for an organisation in relation to its strategy; the importance of the vision for implementing projects in accordance with the technological standards and system interoperability contained in the vision	the importance of formulating recommendations for innovative changes to an organisation's development strategy and IT architecture vision; the impact of the latest technologies on an organisation's development through the use of, for example, cloud solutions and AI
	is able to…	**Vision of IT architecture**			assess the current AS-IS state of the IT architecture; identify the relationships between the main components in the existing IT environment	analyse and evaluate the dependencies between the IT environment components in the TO-BE architecture; create IT architecture diagrams (e.g., C4, ArchiMate); select vision components for project implementation in accordance with technological standards and system interoperability as set forth in the vision	update the status of the AS-IS and TO-BE architecture; help develop and define architectural principles for IT; provide strategic oversight of project delivery in line with the IT architecture vision; limit Shadow IT in accordance with the principles of the vision; manage the layers within the IT architecture component repository (legal, organisational, semantic, technical)	identify and develop innovative technologies that influence an organisation's development, utilising, for example, cloud solutions and AI; develop an innovative approach to complex problems and the interdependencies of components within modern IT architecture

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VIII. IT solutions architecture	knows and understands…	**Technology stack and technology selection**				the typical components of a technology stack (the difference between frameworks, tools, and the stack); the types of technology stacks designed for typical applications; the importance of open-source-based technology stacks for architectural independence	the importance of choosing a technology stack in native cloud technologies and within one's own IT environment, and its impact on IT architecture; the key requirements and components (including AI) of the technology stack for cloud solutions and their security; the impact of the technology stack and its standardisation on performance, scalability, and security	the trends in modern technology stacks for innovative organisational transformation; the need to utilise new elements of the technology stack to build coherent ecosystems with AI tools
	is able to…	**Technology stack and technology selection**				identify the components of a technology stack depending on its intended use; select a technology stack based on key considerations (e.g., design, scalability, budget, team expertise, security); apply selected components from the technology stack for project implementation, including those utilising open source solutions	compile and implement a technology stack for cloud and hybrid environments within an IT architecture; select and apply technological components to build and develop one's own technology stack; conduct the process of standardising the use of the technology stack and develop standards and guidelines for the use of the implemented technologies; conduct a risk analysis of the selected technology stack	modify an innovative IT architecture technology stack and migrate the developed solutions to existing technology; use AI to perform innovative analyses as well as environmental and functional simulations of the technology stack

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VIII. IT solutions architecture	knows and understands…	**Architectural and reference patterns**			the fundamentals of component-based and service-oriented architecture, as well as architectural styles (e.g., SOA, layered, microservices, event-driven EDA)	the significance of architectural and integration patterns (e.g., REST API, SOAP, Kafka); the significance of the relationship between patterns and architectural vision principles (e.g., microservices vs. monoliths) and their interdependencies (e.g., in terms of scalability, reliability, project size); the principles of selecting architectural patterns that implement these principles (e.g., time-to-market, high availability, and vendor independence); the importance of pattern selection for a hybrid cloud computing environment (combining on-premises data centres, private clouds, and public clouds) in terms of business continuity	the methods and principles of creating and maintaining reference architectures; the methods and principles of maintaining and updating IT architecture resilience models; the significance and interdependencies of using patterns based on open-source or commercial platforms; the importance of open-source architectural patterns for the implementation of cloud-agnostic or cloud-native solutions; the methods of defining integration standards	the strategy and innovative directions for developing architectural patterns, particularly through the use of AI, in the creation of innovative digital solutions as part of building a competitive advantage

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VIII. IT solutions architecture	is able to…	**Architectural and reference patterns**					select a design pattern and justify its selection in a given IT project; create reference architectures for the patterns used, as well as catalogues of architectural standards, guidelines, and recommendations; document the use of design patterns and their compliance with principles; apply and utilise open source in reference architectures with a view to optimising costs and reducing vendor lock-in; apply the principles of selecting cloud solutions (cloud-agnostic vs. cloud-native) depending on needs and principles; identify risks and develop an exit plan for key or high-risk IT architecture solutions	modernise legacy systems and services by identifying and resolving architectural technical debt; update, select, and create new architectural patterns, taking into account cloud solutions and AI; utilise new AI-based patterns (e.g., RAG) (combining LLM models with proprietary data resources)
	knows and understands…	**Oversight and development**				the importance of IT architecture in supporting business strategy and ensuring an organisation's development; the principles of selecting IT architecture to suit an organisation's resources (e.g., avoiding vendor lock-in, eliminating the duplication of systems and repetitive technologies, better utilisation of resources)	technology leadership and the role of IT architecture in an organisation's long-term business strategy; architectural frameworks and standards for managing IT architecture and documenting the vision; the importance of overseeing the IT architecture vision in terms of technical debt, security, and compliance; the principles of creating an IT architecture to manage the full spectrum of business capabilities (IT, OT, IoT); the API First approach as not only a technological but also a business strategy	development trends, including the use of AI to create innovative architecture within the Green IT model; the trends in developing new platforms that automate and support IT architecture

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
VIII. IT solutions architecture	is able to…	**Oversight and development**				independently build a system prototype confirming that the IT architecture vision is feasible; verify architectural choices in terms of their alignment with the vision (e.g., using open-source solutions); draw on extensive knowledge of security, IT infrastructure, software, data, and cloud computing to develop the IT architecture	implement and adapt IT architecture in an evolutionary manner, ensuring an organisation's security and sustainable development; conduct IT architecture reviews and document architectural decisions; update reference architectures within an organisation and oversee the implementation of principles (including the reusability of components, services, and code); implement a service-oriented architecture using API management as a principle	identify and test new technologies for implementing and updating the IT architecture; use AI in the design, modelling, and oversight of innovative IT architecture; use IT architecture to create an innovative technological advantage within the digital ecosystem
IX. IT management	knows and understands…	**IT strategy**				business objectives and their links to IT plans; the IT infrastructure and IT systems architecture	the methods of developing an organisation's IT strategy; IT project portfolio management; the trends in IT technology development; the impact of AI on IT and business	current and global technological trends in IT; current sectoral policies and the impact of IT on the economy
	is able to…	**IT strategy**				analyse an organisation's needs and propose appropriate IT solutions; analyse existing IT resources and utilise them to achieve business objectives	develop and implement an IT strategy aligned with an organisation's strategy; propose and integrate IT technologies with business and environmental processes; build IT structures in line with an organisation's needs	shape a long-term and innovative vision for the development of IT within an organisation; influence the current strategy of the whole institution and sectoral policies

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IX. IT management	knows and…	**Technology leadership and digital business transformation**				the principles of managing an IT team; the basics of digital transformation	the methods of change management in IT; the methods of managing IT innovation and their impact on an organisation	innovative models of digital leadership tailored to market requirements; current methods of strategic communication and the role of an organisation's ambassador; digital platforms and ecosystems
	is able to…	**Technology leadership and digital business transformation**				lead an IT team; motivate IT teams and support the implementation of new technologies	manage digital transformation; manage technology debt; lead IT innovation programmes; build interdisciplinary teams to support digital transformation; lead an organisation through a digital transformation	set new directions for digital development; develop the organisation within the digital ecosystem; actively participate in IT conferences on a regular basis
	knows and…	**IT budgeting and finance**				the basics of budget planning and cost control relating to IT expenditures	the methods of analysing ROI, TCO, and financing IT projects; IT financing models, building consortia and clusters; the IT budget within an organisation; IT cost optimisation	strategic IT budget management; the methods of raising funds for IT innovations; the impact of IT investment on the entire organisation and the economy
	is able to…	**IT budgeting and finance**				plan and monitor the budget of an IT team/department/ project	manage an organisation's IT budget; optimise IT and business operating costs within an organisation; influence stakeholders regarding the IT budget	negotiate day-to-day funding and evaluate strategic IT investments; raise external funds for strategic and innovative initiatives in the IT sector
	knows and…	**IT licence management**			open source licensing principles; commercial licensing principles; the licence lifecycle management process; software inventory tools	software licensing models; licence management systems (e.g., SAM, SLM)	the licence management policy within an organisation	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IX. IT management	is able to…	**IT licence management**			identify types of licences; use different licences; establish and update licence registers within an organisation; conduct a market analysis of licence providers; verify that licences comply with contracts and regulations; conduct a software inventory	identify redundant and unused licences within an organisation; conduct software licence audits	plan licence purchases; optimise the costs of selecting and purchasing licences; negotiate licence terms with suppliers; manage licences within an organisation	
	knows and…	**IT service management**				ITIL/COBIT methodologies; the methods of monitoring OLAs and SLAs; the methods of ensuring the continuity of IT services; cybersecurity risks associated with IT services and ways to counteract them	the methods and tools for designing an IT service catalogue; IT service management systems	IT service policy at the digital ecosystem level; current approaches to integrating IT and business with the digital ecosystem; how to maintain stable relationships with key suppliers and individuals within the digital ecosystem
	is able to…	**IT service management**				use ITIL/COBIT methodologies; monitor OLAs and SLAs; ensure the continuity of IT services; identify cybersecurity risks associated with IT services and their impact on an organisation	design an IT service catalogue; apply ITIL/COBIT methodologies in accordance with an organisation's needs; develop IT service management methodologies within an organisation; implement IT service management processes; ensure the quality and availability of IT services	develop IT service policies within the digital ecosystem; integrate IT and business with the digital ecosystem; maintain relationships with key suppliers and key individuals within the digital ecosystem
	knows and…	**IT project management**				IT project management methodologies (e.g., Agile, Scrum, PRINCE2)	IT project portfolio management methods; hybrid methodologies in IT project management (e.g., Water-Scrum-Fall, Agile-Waterfall Hybrid, PRINCE2 Agile); the risk management methods for IT projects	the organisation's project culture and its impact on IT strategy

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IX. IT management	is able to…	**IT project management**				manage IT projects in accordance with the methodologies; monitor the schedule, budget, and scope of IT projects; apply design thinking in IT project management	manage the IT project portfolio; manage IT project risks; implement hybrid methods in IT project management	decide on day-to-day and strategic IT initiatives; present new IT projects to an organisation's management and external stakeholders
	knows and understands…	**Human resources and IT skills management**				the responsibilities and duties of individual IT team members; the methods of monitoring task completion by IT team members (e.g., Kanban, sprints, retrospectives); the methods of recruiting staff for IT teams; the methods of assessing the competences of IT staff	HR policy in IT; training policy for IT department staff; the methods of building IT structures within an organisation; incentive schemes and models for developing the skills of IT staff	the strategy for developing IT talent within an organisation; the ways of collaborating with universities and educational institutions to recruit IT talent; the ways of influencing the IT labour market
	is able to…	**Human resources and IT skills management**				organise the work of an IT team; assign IT tasks and assess their completion; recruit staff for an IT team; assess the competences of IT staff; monitor the completion of tasks by IT team members	supervise the work of individual IT departments within an organisation; set targets for individual IT departments and assess their achievement; plan the development of IT staff competences; develop career paths for IT staff; develop the skills of staff in individual IT departments; implement incentive schemes within IT; initiate the organisation of IT work placements and internships	create and update an organisation's IT talent development strategy; collaborate with universities and educational institutions to continuously recruit IT talent; keep abreast of developments in the IT job market

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IX. IT management	knows and...	**IT risk and compliance management**				the operational risks relating to IT services and IT infrastructure; IT compliance procedures (e.g., GDPR, ISO standards)	the methods of strategic IT risk management; IT control and audit systems; national and EU regulations relating to IT; the principles of developing IT compliance procedures	IT security and compliance policy within an organisation; the methods of cooperation with institutions and regulators influencing IT compliance
	is able to...	**IT risk and compliance management**				identify operational risks relating to IT services and IT infrastructure; apply IT compliance procedures (e.g., GDPR, ISO standards)	manage strategic IT risk; implement IT control and audit methods; apply national and EU regulations in the field of IT; develop IT compliance procedures	develop and update an organisation's IT security and compliance policy; cooperate on an ongoing basis with regulators and international institutions regarding IT compliance
	knows...	**IT business continuity management**				IT contingency and disaster recovery plans	high-availability solutions and IT business continuity programmes	an organisation's IT resilience strategy; the principles of integrating an organisation's plans with national IT security policy
	is able to...	**IT business continuity management**				develop and test IT contingency plans; coordinate the recovery of IT resources	manage business continuity programmes and implement IT recovery	develop and continuously update an organisation's IT resilience strategy; regularly integrate an organisation's plans with national IT security policy
	knows and understands...	**IT quality management**				IT service quality control tools (e.g., process diagrams, process checklists, Ishikawa diagrams); IT service quality metrics; software quality control tools (e.g., functional and non-functional tests, static and dynamic code analysis, test automation using Selenium, JUnit); the tools for performance testing (e.g., JMeter)	ISO/ITIL standards and IT service quality audit methods	the culture of IT service quality and its impact on the IT industry

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
IX. IT…	is able to…	**IT quality management**				apply quality control tools for IT services and software and monitor their performance indicators	design IT service quality management systems; conduct IT service audits	implement and foster a culture of IT service quality; develop current norms and standards within IT standardisation bodies
X. Groundbreaking IT technologies	knows and under-	**Immersive technologies**		the principles of using immersive technologies (e.g., VR, AR, MR); the differences between immersive technologies; how immersive technologies work	IT applications and the tools necessary for using the relevant immersive technologies; the principles of the operation and use of various types of simulators (e.g., medical, aviation)	the principles of configuring the hardware and software necessary for the use of immersive technologies	the trends in immersive technologies; complex immersive technology solutions; the new areas for the application of immersive technologies	
	is able to…	**Immersive technologies**		identify the type of immersive technology	choose the type of immersive technology appropriate for the task at hand; develop a concept for an immersive IT solution; use a simulator for training and in the workplace	implement and launch immersive technology solutions; conduct performance tests of immersive technology	create functional applications compatible with immersive technology; refine the methods of immersive technologies; initiate the work of an interdisciplinary team to develop immersive technologies	
	knows and understands…	**Quantum computers**			the basic concepts of quantum computing; the main differences between classic and quantum computers	the basic practical applications of real quantum computers and simulators; basic quantum algorithms and their potential applications; the theoretical foundations of how quantum computers work	advanced principles of quantum information theory, including quantum error correction mechanisms and quantum communication protocols; a wide range of advanced algorithms and their limitations; the fundamentals of various hardware architectures	the latest scientific advances and theories at the interface between quantum computing, physics, and engineering; current theoretical and practical challenges relating to potential applications of quantum computing

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
X. Groundbreaking IT technologies	is able to…	**Quantum computers**			identify the components of a simple quantum circuit in a ready-made graphical user interface (GUI) or diagram; run a quantum program in accordance with the instructions and read its simple result	use the graphical interface for constructing quantum algorithms; use quantum algorithm software tools; estimate the computational complexity of quantum algorithms	analyse and practically synthesise knowledge at the interface between quantum computing, physics, and engineering; design and modify quantum algorithms; use quantum computer emulators	conduct original scientific research and develop new quantum theories or protocols; define, propose, and implement new, strategic research and development (R&D) projects in quantum computing; disseminate knowledge in the field of quantum computing
	knows and understands…	**Autonomous solutions**		the basic types of autonomous and humanoid systems and their main components (e.g., sensors, controllers, actuators); the general principles of the operation of simple localisation and navigation methods under routine operating conditions; the basics of integrating autonomous systems with IT/OT infrastructure, taking into account security principles	the architecture of typical autonomous systems; the fundamentals of sensor data processing for autonomous solutions; typical communication solutions in autonomous systems and the principles of applying operational requirements and procedures	the operation of key components of autonomous systems and their interdependencies within the solution; the principles of selecting and configuring autonomous solutions to meet business or technological process requirements; the stages of the lifecycle of autonomous solutions and the principles of designing in-system safety measures	the principles of designing target architectures for autonomous and humanoid systems at the level of an organisation or a digital ecosystem; organisational and process models for the operation of autonomous system fleets; the legal, ethical, and social considerations relating to the use of autonomous solutions; the principles of risk identification, assessment, and management at the organisational level in relation to autonomous solutions	in-depth, the principles of perception, localisation, and control in autonomous systems; current trends in scientific research in the field of autonomous and humanoid systems; advanced methods of analysing the safety, reliability, and resilience of autonomous systems

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
X. Groundbreaking IT technologies	is able to…	**Autonomous solutions**		prepare autonomous devices for operation, including the use of localisation and navigation methods; perform basic maintenance and calibration tasks on sensors and actuators; monitor the basic operating parameters of an autonomous device; respond to typical messages and alarms in accordance with procedures	control a selected component of an autonomous device; configure and optimise the operation of off-the-shelf autonomous systems for specific tasks; analyse logs and telemetry data to identify problems; plan and conduct acceptance testing of autonomous devices	select and combine elements of autonomous systems into coherent solutions for a specific process, using available components and IT/OT infrastructure; plan and implement complex deployment, testing, and validation scenarios for autonomous systems (e.g., regression, scenario-based, and security tests); modify the configuration and operating parameters of advanced autonomous systems and advise on the selection and adaptation of solutions from various suppliers	design target architectures for autonomous solutions for organisations; design and refine operational processes for autonomous fleets; coordinate interdisciplinary design and investment teams in the field of autonomous solutions	design and develop new algorithms and innovative models for autonomous and humanoid systems; plan and conduct complex research and development work in the field of autonomous and humanoid systems; help shape technical standards, regulations, and sectoral guidelines in the field of autonomous and humanoid systems; build expert communities and foster collaboration between academia, business, and government in the field of autonomous and humanoid systems
	knows and understands…	**Bio-digital technologies**			bioinformatics issues; the principles of biosensor operation; how wearable technology works; the types of biosensors; the types of wearable technology	the types and examples of bio-digital technologies; the methods of digital modelling and simulation of biological processes	the principles behind brain–computer interfaces (BCIs); the methods of designing brain–computer control systems (e.g., ML and AI tools); the application of ML and AI to analyse biological material; the prospects for the use of biocomputers; the methods and tools for computer navigation in implantology; BCI, biocomputers	the latest trends in research funding for bioinformatics and bio-digital technologies; current IT methods for supporting the diagnosis and treatment of diseases, and the development of new drugs

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
X. Groundbreaking IT technologies	is able to…	**Bio-digital technologies**			read and decode signals from biosensors; use biosensors; use wearable technologies	develop software for bio-digital technologies	design interfaces and brain–computer communication and control systems; apply ML and AI to the analysis of biological material; develop algorithms and design methods and tools for navigation in bio-digital technologies	conduct innovative experiments in the field of bioinformatics and bio-digital technologies; develop new IT methods to support the diagnosis and treatment of diseases and the development of new drugs; design new applications for biocomputers; co-develop innovative components for biocomputers
XI. Green IT	knows and understands…	**Sustainable hardware infrastructure**	**(GC) the general principles of the energy-efficient use of IT equipment**	**(GC) the basic components of IT hardware infrastructure and their impact on energy consumption;** **(GC) the basic principles of handling end-of-life IT equipment and the importance of internal procedures**	**(GC) the electricity requirements of IT infrastructure components;** **(GC) the basics of monitoring the electricity consumption of IT infrastructure components;** **(GC) the principles of sustainability in the life cycle of IT equipment**	**(GC) the relationship between IT infrastructure architecture, energy consumption, and the carbon footprint;** **(GC) the methods and tools for measuring the consumption of IT infrastructure resources and for reporting on its environmental impact;** **(GC) the principles of planning the modernisation and replacement of obsolete IT infrastructure, including the potential use of AI**	**(GC) the principles of designing target IT infrastructure architectures, taking into account green IT at the organisational level (data centre, cloud, network, working environment);** **(GC) the frameworks and standards for managing sustainable IT infrastructure and their links to ESG reporting requirements;** **(GC) the eco-friendly approach to modernising infrastructure environments, with the potential for AI application**	**(GC) advanced technologies and the latest research trends in the field of sustainable IT infrastructure, with the potential for AI application;** **(GC) the development and design of sustainable models for global IT infrastructure architectures within the digital ecosystem**

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
XI. Green IT	is able to…	Sustainable hardware infrastructure	(GC) apply energy-saving settings for simple IT devices	(GC) operate IT hardware in accordance with energy-saving principles; (GC) dispose of end-of-life IT equipment at appropriate collection points	(GC) analyse basic data on the electricity consumption of IT infrastructure components; (GC) apply standard energy-saving solutions in IT hardware infrastructure; (GC) identify the most energy-intensive components of the IT infrastructure for replacement or optimisation	(GC) design and implement eco-friendly improvements in IT hardware infrastructure (e.g., cloud computing, server virtualisation, power and cooling optimisation); (GC) select and implement energy monitoring tools to optimise IT infrastructure; (GC) plan and coordinate the modernisation of energy-inefficient IT infrastructure, with the potential to utilise AI	(GC) design sustainable IT architecture at an organisational level; (GC) define and oversee policies, processes and KPIs relating to sustainable development in the area of IT infrastructure; (GC) coordinate IT infrastructure modernisation programmes with the potential to utilise AI	(GC) design new models, methods, and tools for sustainable IT infrastructure with the potential to utilise AI; (GC) conduct innovative research and development projects on sustainability in IT infrastructure and implement their results in the form of reference solutions; (GC) co-develop standards, guidelines, and policies for green IT
	knows and understands…	Green IT software	(GC) the basic principles of effectively using applications in the context of sustainable development	(GC) the basic impact of software on resource and electricity consumption; (GC) the basics of the software life cycle and its significance for the sustainability of the IT environment	(GC) the basic principles of programming focused on the environmentally friendly use of resources; (GC) practices that limit software's use of resources; (GC) the environmental impact of obsolete software	(GC) the impact of software architecture on resource consumption and energy efficiency; (GC) the methods of measuring and monitoring software resource consumption; (GC) the principles of re-engineering obsolete IT systems, including the potential use of AI, to reduce adverse environmental impact	(GC) the principles of designing target application architectures, taking into account organisational-level sustainable development goals; (GC) advanced approaches to the modernisation and re-engineering of legacy IT systems to protect the environment, and the role of AI in this process; (GC) the economic and environmental aspects of decisions regarding software architecture and development	(GC) the latest approaches, including AI, in the automated analysis, generation, and modernisation of software in the context of sustainable development; (GC) the impact of current regulations, standards, and market requirements on the development of methods and tools for sustainable software development

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
XI. Green IT	is able to…	Green IT software		(GC) use and configure applications in a way that minimises resource consumption; (GC) apply the principles of sustainable development when using software (e.g., optimal use of cloud services); (GC) identify software's basic performance problems and excessive resource consumption	(GC) analyse simple applications or services in terms of resource consumption that impacts the environment; (GC) apply basic green coding practices in the software being developed; (GC) participate in optimisation tasks, proposing changes to the configuration or functionality to reduce resource consumption	(GC) design and implement software architecture components, taking into account sustainability requirements; (GC) configure and use application monitoring tools to identify software requiring optimisation in terms of sustainable development; (GC) participate in the re-engineering of obsolete IT systems, with the potential to utilise AI, in order to reduce their adverse environmental impact	(GC) design software architectures and applications with a view to resource efficiency and sustainable development objectives; (GC) lead software optimisation and modernisation programmes, including initiatives to re-engineer obsolete IT systems with the potential to utilise AI, in order to reduce adverse impact on the environment; (GC) define metrics and management mechanisms and integrate them into software development and maintenance processes to support sustainable development	(GC) design and conduct innovative research and development programmes to produce sustainable software and ensure eco-friendly software operation; (GC) co-create new models, standards, guidelines, and policies on sustainable software, and actively build expert communities and cooperation networks in the field of digital ecosystems

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
XII. Communication, collaboration, leadership	is ready to…	**Communication and collaboration within the IT team**	apply established communication rules within the IT team; cooperate with other members of the IT team under the supervision of a more experienced colleague; inform relevant IT personnel or teams of any encountered technical problems	clearly communicate progress to IT team members and clarify the scope of their tasks; provide the team with reliable and timely updates on the status of IT services; use basic English-language technical documentation and IT tools	assist other members of the IT team in performing tasks and resolving technical problems; communicate in English on technical issues within an international IT team	engage IT team members in the tasks assigned to them; contribute to the development of effective communication within IT teams; **(GC) collaborate with users and teams on the implementation of green IT principles**	implement standards for communication and IT teamwork within an organisation; address conflicts, manage escalations and differing expectations within IT teams and in relations with users and clients; represent and promote the IT team within an organisation; **(GC) promote eco-friendly IT practices within an organisation**	shape innovative standards for communication and cross-team collaboration within the digital ecosystem
		IT communication with users and customers	maintain a polite and professional manner when engaging with the users and customers of IT systems and services (first point of contact); forward tickets/information about problems to the relevant IT personnel or teams	provide feedback on the status of tickets, changes, or IT solutions; communicate autonomously with users and customers to explain basic IT solutions	describe users' and customers' requirements for IT systems and services in a clear and understandable manner to technical teams; act as an intermediary in communication between users and IT teams; communicate with the suppliers and subcontractors of IT solutions	build and maintain long-term relationships with key IT solution users and customers; verify the functional requirements of IT solutions; deliver presentations and conduct technical negotiations with clients/ partners in English	represent the IT department when engaging with external parties; implement communication strategies with users and clients in the field of IT solutions; take responsibility for communication with users and clients in crisis situations concerning IT systems and services	develop new strategies for communicating with external parties in the field of IT solutions; conduct ongoing collaboration with shareholders and key business units to plan and update IT architecture; represent the organisation in the field of digital ecosystems
		Sharing IT knowledge, mentoring, and team leadership		actively participate in regular IT team knowledge-sharing meetings; share knowledge regarding the IT solutions used; document one's work in accordance with the IT department's procedures so that it can be utilised by other team members	initiate meetings aimed at knowledge sharing within the IT team; encourage IT team colleagues to share their knowledge and experience	conduct IT technical training sessions and workshops; precisely delegate tasks within IT teams	act as an IT team leader, adapting one's leadership and communication style as needed; mentor and promote best practices in IT within an organisation	act as an authority in the development of new technical skills, mentoring, and leadership within the IT sector; coordinate current international forms of knowledge exchange in digital ecosystems

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
XIII. User-centred approach	is ready to…	**IT user support**	demonstrate empathy, patience, courtesy, and good manners when interacting with users, including in situations of stress, time pressure, or frustration on the part of the IT system user	actively listen to the IT system user and ask questions to fully understand their situation and genuine needs; adapt the style of communication and form of IT support to the diverse needs of users (e.g., those who are less technically-savvy, older, or working under significant time pressure)	treat IT system users as partners, without blaming them for errors, mistakes, or a lack of technical knowledge	respond assertively to inappropriate behaviour or unrealistic expectations on the part of IT system users, while maintaining a respectful and professional tone; support users in learning to use digital systems and services in a patient, friendly, and non-condescending manner	build and maintain relationships with IT system users based on trust and cooperation; explain the objectives of the changes being introduced to IT system users in the context of the benefits to the organisation	
		Needs analysis and attention to the user experience of IT systems		engage in understanding the needs, expectations, and limitations of IT system users, taking into account people with disabilities and those who are digitally excluded	take the IT system user's perspective into account when planning and implementing activities; accept feedback and criticism from IT system users as a source of information for improving the user experience	collaborate with other individuals and teams to improve the user experience of the IT system; recognise the diversity of users and strive to reduce barriers to the use of IT solutions	build trust in IT solutions by taking into account the needs of IT system users within the context of an organisation's needs	
XIV. Responsibility and ethics		**Digital ethics and the responsible use of technology**	act in accordance with an organisation's internal IT regulations; report unethical behaviour and misconduct in the digital environment, while upholding the principles of confidentiality and the protection of whistleblowers	comply with legal regulations concerning IT	take into account the perspectives of different user groups, including those at risk of digital exclusion; use IT responsibly and for its intended purpose; **(GC) take into account the impact of digital solutions on the environment and sustainable development**	collaborate with other individuals and IT teams to identify ethical risks and develop responsible technological solutions; promote a culture of the responsible use of IT technology within one's work environment	set ethical boundaries when using IT, including in situations of business pressure; engage in educational and awareness-raising activities concerning digital ethics; **(GC) take action and select IT technologies that limit negative impact on the environment**	take innovative measures to protect society from the unethical consequences of IT use
		Ensuring information security		ensure information security, in particular its integrity, confidentiality, and availability within IT systems; respect the privacy of IT system users	take information security and privacy into account when making day-to-day decisions in the digital environment; take into account the needs of those particularly vulnerable to privacy breaches in the digital environment	cooperate in the digital environment to eliminate risks relating to information security, data protection, and privacy	take responsibility for the causes and consequences of the misuse of information and digital data	

SECTORAL DETERMINANT		COMPETENCE SERIES	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	LEVEL 7	LEVEL 8
XIV. Responsibility and…	is ready to…	**Autonomy and responsibility for performing tasks**	draw on the expertise of experienced IT specialists; follow established IT instructions and procedures when performing tasks	independently plan and conduct one's own tasks in accordance with the agreed scope within a digital environment	take responsibility for the completion of one's own tasks or IT projects	take responsibility for the completion of team tasks and the quality of the IT solutions delivered	take responsibility for the consequences of decisions made in the area of IT systems and services	take responsibility for the immediate and long-term consequences of strategic decisions regarding IT systems and services
XV. Development and innovation		**Personal development and adaptation to technological changes**	accept simple guidance on improving one's work in the IT environment	accept feedback on one's work and use it to develop IT skills; learn from mistakes and speak openly about them in a way that encourages learning in a digital environment	openly communicate one's IT development needs; remain flexible in the face of organisational, process, and technological changes in the digital environment	actively seek out new solutions, tools, and practices in the IT environment, and skillfully select and assess their suitability; step outside one's comfort zone and take on new tasks relating to a variety of IT technologies	develop strategies to help colleagues adapt to technological changes in the digital environment; share learning methods and experiences of working with new IT technologies	initiate innovative activities that foster continuous development and experimentation with new technologies within the digital ecosystem
		Developing and supporting digital innovation		collaborate on testing improvements to IT systems	submit ideas for improving processes that use IT systems; encourage colleagues to experiment with new IT solutions and tools	actively participate in initiatives to improve processes that use IT systems; **(GC) support sustainable development initiatives within an organisation**	support an organisation's digital culture based on continuous improvement, experimentation, and learning; work within an interdisciplinary team supporting digital innovation; **(GC) recommend innovative IT solutions while taking environmental aspects into account**	support and act as a leader in innovative transformations across the digital ecosystem create interdisciplinary teams supporting digital innovation

5. Glossary of terms used in the Sectoral Qualifications Framework for Information Technology

TERM	DEFINITION
Access control list (ACL)	ACL is a mechanism for defining who has access rights to what within a system or network. It is a list of rules that specify which operations (e.g., read, write, network connection from a given address) are permitted or blocked for specific users, groups, addresses or services. In practice, it is used to enforce security policies in operating systems, firewalls, and switches, among others.
Access point (AP)	A network device that connects a wired network to a wireless network and enables Wi-Fi devices to connect to the local network. An access point performs the functions of transmitting and receiving radio signals, authenticating users, as well as enforcing basic security and quality of service policies for wireless traffic.
Account takeover	A cyberattack designed to gain access to a victim's profile, e.g., to steal data, send spam or defraud contacts. The most common methods of attack include phishing, malware, and password theft. Protection measures include, for example, changing passwords frequently or using two-factor authentication.
Active directory (AD)	Microsoft directory services for the centralised management of users, computers, and resources in Windows-based networks (equivalent to LDAP).
Actuators	Actuators are devices that convert a signal from a control system into a physical action in an object, for example, opening/closing a valve, changing the position of a cylinder or starting a drive. Actuators are the final element in a control loop—they implement changes in the technological process in accordance with the decisions of the control system.

Address resolution protocol (ARP)	A network mechanism used to determine which hardware address of a network interface (the physical address of a network card) corresponds to a given IP address on a local network. It enables devices to communicate by identifying the hardware address of a network card based solely on its IP address, which is necessary for forwarding frames to the correct recipient on the same network.
Agile	A set of principles and practices for managing software and product development based on the iterative delivery of increments, close collaboration with stakeholders, and rapid response to changing requirements. Agile emphasises short planning and implementation cycles, continuous inspection and adaptation, and building business value in small, frequent increments.
Agile Waterfall Hybrid	A project management approach in which part of the scope or work stream is performed using Agile methodologies (e.g., Scrum, Kanban), and part using a waterfall approach, with coordination at the level of a shared plan and integration points. It requires defined interfaces between teams, agreement on how to report progress, and consistent risk and scope management across both working styles.
Amazon Web Services (AWS)	Amazon's cloud services platform providing computing resources, storage, databases, networking, security, and analytics services. It enables IT systems to be built and operated without the need to purchase one's own infrastructure, based on a pay-as-you-go model.
Ansible	A tool developed by Red Hat for automating and orchestrating infrastructure configuration and application deployment. It allows the desired state of systems (servers, services, containers, network devices) to be described declaratively in text files and configured en masse using tasks executed from a control server. Widely used in configuration management, repeatable deployments, and the 'infrastructure as code' approach, it reduces the number of manual operations and the risk of configuration errors.

Anti-patterns	A term in IT architecture or software engineering that describes repetitive, ineffective or unproductive solutions, which seem reasonable at first glance, but in practice lead to poor results, high technical debt, and difficulties in maintaining the system. Anti-patterns describe common mistakes made when deciding on the IT architecture (e.g., excessive coupling of system components, lack of separation of concerns in the software code, concentrating too many system functions in a single class or module, vendor lock-in or software code with a chaotic structure), as well as the consequences of these decisions and ways to avoid or eliminate them.
Apache Kafka	A distributed platform for the reliable exchange and processing of event streams (e.g., logs, application messages) between systems. It enables events to be published to logical topic-based channels and received in parallel by multiple services, while maintaining data durability and re-readability. Used for system integration, building event-driven architectures, and load balancing between data producers and consumers.
API-first approach	An approach to system development in which the API interface (scope of operations, data formats, errors, versioning, and security rules) serves as the starting point, with services and integrations implemented only afterwards. The aim is to ensure consistent integration, enable teams (backend, frontend, integration) to work in parallel, and provide better control over changes through formal API lifecycle management.
API management	A set of processes, tools and components used to design, publish, secure, version, monitor, and bill for the use of APIs. This includes, among other things, API gateways, API catalogues, authentication and authorisation mechanisms, call limits, traffic analytics, and the API lifecycle (from design to decommissioning), so that integration between systems is controlled, secure, and measurable.
API security testing	The process of detecting vulnerabilities and weaknesses in application programming interfaces. The test simulates a hacker attack, enabling the identification of weak points, and the protection of data against unauthorised access, modification or theft. The data analysis process includes testing of authentication, authorisation, validation, encryption, and resistance to attacks, using both manual and automated methods.

Application architecture	The logical structure of a system that defines how its components are organised, how they interact with one another, and how they support business objectives by ensuring scalability, maintainability, and performance. It defines the division into layers (e.g., presentation, business logic, data) and integration patterns, and also facilitates the development, testing, and management of the system.
Application environment	A specific set of hardware, software, and network resources that hosts an application and enables it to function correctly. Such an environment contains everything needed to run, manage, test, and develop the application.
Application plane	The application logic layer in which network-using programs (e.g., management applications, orchestration systems, security systems) operate and describe the 'intent'—what the network is supposed to do. The application plane communicates with the control plane via interfaces (e.g., APIs), conveying policies and business requirements, but it does not perform physical packet switching.
Application programming interface (API)	A set of rules and specifications enabling communication and data exchange between different applications or systems. It acts as an intermediary, allowing data to be exchanged between different systems and platforms without the need for direct integration. Thanks to APIs, new applications can be built using existing services and data.
ArchiMate	An open, independent modelling language designed to describe, analyse, and visualise enterprise architecture. It integrates the business, data, application, and technology domains in a coherent manner, supporting the management of complex changes within an organisation at various levels of detail.
Architectural patterns	Generalised, tried-and-tested schemes for building IT systems, describing the division into components and layers, their responsibilities, and how they communicate with one another. Architectural patterns (e.g., layered architecture, microservices, event architecture, client–server architecture) serve as a reference point when designing solutions that facilitate consistent design decisions and communication between architects and development teams.

Artificial intelligence (AI)	Artificial intelligence is a field of computer science that develops systems capable of autonomously achieve their goals by learning from their own experiences and adapting to new data. Artificial intelligence can be implemented using various techniques, such as machine learning, deep learning, expert systems, genetic algorithms, neural networks, and natural language processing.
Artificial intelligence (AI) agent	A component of an IT system that uses artificial intelligence methods to independently achieve a goal by planning steps, making decisions, and performing actions within an environment (e.g., invoking tools, using APIs, running procedures). An AI agent can maintain task context (state), apply security rules and access control, as well as perform tasks in a partially autonomous manner under human supervision.
Artificial intelligence trust, risk, and security management (AI TRiSM)	AI TRiSM refers to AI systems that are fault-tolerant (safety), operate in accordance with the law (compliance), and allow for full control over their decisions (auditability).
AS-IS	A business process analysis model describing the current state of components and their relationships, including 'bottlenecks' (the project's baseline).
Attribute-based access control (ABAC) model	An attribute-based access control is a model in which decisions on granting access are made based on a set of attributes describing: the user, the resource, the environment, and the action. The ABAC system analyses these attributes in real time and applies defined policies to determine whether a given access is permitted.
Augmented reality (AR)	A technology that involves superimposing digital information (e.g., graphics, text, 3D models, contextual cues) onto the image of the real world as perceived by the user, in real time. AR uses sensors and algorithms for positioning and environment recognition to place virtual elements in the correct location and scale, supporting, among other things, training, maintenance, navigation, and data visualisation in a physical environment.

Autonomous vehicle (AV)	A vehicle equipped with perception, localisation, and decision-making systems, capable of independently performing driving tasks under specific traffic conditions. It uses data from sensors (e.g., cameras, radar, LIDAR) and control algorithms to maintain its course, detect obstacles, and plan manoeuvres, with limited or no driver involvement, depending on the level of autonomy.
Basic Service Set (BSS)	The simplest logical unit of a Wi-Fi network. BSS is a single access point and the client devices connected to it that share the same radio spectrum. Such a set forms a single wireless network cell within which communication takes place.
Bias	A bias in data or a model consisting of a systematic, recurring deviation in the data, model, or analytical procedure, leading to distorted results, for example, favouring or discriminating against specific groups or misjudging risk or quality. Bias may be caused, among others, by incomplete or uneven training data, labelling methods, feature selection, algorithm design, or the data collection process itself. It is a key issue in the design and evaluation of data-driven and artificial intelligence systems.
Big data	Data sets of such a large scale, volume, and variety that processing them using traditional database tools is inefficient or impossible. They encompass structured, semi-structured, and unstructured data, and require distributed processing platforms, specialist analytical tools, and automated processing workflows to extract business value.
Blockchain	A distributed ledger model in which events (e.g., transactions) are grouped into blocks cryptographically linked together in an ordered chain. Copies of the ledger are maintained by multiple network nodes, and data consistency is ensured by a consensus mechanism. A key feature of blockchain is its resistance to unauthorised modifications of historical records and the ability for all participants to verify the state of the ledger in accordance with the agreed protocol rules.
Border Gateway Protocol (BGP)	The Border Gateway Protocol is used to exchange routing information between autonomous systems on the Internet. BGP enables the selection of routes based on routing policies (e.g., operator preferences) rather than solely on technical metrics, thereby supporting traffic control, link redundancy, and ensuring service availability on a global scale.

Bourne Again Shell (Bash)	A system shell used primarily on Unix-based systems (Linux, macOS). It enables interactive command execution and task automation via shell scripts (e.g., software installation, file processing, system operations). It is the *de facto* standard shell in most Linux distributions and a fundamental tool for system administrators and DevOps engineers.
Brain–Computer Interface (BCI)	A technology enabling communication between the nervous system and a computer system, in which biological signals (e.g., brain electrical activity) are recorded, processed, and translated into commands to control devices or applications. BCI can operate in non-invasive or invasive modes and is used, among other things, in rehabilitation, to assist people with disabilities, as well as in human–machine control and interaction systems.
Bring your own device (BYOD)	This is a company policy that allows employees to use their own personal devices (smartphones, tablets, laptops) for work purposes, such as accessing company emails, data, and applications, rather than relying solely on equipment provided by the employer. It requires the implementation of strict security rules (BYOD policy) and the separation of private and work spaces.
Business architecture	A comprehensive approach to describing an organisation, defining its strategic objectives, processes, structure, capabilities, and value streams. It creates a coherent plan that aligns operations with strategy, enabling better management, planning, and implementation of change. It bridges the gap between business and technology, ensuring the effective functioning of the enterprise.
Business continuity plan (BCP)	A document of strategic importance, setting out procedures and instructions enabling an organisation to continue or rapidly resume critical business functions in the event of serious disruptions. A BCP goes beyond simply responding to incidents, providing a systematic approach to building organisational resilience against a variety of threats and crisis situations. A BCP focuses on maintaining the operational continuity of the entire organisation, not just IT systems or individual processes.

Business intelligence (BI)	A set of methods, processes, and tools used to transform operational data into information used for decision-making within an organisation. It includes, among other things, data warehouses, data integration and processing, reporting, management dashboards, and multidimensional analyses aimed at supporting management and monitoring the achievement of objectives.
Business Process Model and Notation (BPMN)	A standard graphical notation used for modelling business processes in the form of diagrams describing process steps, events, decisions, roles, and workflows. It provides a common language for describing processes for both business and IT, used for the analysis, optimisation, and automation of processes within an organisation.
C4	A method for visualising system software architecture across 4 levels: ▪ Context—users and systems, ▪ Containers—applications, databases, services, ▪ Components—logical groups of code within a container, ▪ Code—implementation, classes, interfaces.
Cache memory (cache)	Very fast temporary memory in electronic devices or software that stores frequently used data. This allows the data to be used without having to be retrieved each time, which significantly speeds up page loading and overall system performance.
Canva	A cloud-based graphic design platform, accessible via a browser or app, used to create simple graphic designs, such as presentations, marketing materials, social media graphics, and simple infographics. It provides ready-made templates, a library of graphic elements, and team collaboration tools aimed at non-technical users.
Carbon-aware computing	An approach to the design and operation of IT systems in which the planning and deployment of computational workloads takes into account the current or projected carbon emissions of electricity. It involves controlling the time and place in which tasks are performed (e.g., rescheduling computational batches, selecting a data centre region, prioritising tasks) in order to reduce emissions while maintaining the required service quality parameters.
Central processing unit (CPU)	The main component of a computer responsible for executing program instructions and processing data, also known as a processor.

Change	The addition, modification, or removal of anything that could have a direct or indirect impact on IT services. Changes must be managed in such a way as to minimise the risk of incidents that disrupt the achievement of business objectives.
Cloud	IT resources (computing power, storage, network services, databases, etc.) provided remotely by an external supplier via a network, without the need to own and maintain one's own physical infrastructure.
Cloud bursting	A cloud usage pattern in which the baseline workload is handled by on-premises or core infrastructure, while also temporarily moving some tasks to the public cloud during periods of peak demand. This allows for increasing computing power only when there is high traffic without the need to maintain an oversized infrastructure on a permanent basis.
Cloud computing	A model for the provision of IT resources (computing power, storage, network services, databases, etc.) by an external provider via a network, usually billed on a pay-as-you-go basis. The user utilises resources made available remotely, without the need to own or maintain their own physical infrastructure.
Cloud financial operations (FinOps)	An approach that brings together technical, financial, and business teams to maximise the business value of the cloud by optimising costs, increasing spending transparency, and sharing financial responsibility. It involves fostering a culture of collaboration and financial discipline within the dynamic cloud environment, enabling informed decisions regarding spending and innovation.
Cloud native	An approach to designing and building applications that fully leverages the benefits of cloud computing, as opposed to simply migrating traditional applications to the cloud. The key pillars of the cloud native approach are: microservices (the application is divided into small, independent modules that communicate with each other), containerization (packaging the application along with its runtime environment), managed services (using ready-made database, queue, or cache services provided by the cloud provider), automation (deployment and updates occur automatically), and scalability (the application automatically adjusts resources to current traffic). The advantages of this approach include high availability, resilience, flexibility, and rapid deployment.

Cloud-native application	Software designed and built from the ground up to leverage the flexibility, scalability, and dynamism of the cloud environment. It utilises microservices, containerisation, and orchestration to create resilient, automatically scaling systems that deliver business value quickly.
Communication encryption	The process of converting data into a code known only to authorised recipients. With the appropriate keys, it protects data from eavesdropping and unauthorised access. It secures data at rest, and in transit, and its implementation is often a regulatory requirement.
Compensation methods	In IT systems engineering and the technical field, 'compensation' refers to error compensation or fault tolerance techniques that ensure the reliability and stability of system operation. IT compensation (fault tolerance) refers to a set of techniques that minimise the effects of delays, data loss, or failures, enabling the system to operate smoothly despite environmental imperfections.
Comprehensive Knowledge Archive Network (CKAN)	Software used to build data portals where datasets are published along with descriptions, metadata, versions, licences, and search mechanisms. It facilitates the management of data catalogues (including open data), the sharing of files or access interfaces, and the quality control and consistency of information about datasets.
Configuration management database (CMDB)	The CMDB stores detailed information about an organisation's IT assets, such as hardware, software, and services, as well as definitions of the relationships between them. It serves as a key repository of knowledge regarding configuration items (CIs).
Containerisation	The process of packaging an application along with its components (libraries, configuration files) into an isolated, portable environment known as a container. This enables the application to run on any infrastructure. It is an alternative to virtual machines–containers share the host operating system's kernel rather than emulating the entire system.
Content delivery network (CDN)	A geographically distributed network of proxy servers that stores copies of content (e.g., static files, video, web resources) closer to end users. It minimises latency and the load on origin servers, increases service availability, and enables the use of additional security mechanisms at the network edge.

Continuous integration and continuous delivery/ deployment (CI/ CD)	CI and CD automate the processes of building, testing, and deploying code, enabling faster and more reliable delivery of updates to users, while eliminating manual steps and errors. CI (continuous integration) involves frequent integration and testing of changes, whereas CD (continuous delivery/deployment) automates delivery or automatic deployment.
Control Objectives for Information and Related Technologies (COBIT)	A set of principles, processes, and reference models used to design and assess corporate governance and manage the IT function within an organisation. COBIT helps to align business objectives with IT objectives, define responsibilities, metrics, control mechanisms, and compliance requirements, so that information technology supports the organisation's strategy in a controlled and auditable manner.
Control Plane	The layer responsible for making decisions regarding how network traffic should be routed. It runs protocols and mechanisms that build a picture of the topology and determine routes (e.g., routing protocols), and then installs the appropriate rules in the data plane. In centrally controlled architectures, the control plane may be moved from devices to an external controller that manages multiple switches simultaneously.
Critical system	A system whose disruption or failure could have serious consequences for human safety, the continuity of an organisation's operations, the environment, or infrastructure. It requires heightened standards in terms of reliability, availability, security (including cybersecurity), redundancy, and strict control of changes throughout its entire lifecycle.
Cross-cloud solutions	An architecture and system operating model in which a single application or service is designed to operate simultaneously across multiple clouds from different providers, with active integration between these environments. It encompasses the consistent management of traffic, identity, security configuration, and data across multiple clouds, enabling controlled load balancing, service redundancy, and the maintenance of uniform policies across the entire environment.
Cybersecurity	Measures, policies, and procedures aimed at maintaining the organisation's business continuity by protecting systems, networks, data, their users, and other entities against unauthorised access, use, disclosure, disruption, modification, or destruction, and the ability to restore business continuity following an incident.

Dashboard	A tool for visualising data in the form of a dashboard or interactive page. It presents aggregated key data, metrics, and performance indicators from various sources in one place, enabling convenient status monitoring, trend analysis, and decision-making.
Data architecture	A general plan and model defining how data is collected, stored, integrated, managed, and utilised within an organisation. It creates a coherent system supporting business and IT objectives, ensuring the consistency and availability of information, as well as managing the data lifecycle.
Data centre	A specialised facility and technical infrastructure designed to support IT systems and digital services, including servers, networks, storage, and an environment ensuring business continuity (primary and backup power supplies, cooling, monitoring, physical security). A data centre meets requirements for availability, capacity, and fault tolerance, and forms part of an organisation's security architecture, including access control, segmentation, event logging, and operational procedures).
Data Ethics Canvas	A structured analytical template used to identify and assess ethical risks associated with the collection, processing, and use of data and analytical models. It organises the analysis in areas such as: stakeholders and impact, data sources and quality, biases and unequal impacts, transparency, consents and legal bases for processing, security, accountability, and risk mitigation measures.
Data lake	A central repository where large amounts of raw data are collected, including structured (tables), semi-structured (logs, JSON), and unstructured (files, multimedia) data. Data is stored without first imposing a uniform schema. The way it is structured and the data model are only defined at the read stage for the purposes of a specific analysis, reporting, or modelling.
Data lakehouse	A data architecture and platform that combines the data storage approach typical of a data lake (a repository of raw and semi-processed data in scalable storage) with mechanisms characteristic of a data warehouse (a layer of tables with transactional guarantees, schema management, SQL support, and analytical capabilities). It enables analyses and models to be performed on a shared data layer, without the need to build separate, duplicated repositories.

Data leak	The unauthorised disclosure of confidential, sensitive, or personal information (e.g., usernames, passwords, credit card details, national insurance numbers) to unauthorised parties. Such data is often used for fraud, identity theft, or account hacking. A leak may occur as a result of deliberate hacking attacks, human error, or vulnerabilities in IT systems.
Data mesh	A data organisation and architecture model in which responsibility for data is distributed across business domains, with each domain publishing its own 'data products' in accordance with agreed standards. Instead of a single centralised data warehouse or data lake, a federated management model is used, along with a shared infrastructure and a set of quality, security, and interoperability rules enforced across the entire data environment.
Data plane	The part of a network device responsible for the actual processing and forwarding of packets in accordance with pre-configured rules. Operations such as forwarding to a specific port, tagging, filtering, or queuing traffic are performed on the data plane without making routing decisions 'from scratch' for each packet.
Data replication	The creation and maintenance of copies of data across multiple servers (replicas), ensuring availability, fault tolerance, and improved performance and scalability through load balancing. It allows for a rapid switchover to a copy in the event of problems. This is a solution that minimises downtime (the basis of business continuity and disaster recovery strategies).
Data science	A field of science combining statistical methods, machine learning, programming, and data engineering to extract knowledge from data and build models supporting business or technical decisions. It covers the full data lifecycle: acquisition, preparation, exploration, model building, and validation, followed by deployment into operational environments.
Data warehouse	A centralised, integrated data repository designed for the long-term storage of information from multiple source systems for reporting and analysis purposes. Data in a data warehouse is typically cleansed, standardised, organised by subject and history, while the structure and access mechanisms are optimised for analytical queries rather than day-to-day transaction processing.

Debian	A Linux-based operating system distribution, developed as a community project, known for its high stability and conservative approach to updates. Often used as a base for other distributions and in production server environments.
Decentralised applications (dApps)	Applications whose business logic is based on a distributed ledger infrastructure (e.g., blockchain), with some functions implemented via smart contracts. A dApp uses a network of nodes to perform operations and state storage, meaning it is not dependent on a single, central server, and its operating rules are derived from the code and network protocol.
Deduplication (or data deduplication)	A technology for eliminating redundant duplicate copies of data in a storage system. Used particularly in backup and archiving systems. It leads to savings in disk space and data transfer time. It works by identifying unique blocks or fragments of data and storing only a single copy of them.
Deep learning (DL)	A subfield of machine learning based on multi-layer neural networks that automatically learn feature representations from input data. Deep learning is used, among other things, in image and speech recognition, natural language processing, and sequence and signal analysis. It typically involves large datasets and high computational demands.
Deepfake	A technology that utilizes advanced forms of artificial intelligence, combining deep learning with content manipulation to create extremely realistic yet false video, audio, and image content. This allows for the creation of illusions for the purpose of disinformation, fraud, but sometimes also entertainment (e.g., creating fake statements by politicians and celebrities, special effects in movies). This technology blurs the line between truth and falsehood, making it difficult to verify information and potentially damaging the reputations of private individuals.
Demilitarised zone (DMZ)	A separate network segment located between the public network and the organisation's internal network, intended for providing services accessible from the outside (e.g., web servers, mail gateways). The DMZ is separated by traffic filtering rules to limit the possibility of direct access to internal resources and to minimise the impact of any compromise of services exposed to the Internet.

Denial of service (DoS)	A type of cyberattack aimed at preventing a service or system from functioning properly by overloading it with an excessive number of requests or by exploiting software vulnerabilities. The result of the attack is that the service becomes unavailable to authorised users. The system runs very slowly, stops responding, or completely refuses to handle further connections.
Design thinking	An iterative approach to problem-solving and the design of products or services, based on a deep understanding of user needs, the generation of multiple concepts, rapid prototyping, and testing solutions. It combines the user's perspective, technical feasibility, and business viability within structured stages of team work.
Development environment	A specially configured environment in which developers create, test, and develop software. It provides the necessary tools, libraries, runtime environment, and other resources required for writing, debugging, and testing code.
DevOps	A combination of the words 'Development' and 'Operations' that refers both to an organisational culture and methodology, as well as a set of practices and tools aimed at automating and integrating processes between software development teams and IT infrastructure teams. The use of DevOps aims to shorten the system development cycle and improve the delivery times, quality, and reliability of the software being developed.
DevSecOps development (Dev) + security (Sec) + operations (Ops)	The evolution of DevOps, which incorporates security as an integral part of every stage of the software development life cycle. It introduces the 'shift left' principle, meaning that security-related activities must be integrated as early as possible—during the design, coding, and testing phases—which allows anomalies to be detected and rectified before they incur costs.
Digital assets	Resources of value to an organisation or individual existing solely in electronic form. These include, among others, data files, databases, software, service accounts, cryptographic keys, tokens in distributed ledgers, and other records that may be traded, licensed, or require protection. In security management, they are treated as assets for which the owner, value, required level of protection, and lifecycle are defined.

Digital ecosystem	An integrated network of interrelated technologies, data, applications, services, and users that interacts via specific interfaces and information flows, creating value for the organisation and its environment. It encompasses technical components, organisational processes, collaboration models, and security mechanisms treated as a single coherent digital services environment.
Digital service	An interactive online solution that enables users to create, process, store, or access data in digital form. Basic examples include social media platforms, financial services, streaming services, search engines, mobile apps, etc.
Digital subscriber line (DSL)	A broadband access technology that uses existing copper telephone lines to transmit data at much higher speeds than traditional analogue telephony. It utilises frequency band division in such a way as to enable parallel data transmission and simultaneous use of telephone services, often in variants tailored to the needs of home and business users.
Digital twin	A digital representation of a physical object, system, or process, maintained and updated based on operational data (e.g., measurements, logs, telemetry). A digital twin enables the monitoring of status, analysis of behaviour over time, simulation of change scenarios, and forecasting the effects of failures and maintenance activities in a manner that reflects the real operating environment.
Direct liquid cooling (DLC)	A technique for removing heat from IT components (e.g., processors, GPUs) using a coolant fed directly to the heat-generating elements, for example, via cooling blocks or immersion in a dielectric fluid. DLC allows for higher power density and better energy efficiency than traditional air cooling, which is particularly important in modern data centres with high equipment density.
Disaster recovery (DR)	A key IT strategy ensuring business continuity. DR focuses on the rapid restoration of services following a major disaster (e.g., fire, flood) using backups and systems at a separate location.

Disaster Recovery as a Service (DRaaS)	DRaaS is a cloud-based service that ensures business continuity and rapid recovery of IT systems after a failure. It involves replicating data and applications to an external data centre, which allows it to take over operations in the event of hardware failure caused by various factors. In case of an outage, the provider's cloud becomes the temporary data centre and, unlike a standard backup, it enables the entire environment to be launched in a very short time.
Disaster recovery plan (DRP)	A detailed, documented set of procedures and instructions that specify how an organisation is to restore its critical functions, IT systems, and data following a major failure. A DRP focusses technically on systems, data, and networks.
Discretionary Access Control (DAC)	An access control model in which the owner of a resource (e.g., a file, directory, or system object) can independently grant and revoke permissions to other users or groups. Access decisions are based on permissions set by the owner, as well as the system's inheritance mechanism and permission lists, rather than a centrally imposed security policy.
Distributed denial-of-service (DDoS)	A type of cyberattack in which a very large number of infected devices simultaneously send traffic to a selected service or system, overloading its resources. This leads to the service becoming unavailable to authorized users, often using a network of infected devices (a botnet).
Distributed Version Control System (DVCS)	A distributed version control system that allows you to track changes to files (usually source code), collaborate effectively on a project as a team, and easily revert to previous versions, enabling multiple people to work effectively on the same code. It runs locally but is often used with cloud platforms (such as GitHub or GitLab) to host repositories and coordinate teamwork.
DKAN—an open-source open-data platform	Software for building an open data portal, enabling the cataloguing and publication of datasets along with metadata and access interfaces. DKAN is developed as open source and is distributed free of charge and without licence fees. The 'no licence/subscription' model applies to the software, not the data.
Docker	A platform for building, packaging, and running applications as containers. It standardises the runtime environment (dependencies, libraries, configurations), which facilitates the porting of applications between systems and the automation of deployments.

Domain Name System (DNS)	A hierarchical, distributed system of network services that maps domain names (e.g., google.com) to their corresponding IP addresses and other records (e.g., MX, TXT, SRV). It enables users and applications to employ user-friendly names instead of numerical addresses. It is a critical component of the Internet infrastructure and a common attack vector (e.g., spoofing, cache poisoning).
Drivers/controllers	Devices or logic modules that process signals from sensors and generate control signals for actuators in accordance with programmed control algorithms. In industrial environments, these are most often programmable controllers (e.g., PLCs), which implement process logic, monitoring, safety functions, and communication with higher-level systems.
Dynamic Host Configuration Protocol (DHCP)	A network protocol used to automatically assign configuration parameters to devices on a network, such as: IP address, subnet mask, default gateway, DNS server addresses, and other options. It centralises address management and reduces errors associated with manual configuration.
Edge computing	An architectural model in which part of the data processing is moved from central data centres closer to where the data is generated, e.g., to local nodes within a plant, branch, operator's network, or device. This allows for faster response times (lower latency), preliminary filtering or aggregation of data, and reduces the load on links to central systems, which is crucial in near-real-time systems and distributed environments.
Embedded system	A specialised computer system that forms part of a larger device or installation, designed to perform specific control, measurement, or communication functions. An embedded system typically operates on limited hardware resources, runs continuously or in real time, and is closely integrated with the physical components of the device. Examples include sensors collecting data from the environment or controlling a device (such as refrigerators, temperature sensors, pacemakers).
Endpoint configuration	The process of customising and securing device endpoints as well as defining communication parameters for APIs (interfaces). This includes setting security policies, managing access, and defining methods of data exchange between applications and systems.

Enhanced Interior Gateway Routing Protocol (EIGRP)	A routing protocol used within an administrative domain, enabling dynamic route determination between subnets. EIGRP uses an algorithm to select the best path based on a composite metric (e.g., delay and bandwidth), ensures rapid route recalculation following a failure, and limits the broadcasting of changes to the absolute minimum, which improves scalability in enterprise networks.
Enterprise architecture	A formal description of an organisation's structure and functions, covering business, data, applications, and technology. Its aim is to ensure consistency, efficiency, and support for the achievement of strategic objectives by mapping relationships, establishing guidelines, and managing change in a complex environment. It acts as a bridge between business and IT, helping to avoid mistakes and make better technological decisions.
Enterprise blockchain	Advanced blockchain technology in organisational environments and consortia (permissioned blockchains) responding to business needs that require the security of a distributed register, but without the complete anonymity and openness of public networks such as Bitcoin, typically in a restricted-access model (permissioned networks). These types of solutions are characterized by participant identity verification, a high level of regulatory compliance, and integration with existing IT systems.
Enterprise Service Bus (ESB)	A central component of integration architecture, through which message exchange takes place between IT systems. The ESB acts as a common integration point, ensuring standardisation of communication, message routing, data format transformation and protocol mediation, as well as the central enforcement of policies regarding security and communication reliability (error handling, retries, queuing) within the framework of system integration.
Environmental, social, governance (ESG)	A comprehensive set of criteria for assessing and reporting on how an organisation is managed across three dimensions: environmental impact (e.g., emissions, energy, resource consumption), social responsibility (e.g., working conditions, impact on stakeholders), and corporate governance (e.g., oversight, compliance, transparency). ESG is used in the IT and cybersecurity sectors to manage non-financial risks, ensure operational stability, build stakeholder trust, and promote the responsible use of technology (e.g., measuring the environmental footprint of digital services).

Ethernet	A family of wired networking technologies used primarily in local area networks. It defines how data is encoded on the transmission medium, the frame format, and the rules for accessing the medium, so that multiple devices can share a single physical network. Ethernet includes both the physical layer (cable type, connectors) and the data link layer (MAC addresses, frames, basic collision detection mechanisms), with subsequent versions developed to support ever-higher data rates.
Event-driven	An architectural and programming model in which system components communicate and respond to events rather than directly calling functions. This enables the creation of flexible, scalable, and decentralised systems commonly used in microservices and modern applications, where producers emit events and consumers receive and process them using, for example, message brokers.
Event-driven architecture (EDA)	A style of system architecture in which communication and the execution of business logic are based on events describing the occurrence of a specific state change. Events are published by source components and consumed asynchronously by other services, enabling the loose coupling of systems, scalable processing, and the construction of near-real-time workflows.
Event logs	Sets of records describing events occurring in systems, applications, network devices, or services. Each log entry contains the event type, a timestamp, and additional context (e.g., user ID, IP address, error code). Event logs are a primary source of information for monitoring, incident analysis, auditing, and reconstructing the sequence of events in an IT/OT environment.
Exit plan	A plan of actions as well as technical and organisational requirements ensuring the ability to cease using a service, platform, or provider and switch to another solution. In particular, it includes the rules for data and configuration migration, business continuity, a disconnection schedule, archiving requirements, and the controlled deletion of data and access rights following migration.

Exploratory data analysis (EDA)	A stage of data analysis involving an initial examination of a dataset to understand its structure, distributions, relationships, and quality. EDA includes, among other things, the identification of missing data, outliers, inconsistencies, and correlations, as well as the verification of the assumptions supporting the selection of processing methods, feature engineering, and further modelling.
Extended service set (ESS)	A group of several interconnected BSSs linked by a shared wired infrastructure and usually operating under the same network name. It forms a single logical Wi-Fi network covering a larger area and allows users to move seamlessly between access points without losing their connection.
Extract, load, transform (ELT)	A data integration process in which data is first retrieved from sources, then loaded into a target system (e.g., a data warehouse or analytics platform), and only then transformed within that system. ELT utilises the computational power of the target platform for transformations and is frequently used in cloud environments and when working with large volumes of data.
Extract, transform, load (ETL)	A classic data processing method in which data is extracted from various sources (operating systems, files, databases); transformed (cleaned, merged, recalculated, and adapted to the target model); and then loaded into a data warehouse, analytical repository, or other target system.
Fibre Distributed Data Interface (FDDI)	A local area network technology based on fibre optics and a dual logical ring. It ensures high reliability; if one ring is interrupted, traffic is automatically switched to the other path. Historically used mainly in critical campus networks and data centres as a high-speed (for its time) backbone network, it has now been superseded by newer variants of Ethernet.
File Transfer Protocol (FTP)	An application layer communication protocol used to transfer files between a client and a server on TCP/IP networks. It enables directory listing, file downloading and uploading, and file management from the client side. Historically, it has often been used in server administration and content publishing.

Firewall (FW)	A security mechanism (hardware or software) that controls network traffic between network segments based on defined rules. A firewall filters connections, allowing or blocking traffic in accordance with security policies, and depending on its functionality, may take into account addresses, ports, connection status, and application-level communication characteristics.
Flow tables	Data structures in network devices or the virtual layer that contain rules describing how to handle specific network traffic. Each entry in the table defines matching conditions (e.g., addresses, ports, protocol type) and actions (e.g., forwarding to a specified port, modifying headers, dropping, forwarding to an analysis module), which allows traffic flows to be controlled in a precise and programmable manner.
Framework	A structured set of components, rules, and patterns that defines how a solution—technical or organisational—is built and organised. In the field of software, a framework is an environment providing ready-made mechanisms (e.g., request handling, data access layer, security modules) into which the application's business logic is embedded. In a broader sense, a framework can also refer to a structured set of rules and practices used to implement specific types of processes (e.g., service or security management).
Function as a Service (FaaS)	A serverless cloud model that allows developers to run code in response to events, without managing the infrastructure. You are only charged for code execution, which speeds up problem-solving and reduces costs. Sometimes the service may refer to testing the resilience of systems against failures (Failure as a Service—FaaS).
Geographic information system (GIS)	An IT system used for the collection, storage, processing, analysis, and presentation of location-related spatial data. GIS integrates map data with descriptive data, enables spatial analysis (e.g., distances, ranges, layer overlay), and supports planning and decision-making in areas such as administration, infrastructure, the environment, and logistics.
GeoServer	A server for sharing spatial data (GIS) via standard web services, supporting the publication of map layers and services used, for example, in open data portals. GeoServer is open-source software, distributed under the GNU GPL v2 licence.

Google Cloud Platform (GCP)	GCP includes computing services, data storage, databases, machine learning services, analytics, and integration. The platform is used to build applications and systems that process large datasets, often integrated with other services in the Google ecosystem.
Google Remote Procedure Call (gRPC)	gRPC is a modern, high-performance framework for inter-application communication. It allows one programme to invoke (call) a function on another computer as if it were local, regardless of the programming language in which both programmes are written.
Grafana	A platform for data visualisation and monitoring that enables the creation of dynamic, interactive dashboards, real-time indicators, and the rapid identification of anomalies in IT systems. It is used to analyse various data sources and logs, and to track system performance.
Green coding	An approach to software design and implementation aimed at minimising the consumption of computational resources (CPU/GPU), memory, disk operations, and network transfer, and consequently, also energy consumption. This includes the selection of algorithms and data structures, performance profiling, the reduction of unnecessary computations, the optimisation of queries and input/output operations, and the conscious management of the application lifecycle (compilation, deployment, configuration, and operation) with a view to efficiency.
Green IT	An approach to the design, operation, and decommissioning of IT infrastructure that takes into account the minimisation of environmental impact. This includes, among other things, reducing energy consumption in data centres and at workstations, extending the lifecycle of hardware, responsible disposal, and the design of software solutions that reduce the demand for computing resources.
Group Policy Object (GPO)	A Windows server component comprising a set of rules and settings that enables administrators to centrally manage and enforce configuration, security, and software settings for users and computers within an Active Directory domain.

Hallucinations	Unreliable behaviour of a language model resulting in the generation of fictitious responses. In the context of generative models, this is a situation where the system generates responses that sound correct and convincing but are inconsistent with reality or unsupported by source data. Hallucinations stem from the probabilistic nature of the model's operation, limitations in the training data, and the lack of built-in fact-checking. They pose a significant risk when using such systems in tasks requiring high information reliability.
Hardening	The process of strengthening the security of a system, application, or device by reducing the attack surface. This includes, among other things, disabling unnecessary services, tightening configurations, using strong authentication mechanisms, updating software, and implementing the principle of least privilege.
Hardware environment	The collection of all physical components and devices that make up a computer system or IT infrastructure. These components form the platform on which the software operates.
Health check	An automated test performed periodically to verify that a service, application, or infrastructure component is functioning correctly and responding as expected. The result of the health check is used, among other things, by load balancers and orchestration systems to take instances that are malfunctioning offline.
Hewlett-Packard Unix (HP-UX)	A Unix-based operating system developed by Hewlett-Packard, designed primarily for enterprise-class servers. Used in critical business environments where high reliability, scalability, and advanced resource management mechanisms are required.
High Availability (HA)	A system feature that ensures business continuity and minimises downtime, even in the event of failures of individual components, services, or entire servers. HA systems aim to maintain full service functionality at all times.
Host	A device with an IP address on a network (computer, server, virtual machine) that provides resources.

Hybrid cloud	A cloud service model that integrates private cloud infrastructure with the public cloud to create a single environment. It allows for the flexible transfer of data and applications between clouds and leverages the advantages of both solutions—the flexibility and scalability of the public cloud and the security and control over data offered by the private cloud.
Idempotence of an operation	Idempotence means that performing an operation multiple times yields exactly the same result as performing it just once. Changes to the state of the system occur only once, regardless of the number of times the request is repeated.
Identity federation	Identify federation in IT is a system that allows users to log in to many different applications and services across various organisations (domains) using a single set of login credentials. This is made possible, by establishing a trust relationship between them. It works using identity providers (IdPs) and service providers (SPs), eliminating the need to juggle multiple passwords, which improves security and convenience, particularly in cloud and hybrid environments.
IEEE 802.11be—Wi-Fi 7 standard	A next-generation wireless standard from the Wi-Fi family designed to provide very high throughput, low latency, and better utilisation of the radio spectrum compared to previous versions. It specifies, among other things, operation in wider radio channels and the parallel use of multiple frequency bands, which is intended to support demanding applications such as high-definition video, gaming, and quasi-real-time systems.
IEEE 802.1X—port-based network access control	IEEE 802.1X is a standard for access control to wired and wireless networks, which requires the authentication of a device or user before allowing traffic through a network port. It uses a mechanism that acts as an intermediary between the client and the authentication server, enabling centralised enforcement of access policies.
Incident	An unplanned interruption or degradation of an IT service or an event which, if not resolved, may disrupt or degrade the performance of IT systems, IT services, or business processes. An incident requires a response to restore normal operations and to limit or minimise the negative impact on the organisation.
Independent Basic Service Set (IBSS)	A wireless network operating mode in which devices communicate directly with one another, without using an access point. It creates an *ad hoc* network in which each device acts as both a client and a traffic relay.

Information Technology Infrastructure Library (ITIL)	A globally recognised framework of best practices in the field of IT service management (ITSM). Its aim is to align IT services with business needs and objectives, as well as to maximise the return on IT investment. ITIL is not a rigid standard or methodology, but a set of flexible guidelines that can be adapted to the specific needs of any organisation, regardless of its size or sector.
Infrastructure as a Service (IaaS)	One of the models of computing services in which computing resources are hosted in the cloud. The service provider hosts the physical infrastructure, software, and a network with a specified bandwidth.
Infrastructure as code (IaC)	An approach to managing infrastructure (servers, networks, services, security configuration) by describing it in the form of code or declarative configuration files, stored in a repository, and versioned like software. It enables the automatic, repeatable recreation and modification of environments, as well as full control over configuration changes throughout the system's lifecycle.
Intent-Based Networking	An advanced approach to network management that allows administrators to describe desired business objectives in natural language, rather than manually configuring individual devices. The system automatically translates these objectives into policies and configurations, and then monitors and adjusts the network to ensure they are met.
Interface	A point of contact or mechanism that enables communication and cooperation between two systems, devices (e.g., a USB port) or between a person and a machine.
Internal developer platform (IDP)	An organisation's internal platform that provides development teams with standardised tools, services, and templates for building, deploying, and maintaining applications. IDP integrates elements of the software lifecycle (e.g., repositories, build and deployment automation, runtime environments, service catalogues, configuration and secret management, observability) into a cohesive set to reduce time-to-delivery, increase deployment repeatability, and facilitate compliance with security policies and organisational standards.

International Organization for Standardization/ International Electrotechnical Commission (ISO/ IEC)	Two international standardisation organisations that jointly develop standards and series of standards in the field of information technology and telecommunications. In an IT context, a reference to 'ISO/IEC' usually signifies a reference to recognised, formal standards for information security management, IT service quality, or software engineering.
Internet of Things (IoT)	A network of objects ('things') equipped with sensors that enable them to collect and exchange data via the Internet with other devices, systems, or users. They can form systems that automate processes, e.g., smart homes, cities, and industry.
InterPlanetary File System (IPFS)	A protocol and file storage system based on a distributed network of nodes, in which data is accessed based on its cryptographic identifier (content-based addressing) rather than the server's location. Files are divided into blocks, replicated across the network, and can be shared without a central server, which promotes fault tolerance and makes it difficult to censor content.
InVision	The name of a popular platform for designing and prototyping user interfaces (UI/UX) as well as for team collaboration.
iOS	A mobile operating system developed by Apple Inc., designed for the company's mobile devices.
IP Hash	IP hashing is a load balancing method in which a client's IP address is used as a key to designate a specific server to handle a given request. This ensures that a given user always reaches the same server. Stickiness is a mechanism ensuring that a user is consistently served by the same physical server throughout a session.
Ishikawa diagrams	Analytical diagrams in the form of a 'fishbone', used to identify and group potential causes of a selected problem or phenomenon. The main 'axis' represents the problem, and the 'branches' represent groups of causes (e.g., people, methods, machines, materials, environment, measurements), allowing teams to systematically analyse the sources of irregularities and plan corrective actions within processes.

IT administration	The practical and operational aspect of technology management within an organisation. It involves the ongoing maintenance, configuration, monitoring, and management of IT infrastructure to ensure its stable, secure, and efficient operation.
IT architecture	A set of principles, structures, and technological components (hardware, software, data) defining how IT systems operate and interact within an organisation. Proper IT architecture ensures consistency at all levels and supports the achievement of business objectives. It is a comprehensive system design encompassing its organisation, relationships between elements, environment and development rules, providing a secure, scalable, and effective foundation for technology.
IT management	A comprehensive process of overseeing, administering, and optimising an organisation's information technology resources. IT management covers a range of areas, including: hardware, software, networks, data, and people. IT management aims to support business needs by delivering effective and secure IT services, as well as by taking risk management into account.
Key management service (KMS)	A system for the secure management of encryption keys. Used in the cloud and on-premises to control access to data and meet security and compliance requirements.
Key performance indicators (KPIs)	Metrics measuring the effectiveness of a company or department. KPIs analyse the status and progress of strategic and operational goals. They provide objective data for decision-making and optimising operations.
Kibana	Software for visualising, exploring, and analysing data stored in Elasticsearch clusters. It enables the creation of dashboards, reports, and charts, searching and filtering logs and metrics, as well as defining visual panels for system monitoring and the detection of events and anomalies in operational data.
Kubernetes	A container orchestration system used to run and manage containerised applications in a distributed environment. It automates, among other things, deployment, scaling, load balancing, updates, and service recovery following failures.

Large language model (LLM)	A deep learning model specialising in natural language processing, trained on very large corpora of text. It enables text generation and paraphrasing, answering questions, summarising, translating, content analysis, and other language tasks, utilising a representation of statistical relationships between words and sentences.
Least Connections	A traffic distribution strategy in which a new connection is directed to the server currently having the fewest active connections. It allows for better utilisation of resources than the simple Round Robin approach, particularly when request processing times are uneven or server performance varies.
Lightweight Directory Access Protocol (LDAP)	LDAP enables access to and management of directory services that store information about users, resources, and devices on a network, operating over the TCP/IP protocol. It enables centralised user authentication and authorisation.
Load balancing (LB)	A mechanism for distributing network traffic or application requests across multiple servers, service instances, or links in such a way as to avoid overloading a single node. Load balancing improves system availability, scalability, and performance. When combined with resource health monitoring, it also enables the automatic removal of malfunctioning components from traffic.
Local Area Network (LAN)	A logically separated network connecting devices (computers, servers, printers, switches) within a limited area, e.g., in an office, production hall, or campus. It provides high bandwidth and low latency, is usually managed by a single organisation, and constitutes the basic communication infrastructure within a company or institution.
Low-code	Low code refers to creating applications (work automation) that require a minimal amount of manual coding. Instead of writing lines of code, a graphical interface is used. Low-code acts as a bridge, enabling the creation of advanced applications.

Machine learning (ML)	ML is a branch of artificial intelligence (AI) and computer science that focuses on using data and algorithms to mimic the way humans learn, thereby gradually improving the machine's accuracy. It is a vital component of the growing field of data science. Through the application of statistical methods, algorithms are trained to classify, predict, and discover key insights in data-driven projects, allowing systems to make decisions without direct human intervention once the training process is complete.
Machine learning operations (MLOps)	A set of practices, processes, and tools used to manage the full lifecycle of machine learning models—from experiments, data, and model versioning, through deployment to test and production environments, to quality monitoring, retraining, and decommissioning. It combines data engineering, machine learning, and DevOps approaches to ensure repeatability, scalability, and control over model changes in production systems.
Malware	A term referring to computer programs designed to cause harm to the user, steal their data, damage devices, or take control of them. This includes, among others, viruses, Trojans, ransomware, and spyware. It operates covertly on computers, phones, or tablets to extract information, display advertisements, or block the system.
Mandatory access control (MAC)	An access control model in which decisions regarding access to resources are enforced by a centrally defined security policy rather than by the resource owner. Permissions are derived from assigned labels or classification levels (e.g., secrecy) for users, processes, and objects, and the user cannot independently change these rules or delegate permissions to other entities.
Mapping	Key-value mapping in smart contracts—a data structure used in smart contract programming languages, representing a 'key-value' mapping. It enables a unique key (e.g., a participant's address, a resource identifier) to be linked to its corresponding value (e.g., a balance, a data structure, a set of permissions) stored in the contract state. Mapping is used for efficient data management in a distributed ledger without the need to iterate through entire collections.

Media Access Control (MAC) address	A fixed, usually 48-bit identifier assigned to a network interface (e.g., an Ethernet card or Wi-Fi module), written as hexadecimal numbers separated by colons or hyphens. It is used to uniquely identify devices on a network at the data link layer. Among others, it is used by network switches to forward frames to the correct port.
Mesh network	A network architecture in which many nodes are interconnected in multiple ways, and traffic can be routed via various paths. In wireless networks, this allows for the automatic bypassing of faulty nodes, extending coverage, and increasing resilience to single-point failures.
Metadata	Information that describes other data, facilitating its interpretation, retrieval, classification, and access control. Metadata may include, among other things, the date of creation, author, format, location, version, confidentiality level, keywords, and links to other resources. It plays a key role in information lifecycle management, auditing, and data security.
Microservices	A type of software architecture involving the construction of applications as a set of small, independent, and loosely coupled services. Each is responsible for a single, specific business function. The services communicate with one another via APIs and can be developed, tested, and deployed independently. This increases the system's flexibility, scalability, and resilience—a failure in one service does not bring the whole system to a standstill.
Microsoft Azure	Microsoft's cloud services platform providing computing resources, storage space, databases, integration services, and solutions for security and identity management. It is often used to run business applications and integrate with Microsoft products (e.g., Windows Server, Active Directory, Office services).
Mobile device management (MDM)	An IT system enabling the remote management, monitoring, and securing of mobile devices used within a company (e.g., smartphones, tablets, laptops). MDM systems allow for the enforcement of security policies, the configuration of applications and networks, as well as the remote locking or wiping of a device in the event of loss or theft.

Mock-up	A term used in graphic and web design, referring to a realistic model or visual representation of a product, website, application, or user interface. Mock-ups are useful in the development process and allow the final result to be visualised before it is actually implemented. They make it easier to identify and correct any errors and to better understand how a given project will look and function in reality.
Monetisation	The process of transforming a product, service, or resource (e.g., an application, platform, data, web traffic) into a source of revenue. Monetisation involves selecting and implementing a revenue model (e.g., subscription fees, resource usage fees, data sales, advertising, or premium features) and measuring the business impact of these activities.
Monolith	A traditional software architecture in which all functions are integrated into a single, undivided unit operating within a single database. It is easy to implement and manage, but difficult to scale and modify, as any change requires the whole system to be redeployed. It is the opposite of microservices.
Multi-cloud	A method of using more than one cloud provider within the same organisation, for example, separate systems in different clouds or the distribution of services across multiple providers. It does not automatically imply tight integration between clouds—the key point is that the organisation consciously uses multiple cloud platforms (e.g., for cost, functional or regulatory reasons, or to reduce dependence on a single provider).
Multi-factor authentication (MFA)	A method of enhancing login security that requires at least two different forms of identity verification (e.g., in addition to the password itself) before access to an account, system, or application is granted.
Multimodal models	Artificial intelligence models capable of simultaneously processing and combining data in various forms, for example, text, images, audio, video, or tabular data. They enable the construction of systems that accept multiple data types as input and generate an output in one or more modalities, for example, a verbal description based on an image and textual context.
Network-attached storage (NAS)	A device for storing and sharing data on a network (home or business), functioning like a simple computer with hard drives and access via the network to which it is connected.

Network Configuration Protocol (NETCONF)	A standard protocol used for the remote reading and modification of network device configurations in a structured manner. It utilises data models describing the configuration and status of devices and provides mechanisms for transactional changes, enabling the consistent and automatic management of a larger number of network elements.
Network environment	A term referring to the infrastructure, technology, and resources that enable electronic devices to connect and communicate with one another. This includes both physical hardware (Ethernet, fibre optics, radio waves) and software (programs and protocols) that manage data traffic, security, and network functionality.
Network functions virtualisation (NFV)	An approach in which traditional functions performed by dedicated network devices (e.g., firewalls, routers, load balancers) are run as software on standard servers and virtual machines. This enables flexible scaling, rapid deployment of new network functions, and automation of their lifecycle using virtualisation or cloud platforms.
Network orchestration, including software-defined networking (SDN)	The process of automating and centrally managing complex processes, workflows, domains, and network elements, where traditional, distributed functions (e.g., routing, switching) are separated from the hardware (infrastructure layer) and managed centrally by an intelligent controller (control layer). This enables the programmatic definition of policies and, in particular, dynamic traffic steering, as well as the effective coordination of the network environment via APIs (rather than configuring each device individually).
Network Time Protocol (NTP)	A protocol used for the precise synchronisation of system clocks on devices in IP networks with trusted time sources. It operates hierarchically and typically uses UDP. Consistent time is crucial for, among other things, log accuracy, certificate validity, the operation of cryptographic mechanisms, and security incident analysis.
Neuromorphic computing	An approach to building computing systems in which the hardware architecture and information processing model are inspired by the functioning of the nervous system. Neuromorphic computing utilises specialised circuits as well as event-driven and highly parallel processing models (e.g., spiking neural networks) to achieve high energy efficiency. It is used, among other things, for analysing sensor data streams, pattern recognition, and edge computing in resource-constrained environments.

Next-generation firewall (NGFW)	A firewall that extends traditional traffic filtering to include application-level analysis, user identification, inspection of encrypted traffic, and threat detection based on signatures and behavioural analysis. It enables the enforcement of complex security policies covering not only addresses and ports, but also specific applications, services, and content categories.
No-code	Tools enabling users to generate applications, websites, and process automations using interfaces with 'drag-and-drop' functionality or ready-made components, thereby eliminating the need to write program code manually.
Non-functional requirements (NFR)	Requirements that define the qualitative properties of a system and the constraints on its operation, rather than specific business functions. They describe, among other things, the level of security, availability, reliability, performance, scalability, fault tolerance, regulatory compliance, maintainability, observability, and usability. In practice, NFRs constitute acceptance criteria and design 'boundary conditions' that determine the architecture and implementation of the solution.
Observability	A system property whereby its internal state can be reliably inferred from data generated during operation. In practice, observability relies on the consistent logging and correlation of operational data, such as logs, metrics, and the tracking of request flows between services, to diagnose the causes of problems more quickly and assess the impact of changes.
Occupational Health and Safety (OHS)	A set of rules, procedures, and organisational and technical requirements designed to ensure safe working conditions and reduce the risk of accidents and occupational illnesses. OHS includes, among other things, hazard identification, risk assessment, the use of protective measures, training, workplace instructions, and supervision of compliance with occupational safety regulations and standards.
On-prem (short for on-premises)	A model for maintaining IT systems in which the infrastructure (servers, storage, network) is physically located at the organisation's premises or in its own data centre and is managed directly by it. In contrast with cloud models, the organisation is solely responsible for the purchase, maintenance, scaling, and security of this infrastructure.

Open Refine	Software for interactive data organisation, detecting inconsistencies, cleaning values, transforming fields, and standardising formats in datasets. It enables, among other things, bulk corrections, transformation rules, and the merging of data from various sources to prepare it for analysis, reporting, or migration.
Open Systems Interconnection (OSI)	A standard describing communication in ICT networks, divided into seven layers: physical, data link, network, transport, session, presentation, and application. Each layer has a defined scope of responsibility and standard services, which enables the design, analysis, and comparison of network protocols and network architectures.
OpenDataSoft	A platform for publishing and sharing data (often in the form of an open data portal) with a catalogue, metadata, search, and visualisation tools, as well as an API. Classified as a commercial solution, it supports the sharing of open data, while the platform's licensing model is independent of the licences of the data published on the portal.
OpenFlow	An open protocol for controlling network devices, enabling an external controller to programmatically manage how traffic is switched in switches and routers. It separates the control logic from the actual packet switching, allowing the controller to install, modify, and delete rules in the flow tables of network devices.
OpenShift	An enterprise-class container platform based on Kubernetes, providing ready-made mechanisms for building, deploying, and maintaining applications. It integrates elements of application lifecycle management, security, and access policies, and also facilitates the standardisation of multi-team environments.
Open-source	Software whose source code is publicly available. This allows users to legally use, modify, and distribute it under the terms specified in the licence.
Operational-level agreement (OLA)	An internal document used within an organisation, which may be linked to an SLA (service level agreement) as an agreement between various internal departments within the same organisation that jointly provide a service to a business client.
Operational technology (OT)	A set of devices and systems used to control, monitor, and supervise production processes and physical infrastructure. It includes hardware and software solutions operating directly in the technological process.

Orchestration	The coordinated control of multiple tools, systems, and processes from a single, central location in such a way that they form a coherent workflow. It involves integrating various systems, transferring data and results between them, and triggering the appropriate actions in a specific order, often as a basis for automation. In the field of security, this involves, among other things, integrating monitoring platforms, threat analysis, and incident response systems into a single environment capable of a rapid, coordinated response.
Organisational unit (OU)	An organisational unit in IT (particularly in Microsoft Active Directory) used to group objects (users, computers).
Penetration tests (pentests)	IT system security tests designed to detect vulnerabilities (weaknesses) in the system by attempting to replicate actions that might occur during a cyberattack. The tests may be conducted manually by a tester or in a partially automated manner using ready-made exploits, that is, scripts containing examples of computer system vulnerabilities. The aim of penetration tests is not only to identify vulnerabilities, but also to attempt to exploit them as a means of 'breaking into' the system. Penetration tests include activities in the form of physical and social engineering security tests.
Phishing	A common method of online fraud using social engineering, involving the impersonation of trusted institutions to obtain confidential data (e.g., usernames, passwords, payment card numbers, personal details). Cybercriminals send fake emails, text messages, or messages containing links to fake websites designed to trick the victim into entering their details or infecting their computer with malware.
Platform	A term referring to a system, environment, or infrastructure that enables the operation of applications, services, and digital interactions. It acts as a base (foundation) that enables interaction between different users and systems.
Platform as a Service (PaaS)	One of the computing service models in which the provider makes a programming or development platform available.

Policy-based access control (PBAC)	An access control model in which the decision to grant or deny access is made on the basis of a set of policies (rules) describing the conditions for access. Policies may take into account the context of the request, for example, the user's identity and role, the type of resource, the operation being performed, the time, location, risk level, and device status. PBAC enables the centralised definition and enforcement of access rules across multiple systems without the need to manually assign permissions to each resource.
Post-quantum cryptography (PQC)	A set of cryptographic algorithms designed to remain secure even in the face of quantum computers capable of breaking some of the public-key cryptography schemes currently in use. PQC includes, among other things, key agreement and digital signature mechanisms based on computational problems considered resistant to known quantum algorithms. PQC is used to plan cryptographic migration in systems with a long-term data protection horizon.
Power over Ethernet (PoE)	A technique enabling the simultaneous transmission of data and electrical power over the same Ethernet cable. It allows devices such as access points or IP cameras to be powered without separate power supplies, simplifying cabling, and enabling centralised power supply and emergency backup for these devices.
PowerShell	A system shell and scripting language from Microsoft, available on Windows, Linux, and macOS. It combines an interactive command-line environment with an object-oriented scripting language, enabling advanced automation of system administration, directory services, cloud platforms, and applications. It operates on objects (rather than text itself), which facilitates filtering, combining, and processing command results in complex administrative scenarios.
Pre-production environment	A key stage in the software development lifecycle, which is virtually identical to the production (prod) environment. Its purpose is to test the latest versions of applications and updates in conditions as close as possible to real-world scenarios, but without the risk of affecting live production. It does so by using anonymised or synthetic data, yet with real credentials, to catch any potential errors before production deployment.

PRINCE2 Agile	An extension of the PRINCE2 methodology, combining classic, process-based project management with Agile practices. It defines how to maintain the structure of roles, management products, and PRINCE2 stages, while delivering the scope in iterations, using a backlog, incremental delivery, and Agile planning by the delivery teams.
Privacy by default	A principle whereby the default settings of a system or service ensure a high level of privacy protection without the need for additional configuration by the user. This means, among other things, collecting only necessary data, disabling unnecessary tracking and profiling functions, as well as sharing personal data with other entities only when the user gives their explicit, informed consent.
Privacy by design	An approach to the design of systems, processes, and services in which requirements regarding the protection of personal data and privacy are taken into account from the earliest stages of a solution's lifecycle (analysis, design, implementation, maintenance). This includes, among other things, data minimisation, access restriction, pseudonymisation, encryption, and designing the architecture in such a way that privacy risks are identified, assessed, and mitigated at the concept stage, rather than only after implementation.
Private cloud	A cloud service model designed exclusively for a single organisation, providing it with full control over the infrastructure, high data isolation, and greater security compared to the public cloud. A private cloud can be hosted in an on-premises data centre or by an external provider.
Privileged access management (PAM)	Privileged access management uses a combination of IT solutions and technologies to secure, control, and monitor access to an organisation's critical information and resources. It protects the organisation against cyber threats, minimises the risk of abuse, and ensures compliance with internal policies and legislation. PAM technology encompasses a range of tools, such as: password management, privileged session management, control of work devices, and application access management.
Privileged Identity Management (PIM)	A procedure enabling the monitoring of privileged users' activities. It prevents unauthorised users from accessing critical data and limits the potential for abuse arising from broad access rights.

Process control sheets	Structured forms or templates containing lists of questions, criteria, and checkpoints used to assess whether a given process is being performed in accordance with established procedures, quality, and regulatory requirements. Used in audits, reviews, and process monitoring to systematically document inspection results, identify non-conformities and areas for improvement.
Process diagrams	Graphical models depicting the flow of a business or technical process: the sequence of activities, decisions, inputs/outputs, roles, and the flow of information or materials. Used for the analysis, design, and optimisation of processes, often based on an established notation (e.g., business process modelling notation), which facilitates communication between business and IT.
Production environment	The actual, final environment in which the deployed software is made available to end users for performing business tasks. It differs from development (dev) or test environments and is characterised by the highest priority being placed on stability, security, performance, and availability.
Projects in Controlled Environments 2 (PRINCE2 method)	A project management methodology based on defined roles, deliverables (outputs), stages, and project control principles. It focuses on business justification, risk management, the allocation of responsibility and progress monitoring through formal decision points in the project lifecycle.
Project tagging	The process of assigning labels, keywords, or metadata to project elements in order to organise, categorise, and facilitate their search and management. It involves adding descriptive tags to digital assets, enabling quick filtering and retrieval of related information within a project management platform.
Prometheus	An open-source metrics monitoring and alerting system, this software collects and stores time-series metrics and generates alerts based on rules. In practice, it is used to monitor services and infrastructure by periodically retrieving metrics from endpoints and analysing how they change over time.

Provisioning	The process of preparing, configuring, and providing IT resources (e.g., user accounts, virtual machines, databases, network services, or licences) in accordance with a specified template or policy. It encompasses both the creation of the object (e.g., an account or instance) and the assignment of appropriate technical parameters and permissions, often performed automatically within identity management systems or cloud platforms.
Public cloud	A cloud service model in which an external provider makes resources available via the internet to multiple customers using a shared infrastructure. The main feature of this solution is that the infrastructure is managed and maintained by the provider, and the user pays only for the resources consumed, which can be scaled flexibly.
Public key infrastructure (PKI)	A set of technical, organisational, and procedural mechanisms used to generate, distribute, store, and revoke cryptographic keys and certificates. It enables the use of public-key cryptography for authentication, encryption, and digital signatures in a trusted manner, based on a hierarchy of certification authorities.
Puppet	A configuration management and automation system, typically operating in a server–client model. It enables the description of the desired state of systems (e.g., packages, services, configuration files) and then enforces this state across multiple servers, reducing the number of manual changes and the risk of configuration discrepancies.
Quality of Service (QoS)	A set of mechanisms within the network infrastructure that allows control over how traffic is handled, for example, by prioritising selected types of transmission, reserving bandwidth, limiting delays and jitter, and controlling packet loss rates. In practice, QoS is used to ensure the predictable performance of delay-sensitive services (e.g., voice, video, control systems) when sharing the same network with other types of traffic.
Quantum computer emulator	Software running on classical computing systems that simulates the operation of a quantum computer at the level of circuit logic and quantum states. It enables the testing, debugging, and comparison of quantum algorithms without access to a physical quantum computer, at the cost of significantly higher computational requirements as the number of qubits increases.

Rancher	A platform for the centralised management of Kubernetes clusters (often multiple clusters across different environments). Rancher provides unified management of configuration, access control, policies, and observability, simplifying operations in multi-cluster environments.
Real-time operating system (RTOS)	An operating system designed to execute tasks with guaranteed time constraints, so that responses to events occur within a predictable timeframe. RTOS provides deterministic task scheduling (priorities, interrupts), delay control, and mechanisms for synchronisation and communication between tasks. This is essential in embedded systems, automation, and mission-critical solutions, where exceeding the response time is treated as a failure.
Real-time system	An IT system in which correct operation depends not only on the result of calculations, but also on responding to events within a specified time. A real-time system ensures predictable delays and the timely execution of control or data-processing tasks, which is crucial in areas such as automation, embedded systems, and mission-critical solutions.
Red Hat Enterprise Linux (RedHat)	A commercial Linux distribution developed by Red Hat for server and enterprise applications. It offers a long support lifecycle, certifications for business environments, and an ecosystem of tools for infrastructure management and technical support.
Redundant Array of Independent Disks (RAID)	A storage organisation and virtualisation technology that combines multiple physical storage components into one or more logical units to provide data redundancy and improve performance. It is a method of utilising two or more hard drives within a computer system that work together. This achieves a range of capabilities that would be unattainable using either a single drive or several drives connected as separate units.
Regulatory sandboxes for AI	A controlled testing environment in which organisations can design, train, validate, and pilot artificial intelligence systems under the supervision of regulatory bodies or within established compliance frameworks. The aim is to safely test the system's operation under conditions similar to real-world scenarios, including risk assessment (e.g., for privacy, security, and equal treatment), verification of legal and organisational requirements, as well as the refinement of documentation and control mechanisms prior to production deployment.

Remote Authentication Dial-In User Service (RADIUS)	A network protocol used for the centralised management of user authentication, granting permissions, and logging the use of network services. It typically works with access devices (e.g., switches, access points, VPN concentrators), which forward login requests to the RADIUS server and then enforce decisions to grant or deny access.
Remote Desktop Protocol (RDP)	A Microsoft communication protocol enabling remote, interactive use of an operating system desktop over a network. It allows the transmission of video, audio, keyboard, and mouse data between a client and a server, enabling an administrator or user to work on a remote machine as if it were local, while maintaining authentication and encryption mechanisms.
Representational State Transfer (REST)	A style of network service design architecture in which applications make resources available via a uniform interface, usually based on the HTTP protocol. Communication is based on simple operations on resources (e.g., read, modify, delete), and the server does not maintain the client's session state, which simplifies scaling and the integration of different systems.
Representational State Transfer Configuration (RESTCONF)	RESTCONF enables access to data defined in YANG via a REST API. It is a stateless protocol using HTTPS to transmit configurations, states, and RPC procedures. It is used for simple configuration changes executed sequentially one after the other for querying status and collecting statistical data.
REST API	REST API uses standard HTTP requests for communication between systems, treating data as resources that can be managed using methods such as GET, POST, PUT, and DELETE, usually exchanging data in JSON (JavaScript Object Notation) format.
Retrieval-augmented generation (RAG)	An architecture for systems based on large language models, in which, before generating a response, the model searches for relevant information fragments in an external knowledge base (e.g., organisational documents) and then uses them as context to generate the result. The aim of RAG is to increase the accuracy and timeliness of responses and to limit the generation of content not supported by data, while maintaining control over the source of information used in the response.

Return on Investment (ROI)	A metric describing the relationship between the profit generated from an investment and the expenditure incurred, usually expressed as a percentage. In the field of IT and digital projects, it is used to assess the profitability of initiatives, compare solution options, and provide business justification for expenditures on infrastructure, software, and services.
Robotic process automation (RPA)	Technology for automating repetitive tasks performed within applications using 'software robots' that mimic user actions (e.g., reading and entering data, filling in forms, generating documents, and executing steps across multiple systems). RPA operates at the level of application interfaces and process rules, thereby enabling automation without the need for extensive system re-engineering, while maintaining access control, activity logging, and operational oversight policies.
Role-Based Access Control (RBAC)	An access control model in which system permissions are assigned to roles, and a user gains access by being assigned one or more roles. Roles reflect organisational functions and responsibilities, which simplifies permission management, supports the principle of least privilege, facilitates auditing, and maintains consistency in access policies.
Round Robin	A method of distributing tasks or network traffic in which successive requests are directed in turn to each server in a pool, in a fixed, cyclical order. It ensures a simple, even load distribution, but does not take into account the current status or performance of individual servers.
Saga	A sequence of local transactions in which each service performs an operation and initiates the next step via events or messages. If a step in the sequence fails, the saga performs rollback transactions to undo the completed steps. This approach helps maintain data consistency.
Scrum	A teamwork framework belonging to the Agile family of approaches, defining roles (e.g., product owner, development team, process owner), artefacts (e.g., product backlog, sprint backlog), and events (e.g., sprint, sprint planning, review, retrospective). Scrum organises work into fixed iterations (sprints), in which the team delivers a potentially usable increment of the product, maintaining transparency of progress, and regularly adapting the way they work.

Secrets management	The process of securely storing, distributing, rotating, and revoking confidential information (passwords, API keys, certificates), which is crucial in DevOps and IT to protect critical resources from unauthorised access. It uses specialised tools (e.g., Vault, AWS Secrets Manager) to dynamically provide temporary credentials rather than storing them in code or configuration files.
Secure Access Service Edge (SASE)	An architecture that combines networking and security functions into a single service delivered from the cloud, as close as possible to the user or device. It enables secure, controlled access to applications and data (in the cloud and in data centres) regardless of the user's location, simplifying infrastructure, and centralising the enforcement of security policies.
Security Operations Centre (SOC)	A specialised organisational unit combining a team, processes, and tools, which is responsible for the continuous monitoring of the IT/OT environment, the collection and correlation of security events, the detection of anomalies, the prioritisation of reports (triage), and incident handling. The SOC implements and develops detection rules, collaborates with response teams, maintains the visibility of the organisation's security status, and supports real-time decision-making.
Secure shell (SSH)	An encrypted network protocol used for remote login to systems, executing commands, and secure file transfer. It ensures data confidentiality and integrity through encrypted communication and enables strong authentication (e.g., cryptographic keys instead of passwords).
Sensors	Measuring devices or modules that record physical or environmental quantities (e.g., temperature, pressure, motion, position, light intensity) and convert them into digital signals used by IT systems. In the context of IT/OT and IoT, sensors are a source of data for monitoring, automation, analytics, and autonomous systems. Their parameters (accuracy, sampling rate, calibration) directly affect the quality of the data obtained.
Serverless architecture	Serverless architecture is a cloud computing model where developers write application code, while the cloud provider handles the server infrastructure, automatic scaling, and management. The customer pays only for the actual use of the functions.

Service Function Chaining (SFC)	A mechanism for constructing a logical path through which network traffic passes via successive service functions, such as: a firewall, an intrusion detection system, a WAN optimiser, a load balancer, or a proxy. Instead of rigid routing through physical devices, the function chain is defined programmatically and can dynamically direct traffic through selected functions in a specific order.
Service level agreement (SLA)	A formal document that specifies the guaranteed level of availability, performance, and quality of IT services provided by the supplier to the client (response time, time to resolve an issue, obligations of both parties, corrective procedures, contractual penalties, etc.)
Service mesh	An infrastructure layer in service-based architectures (e.g., microservices) that takes responsibility for communication between services. It provides functions such as: routing and load balancing between instances, connection encryption, observability (metrics, logs, query tracing), and enforcement of security policies—without the need to implement this in the code of each service.
Service set identifier (SSID)	The name given to a Wi-Fi network, displayed to the user when selecting a network to connect to. The SSID is used to logically distinguish between multiple networks operating within the same radio frequency range. A single device may broadcast several different SSIDs to separate, different groups of users or services (e.g., a corporate network and a guest network).
Shadow IT	The use of unauthorised IT tools, systems, applications, devices, or services by an organisation.
Sharding	A technique for scaling data storage or processing systems that involves dividing a dataset into independent logical fragments (shards), distributed across multiple nodes or instances. Each fragment handles only a portion of the data and queries, which reduces the load on a single node and enables the horizontal scaling of databases or distributed ledgers.
Showback/ chargeback	Cost accounting systems in the IT and cloud sectors. Showback involves reporting costs to teams to raise awareness of their usage, while chargeback involves charging departments for resources consumed, thereby enforcing accountability and efficiency.

Simple Network Management Protocol (SNMP)	A protocol used for monitoring and remotely managing network devices such as switches, routers, firewalls, servers, and network printers. It enables the reading of operational parameters, the receipt of SNMP notifications, and the implementation of selected configuration changes from monitoring systems.
Simple Object Access Protocol (SOAP)	An XML-based communication protocol enabling the exchange of structured information in a decentralised and distributed environment.
Single sign-on (SSO)	An authentication mechanism that allows access to multiple applications or systems via a single login.
Sketch	A vector graphics editor, designed primarily for designing user interfaces (UI/UX) for mobile applications and websites.
Smart contracts	Programs running on a distributed ledger infrastructure (e.g., blockchain) that automatically enforce the rules defined within them once specific conditions are met. A smart contract combines business logic with state storage in the ledger, and the execution of its code leads, for example, to the transfer of digital assets, data updates, or the invocation of other functions in a deterministic manner recorded on the blockchain.
Snapshot	A record of the state of a system, virtual machine, disk volume, or database at a specific point in time. A snapshot allows the system to be quickly restored to that state (e.g., prior to an update or configuration change), without a full restoration from a backup.
Social engineering tests	A process of simulating hacker attacks to test the resilience of staff and security procedures to psychological manipulation. These involve impersonating trusted individuals or institutions or exploiting physical vulnerabilities (e.g., a left-behind USB stick) to extract confidential data, passwords or gain unauthorised access. The main aim of the tests is to identify security vulnerabilities arising from human error and to raise awareness among employees, who are often the weakest link in the data security process.
Socrata	A platform for publishing and sharing data (often public) in the form of data catalogues and APIs, used by organisations to increase the accessibility, utilisation, and publication of open data.
Software as a Service (SaaS)	One of the cloud computing service models, in which the service provider hosts the client's software.

Software Asset Management (SAM)	The infrastructure and processes necessary for the efficient management, control, and protection of an organisation's software assets throughout all stages of their lifecycle (from purchase to software retirement). SAM is part of the broader field of IT Asset Management (ITAM), but it focuses solely on software.
Software Carbon Intensity (SCI)	An indicator describing the volume of greenhouse gas emissions attributed to software operation in relation to a defined functional unit (e.g., transaction, request, user, hour of operation). SCI takes into account emissions resulting from the energy consumed by computing resources, storage, and data transmission, as well as the carbon intensity of electricity in a given runtime environment, thereby supporting the comparison of architectural variants and optimisation in terms of the carbon footprint.
Software-defined storage (SDS)	A resource that separates storage management software from physical hardware. It enables the virtualisation and centralised management of storage resources (e.g., from different vendors) as a single pool. This provides greater flexibility, scalability, and performance due to independence from specific hardware.
Software Licence Management (SLM)	The process of managing, controlling, and optimising software licences within an organisation throughout their entire lifecycle. It ensures legal compliance and cost optimisation by identifying unused software and minimises operational risk.
Software updates	The process of introducing updates, patches, or upgrades to an existing program, operating system, or application. The aim is to fix bugs, enhance security, improve performance, or add new features. A lack of regular updates makes software vulnerable to hacking attacks and renders it non-functional.
Spine-leaf	A data centre network topology in which spine switches connect in a full or near-full mesh with leaf switches. Each access switch has connections to multiple spine switches, ensuring a predictable number of hops, high horizontal bandwidth, and easy scalability by adding further leaf and spine switches.
Storage classes	Predefined categories of data in the cloud or IT systems that determine how data is stored, what the storage and access costs are, and how quickly it can be accessed. Storage classes enable optimisation in terms of performance and cost.

Structure	A composite data type used in programming languages (including smart contract languages) to group several related fields into a single logical unit. The structure defines a set of named attributes (e.g., identifier, owner, balance) that are stored and processed as a single object, which facilitates the modelling of more complex entities in the code and in the contract state.
Supplier certification	The process by which an independent external body confirms that a particular supplier meets specific norms, standards (e.g., quality, safety), or legal requirements. This gives buyers confidence in the supplier's reliability and competence, and in the fact that they operate in accordance with the law, while simplifying the verification and selection of business partners.
Synthetic media	Text, graphic, audio, or video content that has been created or significantly transformed automatically by generative algorithms, rather than merely recorded from the real world. This includes, among other things, generated images, voice recordings, avatars, and videos, which result in additional requirements regarding content attribution, authenticity verification, and protection against disinformation.
System Center Configuration Manager (SCCM)	Microsoft software for the centralised management of computers and servers within an organisation. It is used, among other things, for hardware and software inventory, remote installation of systems and applications, distribution of updates, and enforcement of selected configuration policies.
System logging protocol (syslog)	A protocol and message format used to transmit logs from systems, applications, and network devices to a server that collects logs. It enables the centralised collection, filtering, and analysis of events (e.g., errors, warnings, logins) from multiple sources, which forms the basis for monitoring and building incident detection systems.
System on a chip (SoC)	An integrated circuit that combines key components of a computer system, such as the processing unit, memory controllers, input/output interfaces, and communication modules, onto a single chip. SoC is used in embedded and mobile devices, where space, power consumption, and cost constraints are critical, and a high level of integration simplifies hardware design and enables the construction of compact systems.

TeamViewer	Software for remote access, remote control, and remote technical support. It enables the establishment of a secure, encrypted connection between two computers or mobile devices over the Internet.
Technical debt	A term from the field of software engineering that serves as a metaphor describing the negative consequences of making short-term, less effective decisions in IT (e.g., cutting corners on testing). Such decisions generate additional costs and work in the future, and hinder development (analogous to financial debt, which requires interest payments).
Technology and critical systems architecture	A strategic plan and framework describing the interaction of systems, data, hardware, software, and processes within an organisation, taking into account the critical systems essential to the organisation's operations. It is essential for stable operations as well as for managing the complexity and scalability of IT systems.
Technology principles	A set of fundamental, enduring principles and guidelines used in all decision-making processes concerning the architecture, technology, development, and management of IT systems (within an organisation). They define the fundamental relationship between business strategy and IT architecture, ensuring technological consistency and cross-functional efficiency in the achievement of business objectives.
Technology stack	A set of technologies used to build and maintain an IT solution, which includes: programming languages, frameworks, libraries, database systems, integration tools, front-end and back-end components, infrastructure elements, and cloud services. A description of the technology stack shows the technical components on which a given system or the entire architecture is based.
Terraform	An 'infrastructure as code' tool used for the declarative description, automatic creation, and modification of infrastructure (cloud and on-premises). It allows resources to be defined in configuration files and their state to be maintained in a versioned manner, so that the recreation and modification of environments are repeatable and controlled.
Test environment	An isolated, controlled space simulating production conditions, used to verify that a new version of software works correctly before it is deployed. It typically includes a database, servers, and infrastructure, and ensures the security of the systems.

The Open Group Architecture Framework (TOGAF)	An open standard and comprehensive methodology for the design, planning, implementation, and management of enterprise architecture (EA). It helps organisations align business objectives with IT infrastructure, ensures the standardisation of complex systems management, and supports digital transformation. A key element of TOGAF is the Architecture Development Method (ADM), a sequential process for producing architecture covering four domains: business, applications, data, and technology.
TO-BE	A business process analysis model describing the expected (target) state, free from the shortcomings and limitations described in the initial (AS-IS) state.
Token Ring	A local area network technology based on a logical ring topology, in which the right to transmit data is granted sequentially to each device via a so-called token (a special frame circulating within the network). It ensures deterministic access to the medium (it is easy to predict when a device will be able to transmit). Historically used mainly in corporate networks, today it has been practically replaced by Ethernet.
Total Cost of Ownership (TCO)	The estimated total cost of an IT resource (e.g., a system, application, or infrastructure) calculated over its entire lifecycle, covering not only the purchase price but also the costs of implementation, maintenance, licensing, training, development, support, energy, and decommissioning. TCO is used to compare technical options in terms of their actual long-term cost-effectiveness.
Transmission Control Protocol/ Internet Protocol (TCP/IP)	A set of communication protocols used in the Internet and IP networks. It comprises a layer responsible for addressing and forwarding packets between networks, as well as a layer ensuring the reliable delivery of data streams between applications (connection control, sequencing, and data integrity).
Transport Layer Security/ Secure Sockets Layer (TLS/SSL) termination	A mechanism in which an encrypted connection based on TLS/SSL protocols is terminated on an intermediary device (e.g., a load balancer or proxy server). The device decrypts incoming traffic from the client and then forwards it to application servers in either decrypted or re-encrypted form, simplifying certificate management and reducing the load on servers.

Unauthorised access	Gaining access to systems, data, or IT resources without the permission of the owner or operator. This is a breach of security policy involving, among other things, attempts to log in, access files, or use devices without authorisation.
Unified Modelling Language (UML)	A unified modelling language is used for modelling problems (specifying, constructing, and documenting the functioning of various types of systems). It is a collection of different elements that help to understand the structure and behaviour of a system before, during, and after its construction. UML is usually used together with its graphical representation (its elements are assigned appropriate symbols and modelling relationships). UML is officially defined by the Object Management Group (OMG).
Uninterruptible power supply (UPS)	A device or system designed to provide power in the event of power cuts in the mains supply.
Uptime Institute Tier Standard	A set of criteria for classifying data centres into four tiers (Tier I–IV) based on their resilience to failures and the service availability they provide. Among other things, the standard outlines the requirements for power and cooling redundancy, the ability to perform maintenance work without interruptions, and resilience to single points of failure, thereby enabling the comparison of the reliability of different facilities.
User-centred design (UCD)	An approach in which the needs, requirements, and constraints of the end user are placed at the centre of the entire product or service development process to ensure maximum usability, intuitiveness, and user satisfaction. It involves detailed research into the target user group and engaging them at every stage of the design process.
User flow	A visual representation of the path a user takes within a digital product (website, app) to achieve a specific goal, for example, to make a purchase, register, or find information. It is a key tool in UX design, mapping the user's successive steps, interactions (clicks, data entry) and decisions, and helping to create the most intuitive, seamless, and effective path.
User interface (UI)	In IT, this refers to everything the user sees and interacts with in applications, systems, or on websites: buttons, menus, colours, layouts, icons, etc.

UX	The overall user experience associated with using and interacting with a digital product, encompassing its usability, accessibility, emotional response, and level of satisfaction.
UXPin	An advanced tool (software) for designing user interfaces (UI) and user experiences (UX), enabling the creation of interactive prototypes, website and app mock-ups, and allowing teams to collaborate on products and test them.
Vendor lock-in	A situation in which a customer becomes dependent on the products or services of a single supplier (e.g., software, cloud platform). The consequence of this is a situation where switching to a competitor's solution becomes too difficult, technically complex, or financially unviable. This stems from the use of proprietary technologies, data formats, or long-term contracts that limit flexibility and bargaining power.
Virtual desktop infrastructure (VDI)	Virtualisation technology that allows desktop environments (operating systems and applications) to be hosted on a central server or cluster of servers in a data centre or in the cloud in order to deliver services remotely to end users.
Virtual local area network (VLAN)	The logical separation of several distinct networks within a single physical switch infrastructure. It enables traffic to be segregated (e.g., finance department, guests) without the need to install separate cables or switches. Identification is performed with a VLAN tag in the frame (port or traffic tagging), allowing the administrator to control which devices 'see' each other within the same broadcast domain.
Virtual machine (VM)	An isolated runtime environment in which the operating system and applications run as if on a separate computer, although they share physical hardware with other virtual machines. Virtual machines are created and managed by virtualisation software, which allows for the flexible sharing of hardware resources, as well as the easy migration and restoration of entire environments.
Virtual Network Computing (VNC)	A system enabling remote graphical control of another computer's desktop. Unlike RDP, it is an open and cross-platform protocol.

Virtual Private Network (VPN)	A technology that creates a secure and encrypted connection between a device and a network (e.g., the internet or a company's local area network). It acts as a tunnel that protects data from being viewed, intercepted, or manipulated. Information inside the tunnel is encrypted.
Vulnerability scanners	Automated tools (software) used to identify, analyse, and report security vulnerabilities in networks, systems, and applications. They work by comparing the analysed object against databases of known threats. Scanners help detect outdated software, open ports, and incorrect configurations, thereby protecting against cybercriminals.
Water Scrum Fall	A project organisation model in which the analysis and high-level planning phases are conducted in a waterfall-like manner, implementation occurs iteratively using Scrum, and final testing and deployment take place again in a structure similar to the waterfall approach. The model integrates the work of Agile teams with a traditional organisational environment that uses classic project processes.
Web Content Accessibility Guidelines (WCAG)	An international standard (a set of guidelines published by the World Wide Web Consortium, W3C) defining the principles for creating web content (websites, mobile and web applications, and other digital resources) in a way that is accessible to the widest possible audience, particularly people with disabilities.
Weighted round robin (weighted RR)	A variant of the Round Robin algorithm in which each server is assigned a weight reflecting its processing power or preferred share of traffic handling. A server with a higher weight receives proportionally more requests, enabling more efficient utilisation of a diverse pool of servers.
Wi-Fi Protected Access (WPA)	A family of wireless network security mechanisms that replaced WEP, introducing stronger encryption and dynamic key exchange. WPA allows a shared password or a central authentication server to be used for operations, and is the standard method of securing Wi-Fi networks in organisations and at home.

Windows Server Update Services (WSUS)	A server role in Microsoft Windows Server that enables the centralised download, approval, and distribution of updates for Windows operating systems and selected Microsoft products within corporate network environments. It allows one to control which patches are installed and when they are installed in workstations and servers, reduces network bandwidth usage, and ensures compliance with the organisation's update policy.
Wired equivalent privacy (WEP)	An encryption and authentication mechanism for wireless networks, introduced as the first Wi-Fi security method. It relies on a static key and simple encryption. It is now considered obsolete and extremely insecure due to numerous vulnerabilities and security flaws, which allow the system to be compromised within minutes.
Wireframe	A simplified, schematic sketch of a website or application interface that focuses on structure, the layout of elements (headings, buttons, text fields), and functionality, omitting colours, graphics, and styling. It is used to plan navigation logic and user flow, making it easier to identify problems at an early stage of design.
Yet another next generation (YANG)	YANG is a data modelling language used to formally describe the configuration structure and status of network devices and services. YANG models define which parameters are available, their types, dependencies, and constraints, enabling management tools (e.g., those based on NETCONF or RESTCONF) to consistently read and modify the configurations of many different devices compliant with this model.
Zabbix	Enterprise-class (open-source) software for the real-time monitoring of networks, servers, virtual machines, containers, and cloud services. It is used to collect data (metrics), monitor performance, and generate event notifications. It enables the tracking of the performance and availability of servers, virtual machines, network devices, databases, and applications, generating detailed reports and charts. It uses agents or protocols such as SNMP, IPMI, or JMX to collect information and displays it in the user dashboard.

Zero Trust	A security model based on the principle of not trusting any user, device, or service by default, regardless of whether they are located 'inside' or 'outside' the organisation's network. Access to resources is granted solely on the basis of ongoing verification of identity, context, and device status, with the minimum necessary permissions and strong environmental segmentation.