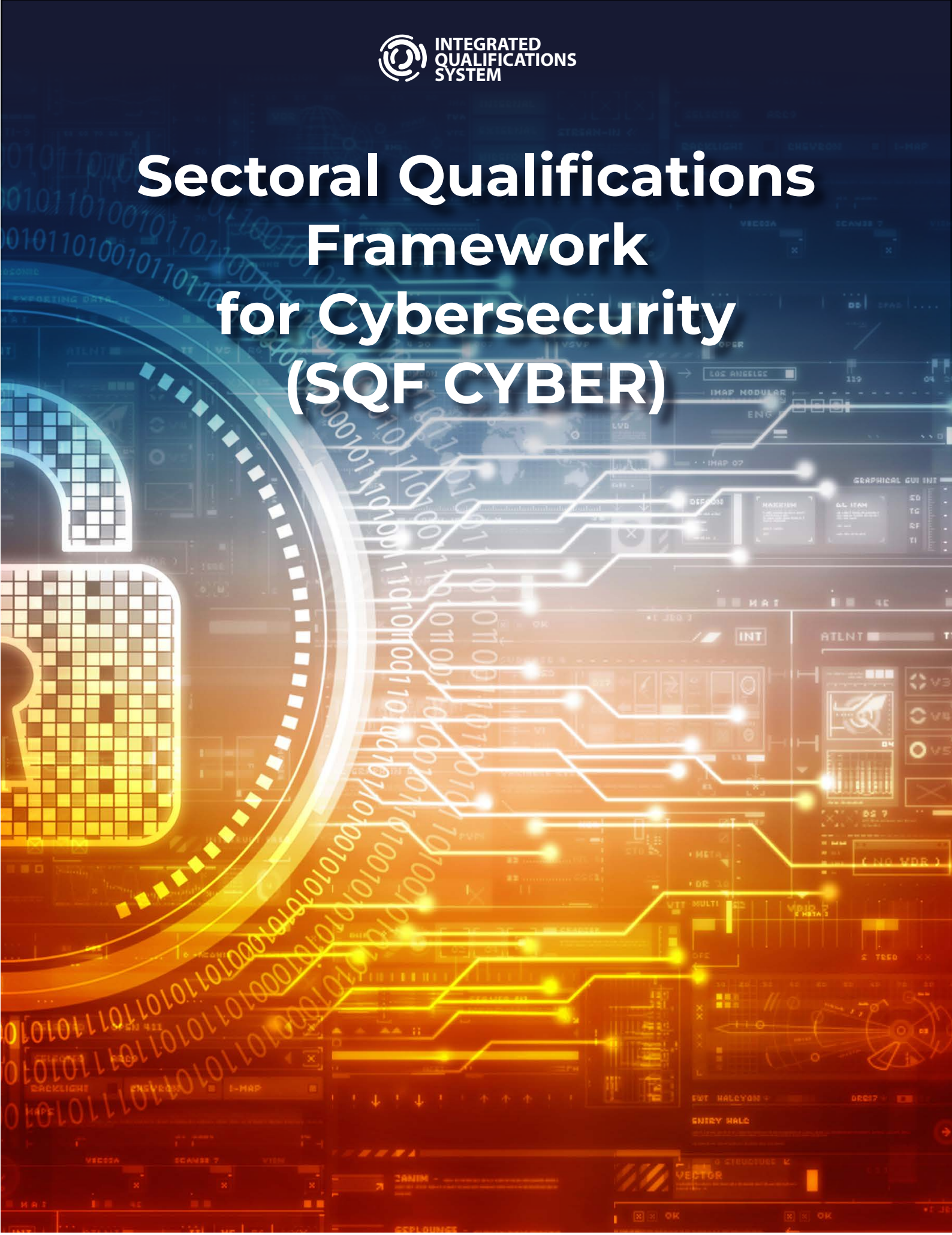
INTEGRATED QUALIFICATIONS SYSTEM

Sectoral Qualifications Framework for Cybersecurity (SQF CYBER)



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

Authors:
Edyta Cieszkowska, Andrzej Cieślak, Monika Drzymulska-Derda, Dr. Dawid Dymkowski, Dr. Przemysław Jatkiewicz, Łukasz Jaworski, Tomasz Klekowski, Dr. Rafał Kołodziejczyk, Beata Ostrowska, Mateusz Panowicz, Damian Parol, Mateusz Przywara, Dariusz Słomkowski, Sławomir Smugowski, Dawid Suder

Language editors: Elżbieta Łanik, Monika Niewielska

Translation: Barbara Przybylska

Cover design and layout: Wojciech Maciejczyk

Cover photo: Shutterstock.com

ISBN: 978-83-67385-68-8

Citation format: Cieszkowska, E., Cieślak, A., Drzymulska-Derda, M., Dymkowski, D., Jatkiewicz, P., Jaworski, Ł., Klekowski, T., Kołodziejczyk, R., Ostrowska, B., Panowicz, M., Parol, D., Przywara, M., Słomkowski, D., Smugowski, S., Suder D. (2023). *Sectoral Qualifications Framework for Cybersecurity* (B. Przybylska, Trans.). Warsaw: Instytut Badań Edukacyjnych (original work published in 2023).

Publisher:
Instytut Badań Edukacyjnych
ul. Górczewska 8
01-180 Warszawa
www.ibe.edu.pl

IBE EDUCATIONAL RESEARCH INSTITUTE

This publication was prepared as part of the systemic project "Supporting IQS functioning and improvement in order to use its solutions in achieving the country's development strategy aims" co-financed by the European Social Fund.

Free copy

Table of Contents

Definition of the sector

The cybersecurity sector includes entities/organisations/persons conducting activities to protect information systems, services, products as well as users and other entities from cyber threats to ensure their uninterrupted functioning.

In defining the terms used above:

Cyber threats are understood to be any potential circumstance, event or activity that could harm, disrupt or otherwise adversely affect systems, services, products or their stakeholders.

Activities to protect systems, services and products are understood to be those performed during the identification, protection, detection, response, recovery and audit phases of the cybersecurity process; these activities are conducted both during the implementation of a system, service or product, its operation, and the decommissioning of that system, service or product.

An **information system** is understood to be a structure that includes technical and organisational components enabling information to be processed.

Instructions for using the Sectoral Qualifications Framework for Cybersecurity

The Sectoral Qualifications Framework for Cybersecurity (SQF CYBER) is a structured set of competences specific to the cybersecurity sector. The competences in SQF CYBER are organised in the following 9 sectoral determinants – the main areas of activity in the sector:

Preliminary cybersecurity requirements
Identification
Protection
Detection
Response
Recovery
Cybersecurity audit as part of security management
Work standards
Communication and cooperation

Since the structure of sectoral qualifications frameworks does not take into account specific business solutions, SQF CYBER is a universal tool for managing industry competences. Among the many functionalities of this tool, one is the ability to search for competences in specific areas and processes of the sector as well as for the specific competences included in SQF CYBER.

Searching for competences in particular areas and processes of the sector

STEP 1:

Review the definition of the sector and determine whether the competence you are looking for falls within its scope.

STEP 2:

Choose the relevant sectoral determinant.

STEP 3:

Sectoral determinants consist of competence series, that is, processes and sub-processes characteristic of the sector. Depending on the type of competence, they are divided into specific categories: knowledge (knows and understands...), skills (is able to...) or social competence (is ready to...).

Choose the appropriate competence series. Remember that often a specific process can only be fully described by combining competence series from the categories of knowledge and skills.

STEP 4:

The sought competences in the selected series describing a specific process (series name) in the sector are arranged by the degree of their complexity (the higher the level, the greater the complexity).

Importantly, SQF CYBER competences at particular levels correspond to second stage Polish Qualifications Framework levels (1–8) for vocational education and training.

Searching for specific competences in SQF CYBER

STEP 1:

Review the definition of the sector and determine whether the competence you are looking for falls within its scope.

STEP 2:

Match the competence being sought to one of the sectoral determinants.

STEP 3:

Depending on the type of competence you are looking for, review the relevant competence categories of the determinant: knowledge (knows and understands…), skills (is able to…) and social competence (is ready to…).

STEP 4:

The sectoral determinants are divided into competence series, that is, sets of thematically-related competences forming a logical series of increasingly complex entries. Match the competence being sought to a competence series in the chosen sectoral determinant.

STEP 5:

Find the competence you are looking for on levels 3 to 8 of SQF CYBER. If you can't find the sought-after competence, it may not be one specific to the cybersecurity sector, but could be: a transversal competence (see the second stage Polish Qualifications Framework typical for vocational education and training), a competence in a related sector (e.g., SQF for Information Technology or Telecommunications), or it may be in another entry of the framework (then repeat steps 1–4).

STEP 6:

If needed, provide further details to the description of the competence you found.

STEP 7:

Write down the code next to the competence you found. This will make it easier to find it again. For example, the code L3SCB_SII5(2) indicates the competence „(is able to) identify critical processes" found in the „Identification" sectoral determinant, and in the competence series „Identify the organisation's processing assets" of SQF CYBER. The individual elements of the code are:

- L3 – a level 3 competence,
- SCB – abbreviation of the Sectoral Qualifications Framework for Cybersecurity,
- S – competence in the skills category, similarly, the letter K stands for knowledge and SC for social competence,
- II – the Roman numeral indicates the second sectoral determinant of the framework,
- 5 – the Arabic numeral indicates the fifth competence series in the skills category of the given determinant,
- (2) – an ordinal number in parentheses is added when several competences are listed in a given SQF CYBER entry.

One of the elements of SQF CYBER is a glossary of terms used in the framework to explain ambiguous or specialised terms. It can be found on **page 43**.

Ways of using the Sectoral Qualifications Framework for Cybersecurity in practice

The Sectoral Qualifications Framework for Cybersecurity is a universal tool for managing the competences in the cybersecurity sector. Due to the fact that the construction of SQF CYBER does not impose specific business solutions, it can be used in any a number of ways by many different users.

Employers

With the help of SQF CYBER, employers can take a broader look at the industry competences present in their business environment, and thus manage human resources more efficiently as well as compete more effectively in the labour market. The biggest advantages of using this tool include support in the process of analysing competence gaps in the industry or company, planning the development of human resources 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 criteria for recruiting employees based on key competences in the industry, as well as to prepare job descriptions.

HR employee of a large company

> After identifying the main competence gaps in the industry, we launched an apprenticeship programme with the task of preparing our students to effectively enter the labour market right after graduation.

Vocational school director

Schools and educational institutions

Based on SQF CYBER, schools and educational institutions can adapt implemented curricula to the current and real labour market needs. This means that the table of competences supports these entities in expanding and modifying the implemented curricula and responding to the competence gaps of students, for example, concerning practical or soft skills. In addition, it can be useful in career counselling for students or in monitoring the success of school graduates.

Higher education institutions

SQF CYBER is a tool that supports higher education institutions in matching study programmes to the current trends in industry development. As a result, students can be better prepared to enter the labour market and achieve career success. The tables of competences also make it possible to monitor students' progress and assess the effectiveness of the programmes in various fields of study.

Rector of a higher education institution

Training companies

Training companies using SQF CYBER can effectively design specialised training courses, enabling them to prepare a tailor-made offer to meet the needs of a specific industry and the expectations of their customers. 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. The gradation of the complexity of competences in SQF CYBER also makes it easier for them to prepare training offers at various levels of proficiency.

Owner of a training firm

IQS stakeholders

Among the broad audience of IQS users, the groups most likely to benefit from the developed SQF CYBER are industry organisations and those describing market or sectoral qualifications. Industry organisations are tasked with, among other things, establishing education agreements that strengthen cooperation between schools and employers as well as providing information on the demand for sectoral competences to educational and/or labour market institutions. In turn, persons describing market qualifications and sectoral qualifications can use the prepared material to more easily define sets of learning outcomes.

Other entities

SQF CYBER can be used for many other purposes depending on the current needs of the industry. In the case of the cybersecurity sector, it can be a supplementary tool for preparing materials to assess the knowledge of a given company's employees regarding threats on the Internet, as today every employee is vulnerable to attack in cyberspace. Verifying basic cybersecurity competences can protect a company from negative consequences in the future. Moreover, the cybersecurity sector is currently facing a shortage of workers. The Sectoral Qualifications Framework for Cybersecurity can serve to retrain and launch the careers of people from closely related sectors, such as IT.

IT team manager

The Sectoral Qualifications Framework for Cybersecurity

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Preliminary cybersecurity requirements	Data	L3SCB_KI1	the types of data sources and their impact on the system the ways of generating data and objects the principles for data extraction and acquisition the reasons and principles for data protection basic security attributes	L4SCB_KI1	data exchange principles and protocols the principles for linking data to the boundaries of processes within or between objects the possibilities of the tools used for data processing the methods of protecting data against damage and leakage the external conditions for data transfer	L5SCB_KI1	the principles of the data model in information systems database creation and modification tools	L6SCB_KI1	the IACS Reference Model				
		Communication systems			L4SCB_KI2	the principles of analogue communication the principles of digital communication	L5SCB_KI2	communication system composition and decomposition methods	L6SCB_KI2	the relationships between communication system components				
		Communication architecture			L4SCB_KI3	the architecture and structure of ICT networks, including the ISO/OSI reference model	L5SCB_KI3	the principles of operating and managing ICT networks	L6SCB_KI3	the principles of compatibility in data communication networks				
		Types of digital environments	L3SCB_KI4	the types of digital environments and complex systems components comprising the IT domain	L4SCB_KI4	the methods of data transmission among devices operating in a digital environment	L5SCB_KI4	the premises of different types of digital environments	L6SCB_KI4	the methods of transferring data between different independent digital environments				
		Systems of electronic devices	L3SCB_KI5	the elements comprising the IT domain the elements comprising the OT domain the elements comprising the IoT domain	L4SCB_KI5	the specific conditions of the IT domain the specific conditions of the OT domain the specific conditions of the IoT domain	L5SCB_KI5	the relationships between IT, OT and IoT						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Preliminary cybersecurity requirements	Operating system architecture			L4SCB_KI6	operating systems and network operating systems architecture the principles of starting up an operating system, including the network	L5SCB_KI6	operating system virtualization methods	L6SCB_KI6	application containerization methods	L7SCB_KI6	container orchestration methods		
		Scripts and applications	L3SCB_KI7	the methods of running individual scripts on selected operating systems at least one scripting language	L4SCB_KI7	object-oriented programming fundamentals the methods of starting up software based on various scripting languages in a single runtime environment	L5SCB_KI7	the possibilities of using ready-made libraries in a project the software environment of the application, including the possibility of integration with external tools	L6SCB_KI7	design patterns web application development methods mobile application development methods desktop application development methods the principles of maintaining the operational continuity of applications	L7SCB_KI7	the methods of developing innovative software libraries		
		Tools using artificial intelligence in cybersecurity systems	L3SCB_KI8	the methods relating to the use of artificial intelligence	L4SCB_KI8	the characteristics of artificial intelligence systems, their principles of operation and limitations	L5SCB_KI8	the groups of applications of artificial intelligence in the organisation the groups of applications of artificial intelligence in cybersecurity the formal requirements for artificial intelligence systems						
		National, EU and international laws, norms and standards	L3SCB_KI9	the basic principles of organising a cybersecurity system	L4SCB_KI9	the principles, procedures and requirements relating to organisational security the obligation to report critical infrastructure incidents	L5SCB_KI9	legal regulations defining cybersecurity requirements national cybersecurity standards good practices in cybersecurity	L6SCB_KI9	international cybersecurity norms and standards international internal audit standards international standards of professional ethics for auditors	L7SCB_KI9	the principles and procedures of industrial property and copyright protection		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Preliminary cybersecurity requirements	Personal data protection	L3SCB_KI10	the basic issues relating to data protection	L4SCB_KI10	the principles, procedures and requirements relating to personal data protection the obligation to report personal data security incidents	L5SCB_KI10	the legal provisions of personal data protection						
		Building awareness about cybersecurity	L3SCB_KI11	the basic terms relating to cybersecurity the principles of applying cybersecurity in a given job	L4SCB_KI11	the principles of cybersecurity for organisations and society	L5SCB_KI11	the methods and techniques for ensuring the security of infrastructure and services the certification system in the cybersecurity sector the role of national cybersecurity organisations	L6SCB_KI11	the role of cybersecurity organisations at the international level	L7SCB_KI11	trends in cybersecurity		
is able to:														
SKILLS	Preliminary cybersecurity requirements	Developing contract specifications	L3SCB_SI1	conduct market research on the desired features and parameters	L4SCB_SI1	define the parameters and functionalities for contract specifications	L5SCB_SI1	define the conditions for product and service delivery	L6SCB_SI1	foresee the risks that may occur during contract execution				
		Monitoring, control, reporting, visualization, response (SOC) systems	L3SCB_SI2	verify situations against false positives (SOC 1)	L4SCB_SI2	support the operational continuity of the managed object in the event of an anomaly (SOC 1)	L5SCB_SI2	analyse data sources, protocols, processing rules of objects and systems (SOC 2) use tools to analyse operational stability, systems integrity, event correlation, data correlation (SOC 2)	L6SCB_SI2	develop in-depth data analytics and data inter-relationships (SOC 2) build security system extension components (SOC 2)	L7SCB_SI2	develop system solutions to counter anomalies and their consequences (SOC 3)		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Preliminary cybersecurity requirements	Data processing	L3SCB_SI3	determine the origin and destination of data select appropriate data sources depending on the system select and organise data visualise data	L4SCB_SI3	process data in unified systems parse data	L5SCB_SI3	monitor distributed, unmanaged data processing scripts verify data transfer conditions for their security	L6SCB_SI3	develop simple programs to solve data processing problems implement data from multiple locations	L7SCB_SI3	process data in a distributed environment		
		Data correlation	L3SCB_SI4	compare a sample of information with a specific signature build information based on acquired data	L4SCB_SI4	perform data correlation using available software	L5SCB_SI4	write a correlator in a chosen programming language	L6SCB_SI4	develop information and possible scenarios on a specific object using a correlation	L7SCB_SI4	design an environment model on the basis of the processed data		
		Communication and data exchange	L3SCB_SI5	find information on communication and data exchange identify the components in the data exchange between objects use applications for communication and data exchange	L4SCB_SI5	define data transmission limits classify a set of data in accordance with specified criteria	L5SCB_SI5	analyse communication and data exchange information manage the communication infrastructure	L6SCB_SI5	design communication infrastructure	L7SCB_SI5	design data exchange standards		
		Industry-specific terminology in Polish and English					L5SCB_SI6	communicate as a team in English use specialised vocabulary in communication in Polish use specialised literature in Polish use specialised systems documentation in Polish	L6SCB_SI6	use specialised vocabulary when communicating in English use specialised literature in English	L7SCB_SI6	communicate in the international business community	L8SCB_SI6	communicate in the international scientific community
		Test, development and production environment			L4SCB_SI7	conduct tests in a test or development environment	L5SCB_SI7	design tests in a test or development environment conduct tests in a production environment with the possibility of stopping test objects	L6SCB_SI7	conduct tests in a continuous production operating environment	L7SCB_SI7	design tests in a production environment		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
								is able to:						
SKILLS	Preliminary cybersecurity requirements	Managing a virtualized environment					L5SCB_SI8	create and manage a virtual machine select a suitable cloud application install and manage a hypervisor	L6SCB_SI8	containerise applications recommend security measures for containerised applications	L7SCB_SI8	orchestrate containers create a high availability (HA) virtual machine environment		
		Creating scripts and applications	L3SCB_SI9	create simple scripts	L4SCB_SI9	create scripts based on external libraries	L5SCB_SI9	implement design patterns in applications use front-end frameworks	L6SCB_SI9	create web applications create mobile applications create desktop applications combine individual components to create a system				
		Managing the application runtime environment	L3SCB_SI10	check the compatibility of operating systems	L4SCB_SI10	identify system malfunctions take precautions to avoid destabilising systems	L5SCB_SI10	respond to application errors that occur after updating operating systems	L6SCB_SI10	analyse the effects of upgrading the runtime environment on an application				
		Personal development			L4SCB_SI11	choose one's own development path take advantage of the cybersecurity training programmes taking place in one's organisation	L5SCB_SI11	search for and use external training courses on cybersecurity use various sources of knowledge, including alternative sources acquire knowledge about news in the sector from various sources develop sector-specific language skills, including in English						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
is able to:														
SKILLS	Preliminary cybersecurity requirements	Supporting the development of others			L4SCB_SI12	provide cybersecurity training develop a basic training programme on cybersecurity	L5SCB_SI12	monitor the level of awareness of users regarding cybersecurity diagnose the cybersecurity training needs of staff share knowledge and experiences with others propose modifications to cybersecurity training	L6SCB_SI12	define career paths for employees implement a system for sharing knowledge and experiences in the organisation manage the knowledge and experience sharing system in the organisation develop specialised cybersecurity training	L7SCB_SI12	transfer one's knowledge and experiences in a variety of forms, including sectoral meetings design an employee development plan design an employee competence management system	L8SCB_SI12	design cybersecurity training programmes for the organisation
knows and understands:														
KNOWLEDGE	Identification	Internal and external context of the organisation	L3SCB_KII1	the micro- and macro-economic terms necessary for the performance of tasks in the organisation	L4SCB_KII1	the organisation's business standards the organisational structure and main processes of the organisation the operating principles of different types of organisations, including companies, public institutions, NGOs	L5SCB_KII1	external stakeholders' expectations of the organisation's services and products	L6SCB_KII1	the principles of developing and implementing new business processes the principles of optimising implemented business processes	L7SCB_KII1	the principles, processes and timeline for developing standards, regulations and legislation, taking into account the context of the sector/organisation		
		Supply chain and value chain			L4SCB_KII2	the organisation's supply chain model	L5SCB_KII2	the organisation's value chain model						
		Risks in the organisation	L3SCB_KII3	the potential risks to the organisation, including sources of risk the methods for documenting potential risks in the organisation the importance of risk monitoring for cybersecurity	L4SCB_KII3	the methods and tools for identifying risks in the organisation the needs of stakeholders for monitoring risk	L5SCB_KII3	the methods, tools and organisational solutions used to counteract the occurrence of risks in the organisation	L6SCB_KII3	the impact on the company's threat level of particular risks occurring	L7SCB_KII3	the development trends of the methods, tools and organisational solutions for preventing and minimising risks in the organisation	L8SCB_KII3	the latest developments in the methods, tools and organisational solutions for protecting against potential risks in the organisation

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Identification	Internal and external processes, products and services in the organisation			L4SCB_KII4	the cybersecurity requirements for processes, products and services within and outside the organisation and the people responsible for them	L5SCB_KII4	the basics and principles of using process analysis the processes of the whole life cycle of purchased and sold products and services with digital elements, including design, development, installation, implementation, maintenance, updating, servicing and decommissioning	L6SCB_KII4	the principles of change management and the implementation of new ways of organising work at the team/ departmental level	L7SCB_KII4	the impact of financial constraints on implementing solutions that meet cybersecurity requirements the principles of change management and implementing new ways of organising work at the level of the whole organisation		
		Assets in the organisation	L3SCB_KII5	the types of assets in an organisation	L4SCB_KII5	the solutions used in an organisation	L5SCB_KII5	the potential interdependencies between different assets in the organisation relevant to cybersecurity the importance of financial, intangible and legal assets the operation of CMDBs or other databases containing information about users and system configurations						
		Design principles and the implications of technology selection on the life cycle of products and services			L4SCB_KII6	the role of cybersecurity in the design of products and services from a life cycle perspective	L5SCB_KII6	the functional and non-functional requirements of products and services	L6SCB_KII6	the cybersecurity implications of using specific technologies and tools for products and services from a life cycle perspective	L7SCB_KII6	the principles of integrating cybersecurity requirements in the creation of new products and services and their life cycle	L8SCB_KII6	the cybersecurity requirements in the process of technology creation and development

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Identification	Identifying components, events, objects			L4SCB_SII1	select tools, procedures and processes to identify known objects, including their characteristics, as well as groups of objects correct identification results	L5SCB_SII1	profile known objects or groups of objects extend profile records with new characteristics	L6SCB_SII1	select tools, procedures and processes to identify unknown objects and groups of objects profile systems, physical environments visualise static and dynamic environments	L7SCB_SII1	profile unknown objects or groups of objects profile ethereal objects perform deep identification for communication protocols and protocol stacks build identification tools from known solutions	L8SCB_SII1	build tools to identify complex systems and their interrelationships
		Directory services	L3SCB_SII2	use directory services to identify an organisation's assets	L4SCB_SII2	use directory services to gather information about an organisation's assets	L5SCB_SII2	configure directory services, including defining rules for handling objects						
		Identifying an organisation's human assets	L3SCB_SII3	identify key people in individual processes	L4SCB_SII3	identify the roles and responsibilities of individuals in specific processes, including key persons define the requirements to be met by suppliers and external partners as well as employees identify the roles and requirements of the persons responsible for cybersecurity, including the ones arising from legislation and good practices	L5SCB_SII3	identify critical roles for people in the organisation identify critical relationships among key individuals	L6SCB_SII3	develop cybersecurity requirements to be met by key persons and other employees	L7SCB_SII3	assess and shape the organisational structure from the perspective of the integration and application of cybersecurity requirements		
		Identifying an organisation's hardware and software assets	L3SCB_SII4	identify IT and OT devices and software	L4SCB_SII4	identify the dependencies between systems, networks, devices and software	L5SCB_SII4	identify the critical dependencies between systems, networks, devices and software for cybersecurity	L6SCB_SII4	develop cybersecurity requirements for systems, networks, devices and software				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
								is able to:						
SKILLS	Identification	Identifying an organisation's process assets	L3SCB_SII5	identify information flow paths	L4SCB_SII5	identify information systems structure describe critical processes	L5SCB_SII5	identify critical processes for cybersecurity identify critical dependencies	L6SCB_SII5	develop cybersecurity requirements for critical processes	L7SCB_SII5	include and integrate cybersecurity requirements into operational plans		
		Designing products and services					L5SCB_SII6	define and integrate typical functional and non-functional requirements for products and services	L6SCB_SII6	define and integrate complex functional and non-functional requirements for products and services	L7SCB_SII6	define and integrate diverse and technologically heterogeneous functional and non-functional requirements for products and services	L8SCB_SII6	create and develop tools for securing products and services in their life cycle incorporate cybersecurity principles into the design or development of products and services
		Socio-economic environment of the organisation			L4SCB_SII7	identify the legal requirements, good practices and business standards affecting the organisation identify external partners obtain legal support in interpreting regulations relating to cybersecurity in the organisation	L5SCB_SII7	indicate the solutions that will meet the requirements, including legal ones	L6SCB_SII7	identify and determine the extent of the need to cooperate with others, including with institutions, universities, vocational schools	L7SCB_SII7	identify new concepts and technologies, including their effect on the organisation's cybersecurity	L8SCB_SII7	initiate changes, including legal ones, affecting the organisation's cybersecurity
		Supply chain	L3SCB_SII8	verify that suppliers have fulfilled the contract	L4SCB_SII8	establish a supply chain and identify suppliers	L5SCB_SII8	identify dependencies in the supply chain	L6SCB_SII8	identify the service provision parameters of suppliers prioritise supply chain dependencies and identify critical dependencies identify the cybersecurity requirements for suppliers and supply chains				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Identification	Risk assessment	L3SCB_SII9	identify external and internal risks determine the vulnerability of assets and processes to the identified risks	L4SCB_SII9	develop, categorise and document identified risks	L5SCB_SII9	assess the scale of the risk and its impact on the organisation determine the impact and likelihood of a risk occurring prioritise the diagnosed potential risks to the company determine the level of acceptable risk select methods of handling potential risks, including counteracting them, minimising their occurrence, transferring them develop an action plan with tools to address potential risks	L6SCB_SII9	develop a policy for handling risks	L7SCB_SII9	develop a strategy to counteract the occurrence of risks in the organisation		
		Introducing safety requirements into processes, products and services	L3SCB_SII10	identify the persons responsible for preparing new products and services	L4SCB_SII10	present and explain to the persons responsible for preparing new products and services their responsibilities in the area of cybersecurity	L5SCB_SII10	align business processes with cybersecurity requirements in new services and products monitor the implementation of cybersecurity policies by the persons responsible for developing new products and services analyse and document the processes affecting the level of security of new products and services	L6SCB_SII10	adapt the scope of cybersecurity requirements to new products and services propose changes to the structure of the cybersecurity system change cybersecurity management at the team/departmental level	L7SCB_SII10	manage the budget for implementing solutions that meet cybersecurity requirements analyse the financial and organisational impact change cybersecurity management at the organisational level		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Protection	Identity, authentication and access control, including remote access	L3SCB_KIII1	the basic concepts of identity and authentication access mechanisms, including remote access	L4SCB_KIII1	the principles of using single and multi-factor authentication systems as well as biometric systems	L5SCB_KIII1	the good practices of identity management, authentication and access control, including remote						
		Protection of IT systems	L3SCB_KIII2	the reasons for protecting IT systems	L4SCB_KIII2	the ways IT protection systems function and their mechanisms the ways of protecting the data processed in IT systems	L5SCB_KIII2	the requirements resulting from the use of specific IT protection systems the division of responsibilities between protection mechanisms, including in cloud systems (between the provider and the client) for various cloud service models (SaaS, IaaS, PaaS)	L6SCB_KIII2	advanced protection systems, including vulnerabilities and limitations due to the need for the operational continuity of IT systems	L7SCB_KIII2	trends in the development of protection mechanisms for IT systems	L8SCB_KIII2	new threat areas where IT protection mechanisms need to be developed
		Protection of OT systems	L3SCB_KIII3	the reasons for protecting OT systems	L4SCB_KIII3	the ways OT protection systems function and their mechanisms the specificity of the functioning of OT systems and the requirements they have to fulfil, including those relating to ensuring the availability and security of the implemented processes	L5SCB_KIII3	the operation of OT protection systems the requirements resulting from the use of specific OT protection systems the dependencies between the IT systems and OT systems used in an organisation	L6SCB_KIII3	advanced protection systems, including vulnerabilities and limitations due to the need for the operational continuity of OT systems	L7SCB_KIII3	trends in the development of protection mechanisms for OT systems	L8SCB_KIII3	new threat areas where OT protection mechanisms need to be developed
		Malware	L3SCB_KIII4	the basic types of malware	L4SCB_KIII4	the principles of static and dynamic malware analysis, including sandbox analysis, machine code	L5SCB_KIII4	the way the malware used by attackers works						
		Signatures for monitoring systems			L4SCB_KIII5	types of signature attacks	L5SCB_KIII5	the methods for creating signatures for the recognition of attacks and malware	L6SCB_KIII5	the methods for designing new signature solutions/algorithms				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Protection	Managing remote access control	L3SCB_SIII1	configure and manage remote access mechanisms	L4SCB_SIII1	propose a remote access mechanism for the organisation and present its advantages and disadvantages verify the remote access rights assigned to users	L5SCB_SIII1	propose appropriate solutions for the implementation of remote access control systems in the organisation develop the principles of remote access control management verify a remote access control management system	L6SCB_SIII1	implement a remote access control management system in an organisation	L7SCB_SIII1	develop a remote access control management system in an organisation		
		Managing identity and authentication	L3SCB_SIII2	grant permissions to users and user groups in an operating system	L4SCB_SIII2	identify and select an authentication mechanism for different classes of systems select authentication devices and techniques enforce rules on the length, complexity and retention of passwords	L5SCB_SIII2	propose solutions for implementing identity and authentication management systems in an organisation develop identity and authentication management policies	L6SCB_SIII2	implement an identity and authentication management system in an organisation	L7SCB_SIII2	develop an identity and authentication management system in an organisation		
		Solutions analysing user behaviour in an IT system			L4SCB_SIII3	use solutions that analyse user behaviour	L5SCB_SIII3	configure solutions that analyse user behaviour	L6SCB_SIII3	adapt and implement solutions that analyse user behaviour				
		Protected environment	L3SCB_SIII4	identify the boundaries between components install and configure an anti-virus program set up an account with a password	L4SCB_SIII4	identify the boundaries between objects	L5SCB_SIII4	identify the boundaries between systems	L6SCB_SIII4	participate in the administration of protected systems in the organisation				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Protection	Analysis of malware and IT systems	L3SCB_SIII5	identify malware types search for information on malware and the tools it uses	L4SCB_SIII5	identify vulnerabilities in the IT systems exploited by malware	L5SCB_SIII5	analyse malware and vulnerabilities in IT systems	L6SCB_SIII5	analyse malware trends	L7SCB_SIII5	modify malware to increase the protection of systems	L8SCB_SIII5	develop methods to protect IT systems from unknown malware
		Monitoring users and systems	L3SCB_SIII6	apply the technique of remote and fixed access	L4SCB_SIII6	use system monitoring hardware and software, including logs	L5SCB_SIII6	analyse data from system monitoring hardware and software apply the technique of active user session monitoring correlate events from multiple devices and draw conclusions						
		Monitoring risks	L3SCB_SIII7	monitor risks in accordance with agreed procedures, using available tools	L4SCB_SIII7	report monitoring results to stakeholders, i.e., ensure that useful, complete and up-to-date risk information is available	L5SCB_SIII7	develop policies and procedures for monitoring risks select tools to monitor and report risks	L6SCB_SIII7	develop tools to support risk monitoring				
		Preparing signatures for monitoring systems	L3SCB_SIII8	indicate an ongoing attack or unusual activity	L4SCB_SIII8	create signatures for known attack types	L5SCB_SIII8	create signatures for as yet unknown attack types						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
is able to:														
SKILLS	Protection	Using tools utilising artificial intelligence in cybersecurity systems			L4SCB_SIII9	interpret information received from artificial intelligence systems	L5SCB_SIII9	parameterise artificial intelligence systems and assess their performance maintain the performance efficiency of artificial intelligence systems	L6SCB_SIII9	propose the use of artificial intelligence methods to address the size, complexity and processing time of datasets for the purpose of automation create the requirements for artificial intelligence-based tools to ensure cybersecurity integrate artificial intelligence solutions with the systems operating within an organisation	L7SCB_SIII9	implement artificial intelligence solutions in the systems operating within an organisation		
		Maintaining operational continuity	L3SCB_SIII10	perform standardised activities to maintain the organisation's operational continuity	L4SCB_SIII10	cooperate with external suppliers to maintain operational continuity in the supply chain	L5SCB_SIII10	define the requirements for the operational continuity of specific areas manage cooperation with external suppliers to maintain operational continuity in the supply chain verify operational continuity activities	L6SCB_SIII10	prioritise the areas requiring operational continuity	L7SCB_SIII10	design operational continuity processes	L8SCB_SIII10	develop standards and specialised solutions for operational continuity processes
knows and understands:														
KNOWLEDGE	Detection	Vulnerabilities of and attacks on web applications			L4SCB_KIV1	the categories of web application vulnerabilities the categories of penetration tests and tools for penetration tests on web applications	L5SCB_KIV1	the typical vulnerabilities and attacks on server-side and client-side web applications, including SQL injection, XSS, CSRF, IDOR, Broken Access Control penetration testing methods for web applications, including OWASP Web Security Testing Guide, OWASP ASVS	L6SCB_KIV1	complex web vulnerability attacks, including SSRF, SSTI, data deserialization bugs, XXE, API vulnerabilities				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Detection	Vulnerabilities of and attacks on mobile systems and applications			L4SCB_KIV2	the categories of vulnerabilities of mobile systems and applications the categories of penetration testing and tools for mobile systems and applications	L5SCB_KIV2	the typical vulnerabilities of and attacks on server-side and client-side mobile applications penetration testing methods for mobile applications, including OWASP MASTG, OWASP MASVS	L6SCB_KIV2	complex vulnerability attacks on mobile applications, including API vulnerabilities the decompilation process (reverse engineering) for mobile applications				
		Vulnerabilities of and attacks on the network infrastructure	L3SCB_KIV3	network identification methods, including scanning of IP addresses, port numbers of active services	L4SCB_KIV3	the categories of vulnerabilities of network infrastructures the categories of penetration testing and tools for network infrastructures	L5SCB_KIV3	the typical vulnerabilities of and attacks on network infrastructures, including wireless networks penetration testing methods for network infrastructures, including OSSTMM	L6SCB_KIV3	complex vulnerability attacks, e.g., relating to network protocols and services, including MitM, DHCP and ARP spoofing				
		Vulnerabilities of and attacks on server and client systems			L4SCB_KIV4	the categories of server and client system vulnerabilities the categories of penetration tests and the tools to perform them for server and client systems	L5SCB_KIV4	the typical vulnerabilities and attacks on operating systems and the applications installed on them, including buffer overflow, format string, escape to shell	L6SCB_KIV4	the complex attacks on the vulnerabilities of directory services, including Active Directory				
		Vulnerabilities of and attacks on cloud environments			L4SCB_KIV5	the categories of cloud environment vulnerabilities the categories of penetration tests and the tools to perform them for cloud environments	L5SCB_KIV5	the typical vulnerabilities and attacks on cloud environments	L6SCB_KIV5	the complex attacks on the vulnerabilities of cloud environments				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Detection	Code analysis	L3SCB_KIV6	the principles of static and dynamic code analysis	L4SCB_KIV6	the methods and tools of static and dynamic code analysis	L5SCB_KIV6	code vulnerabilities, including those relating to memory management and data input	L6SCB_KIV6	the process of analysing the source code of a compiled software program (reverse engineering)				
		Principles of designing and managing IoT solutions	L3SCB_KIV7	IoT components IoT communication protocols the types of IoT solutions	L4SCB_KIV7	the principles of building complementary and centralised environments based on IoT components the basics of distributed communication in IoT the issues of powering IoT components the basic issues of operating stability in IoT systems	L5SCB_KIV7	the principles of monitoring IoT components and environments the basics of designing IoT solutions the typical vulnerabilities of and attacks on IoT solutions	L6SCB_KIV7	the issues of powering IoT components specialised networks, including AIM networks the principles of managing data in IoT environments the principles of designing IoT solutions	L7SCB_KIV7	the principles of developing IoT solutions requiring special protection		
		Principles of designing and managing OT solutions	L3SCB_KIV8	OT components OT communication protocols the types of OT solutions	L4SCB_KIV8	the principles of building complementary and centralised environments based on OT components the basics of distributed communication in OT the basic issues of operating stability in OT systems	L5SCB_KIV8	the principles of monitoring OT components and environments the basics of designing OT solutions the typical vulnerabilities of and attacks on OT solutions	L6SCB_KIV8	the issues of powering OT components specialised networks, including field networks the principles of managing data in OT environments the principles of designing OT solutions	L7SCB_KIV8	the principles of developing OT solutions requiring special protection		
		Principles of designing and managing large-scale complex automation systems	L3SCB_KIV9	the criteria defining the need for work automation the potential areas of work automation	L4SCB_KIV9	the principles of work automation	L5SCB_KIV9	the tools for building automation systems, including those based on artificial intelligence the basics of automation	L6SCB_KIV9	the principles of designing linear automation systems	L7SCB_KIV9	the principles of designing automation in co-linear, multithreaded systems	L8SCB_KIV9	the principles of integrating incompatible systems
		Simulated hacker attack	L3SCB_KIV10	the types of social engineering attacks the types of software used in internet redteaming attacks	L4SCB_KIV10	construction and functioning of software used in an internet redteaming attack	L5SCB_KIV10	the premises of the tests used in a redteaming attack						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Detection	Simulated physical attack			L4SCB_KIV11	the methods of physical redteaming attacks	L5SCB_KIV11	the security, alarm systems and access control methods used the tools used for testing security, alarm systems and access control methods	L6SCB_KIV11	the operation and vulnerabilities of alarm systems and access control methods				
		Social engineering	L3SCB_KIV12	the types of social engineering tests	L4SCB_KIV12	the principles of reading body language the typical behaviours of users susceptible to manipulation manipulation techniques the tools used in social engineering attacks	L5SCB_KIV12	the construction and operating principles of software supporting social engineering tests						
is able to:														
SKILLS	Detection	Penetration test baseline areas			L4SCB_SIV1	describe the vulnerabilities found	L5SCB_SIV1	assess the results of the conducted penetration test identify critical system areas requiring detailed testing prepare a report with recommendations based on the conducted penetration test develop one's own simple tools to support the implementation of penetration tests, including scanners, exploits	L6SCB_SIV1	prepare a penetration test plan supervise the implementation of penetration tests by a subordinate team	L7SCB_SIV1	modify tools for penetration tests	L8SCB_SIV1	develop tools for penetration tests

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Detection	Penetrations tests for web applications			L4SCB_SIV2	test web applications using automated tools	L5SCB_SIV2	test web applications using common types of vulnerabilities and attacks, including SQL injection, XSS, CSRF, IDOR, Broken Access Control perform web application tests in accordance with defined methods, including OWASP Web Security Testing Guide, OWASP ASVS	L6SCB_SIV2	conduct complex attacks against web vulnerabilities, including SSRF, SSTI, data deserialization errors, XXE, API vulnerabilities	L7SCB_SIV2	detect new vulnerabilities (zero-days) in web applications and exploit them for attacks		
		Penetration tests for mobile systems and applications			L4SCB_SIV3	test mobile systems and applications using automated tools	L5SCB_SIV3	conduct server-side and client-side attacks against typical mobile systems and applications using mobile application penetration test methods, including OWASP MASTG, OWASP MASVS	L6SCB_SIV3	conduct complex attacks against mobile applications, including API vulnerabilities perform mobile application decompilation (reverse engineering)	L7SCB_SIV3	detect new vulnerabilities (zero-days) in mobile systems and applications and exploit them for attacks		
		Penetration tests for network infrastructure			L4SCB_SIV4	test network infrastructure using automated tools perform network reconnaissance, including scanning IP addresses and the port numbers of active services	L5SCB_SIV4	conduct typical attacks against network infrastructure, including wireless networks	L6SCB_SIV4	conduct attacks on network protocols and services, including MitM, DHCP and ARP spoofing exploit devices to conduct attacks on network protocols and services	L7SCB_SIV4	detect new vulnerabilities (zero-days) in the network infrastructure and exploit them for attacks		
		Penetration tests for server and client systems			L4SCB_SIV5	test server and client systems using automated tools	L5SCB_SIV5	conduct attacks on typical operating systems and their applications, including buffer overflow, format string, escape to shell	L6SCB_SIV5	conduct attacks on directory services, including Active Directory	L7SCB_SIV5	detect new vulnerabilities (zero-days) in server and client systems and exploit them for attacks		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Detection	Penetration tests for cloud environments			L4SCB_SIV6	assess the correctness of the configuration of a cloud computing instance in terms of security perform a reconnaissance of public computing clouds	L5SCB_SIV6	plan and assess the effects of planned penetration tests in a cloud environment	L6SCB_SIV6	draw conclusions from conducted penetration tests of individual cloud computing instances propose solutions to increase the security of cloud computing instances				
		Analysing code			L4SCB_SIV7	perform automation code analysis identify the categories of vulnerabilities found with the automation tool	L5SCB_SIV7	identify the consequences of exploiting the vulnerabilities found	L6SCB_SIV7	analyse decompiled code autonomously identify vulnerabilities verify the results of an automated analysis	L7SCB_SIV7	detect new types of vulnerabilities in the code further develop code analysis tools	L8SCB_SIV7	develop solutions for IoT requiring special protection
		Building and managing IoT solutions	L3SCB_SIV8	build a simple IoT system based on direct communication	L4SCB_SIV8	build an IoT system based on algorithms or use scenarios	L5SCB_SIV8	monitor the operational status of individual devices and the entire IoT system	L6SCB_SIV8	automate the management of cybersecurity issues in IoT environments resolve vulnerability issues in IoT environments build a response system in the IoT environment based on monitored parameters	L7SCB_SIV8	solve instability issues in the OT operating environment build process systems in the OT environment	L8SCB_SIV8	develop solutions for OT requiring special protection
		Building and managing OT solutions	L3SCB_SIV9	build a simple OT system based on direct communication	L4SCB_SIV9	build an IoT system based on algorithms or use scenarios	L5SCB_SIV9	monitor the operational status of individual devices and the entire OT system	L6SCB_SIV9	automate the management of cybersecurity issues in OT environments build a response system in the OT environment based on monitored parameters resolve vulnerability issues in OT environments	L7SCB_SIV9	solve instability issues in the OT operating environment build process systems in the OT environment	L8SCB_SIV9	develop solutions for OT requiring special protection

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Detection	Building and managing large-scale complex automation systems			L4SCB_SIV10	build large-scale complex automation algorithms	L5SCB_SIV10	build a typical large-scale complex automation system monitor and maintain large-scale complex automation systems	L6SCB_SIV10	build large-scale complex systems with real-time requirements	L7SCB_SIV10	design large-scale complex systems with real-time requirements apply artificial intelligence to automate work in large-scale complex systems	L8SCB_SIV10	integrate incompatible systems
		Detecting changes	L3SCB_SIV11	detect changes at the component level	L4SCB_SIV11	detect unwanted changes at the code level	L5SCB_SIV11	detect changes at the system performance level	L6SCB_SIV11	detect and control changes after a reaction event	L7SCB_SIV11	detect and monitor changes in automated systems on a continuous basis		
		Redteaming			L4SCB_SIV12	conduct reconnaissance before launching a redteaming attack on the internet	L5SCB_SIV12	prepare the premises for a redteaming attack on the internet select the penetration test for a redteaming attack on the internet analyse the results of the redteaming attack on the internet	L6SCB_SIV12	adapt software to the premises of a redteaming attack on the internet perform a penetration test in a redteaming attack develop recommendations after a redteaming attack	L7SCB_SIV12	escalate a redteaming attack exploit newly found vulnerabilities in a redteaming attack identify possible new methods of redteaming attacks on the Internet	L8SCB_SIV12	develop tools for new types of redteaming attacks on the Internet

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
								is able to:						
SKILLS	Detection	Physical redteaming			L4SCB_SIV13	conduct reconnaissance before launching a physical redteaming attack	L5SCB_SIV13	prepare the premises for a physical redteaming attack select the penetration test for a physical redteaming attack select the methods for a physical attack develop one's own simple support tools bypass typical security features, alarm systems and access control methods use tools to test security, alarm systems and access control methods analyse the results of the physical redteaming attack test access control in the organisation	L6SCB_SIV13	conduct a physical attack bypass advanced security features, alarm systems and access control methods adapt software to the premises of a physical redteaming attack perform a penetration test in a physical redteaming attack develop recommendations after a physical redteaming attack	L7SCB_SIV13	escalate a physical redteaming attack exploit newly found vulnerabilities in a physical redteaming attack identify possible new methods of physical attacks	L8SCB_SIV13	develop tools for new types of physical attacks
		Social engineering tests					L5SCB_SIV14	apply manipulation techniques conduct social engineering tests develop one's own simple tools to support the implementation of social engineering tests	L6SCB_SIV14	define the expected results of the social engineering tests prepare a social engineering test plan develop recommendations after a social engineering attack				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Detection	Threat modelling	L3SCB_SIV15	recognise system components and their functions	L4SCB_SIV15	recognise the dependencies among system components	L5SCB_SIV15	detect the typical threats associated with system architecture	L6SCB_SIV15	perform a risk analysis, including an assessment of the potential impact of attacks, the likelihood of their occurrence and predict their impact on the system use various threat modelling working methods such as STRIDE, DREAD, OWASP Threat Modelling Guide	L7SCB_SIV15	predict new areas where threats may occur		
				knows and understands:										
KNOWLEDGE	Response	Terminology and technology relating to evidence	L3SCB_KV1	the types of evidence the types of evidence preservation the basic terminology relating to digital evidence, including the concepts of evidence manipulation and degradation, timestamp, system time, volatile and non-volatile evidence the algorithms for hash functions the concepts of logs as well as system and application configurations	L4SCB_KV1	the types of information processed in IT systems, including digital devices, databases, system-generated documents, user-generated data and volatile data	L5SCB_KV1	the ability of a file system structure to be audited the ways of securing information processed in the various components of an IT system						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Response	Securing evidence	L3SCB_KV2	the basic techniques of preserving different types of evidence the methods of determining the requirements for preserving evidence the effects of external factors on evidence, such as moisture, temperature and jolts the techniques for transporting evidence in such a way that it can be used in subsequent evidentiary proceedings	L4SCB_KV2	the techniques for evidence replication the certification standards for processing evidence samples during proceedings the consequences, including legal ones, of errors due to the investigator or the environment, affecting the quality and reliability of the evidence	L5SCB_KV2	the legal requirements for handling digital evidence the dependencies among different information groups, data formats the techniques of information aggregation the techniques of receiving and preserving information for laboratory proceedings						
		Handling digital evidence	L3SCB_KV3	the potential locations for obtaining information to analyse an incident the requirements and procedures for maintaining the chain of evidence in accordance with legal requirements the principles of preparing digital evidence for transport, transmission, transfer and storage	L4SCB_KV3	the principles of analysing digital evidence the principles of generating documents for an evidence audit the principles of determining the parameters of the documentation the principles of ensuring information security the principles of preserving digital evidence	L5SCB_KV3	the legal requirements for obtaining digital evidence the means of applying protection measures to secure digital evidence the procedures for documenting evidence						
		Incident response systems	L3SCB_KV4	specific incident response plans, including those developed for the organisation and its internal systems the principles of external and internal communication concerning an incident	L4SCB_KV4	the good practices of incident response the principles of preparing an incident handling report how particular incident response systems work	L5SCB_KV4	legal incident reporting requirements contractual incident reporting requirements						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Response	Identifying evidence	L3SCB_SV1	reconnoitre the environment having the evidence that needs to be secured	L4SCB_SV1	identify the systems having the evidence that needs to be secured identify the passwords required for the evidence to be analysed identify the impact of system and application configurations on how they operate verify information during a discussion, including with the person to whom the evidence relates	L5SCB_SV1	aggregate seemingly inconsistent information or incompatible systems link detected events from multiple sources of attack	L6SCB_SV1	identify the level of risk threats from the outside world, taking into account the specificity of the organisation resolve the failures or unavailability of the system				
		Securing and obtaining evidence	L3SCB_SV2	obtain and collect digital evidence following standard procedures secure the evidence in accordance with the accepted protocol select a method of transporting groups of evidence appropriate to the situation	L4SCB_SV2	obtain and collect analogue evidence required for analysis obtain, collect and process digital evidence in accordance with non-standard procedures document evidence, including evidence that cannot be seized select the appropriate technique for securing evidence in a particular system environment working in a specific physical environment copy evidence and forward it to another analysis work station collect groups of evidence select the techniques of receiving evidence indicate potential evidence not covered by procedures	L5SCB_SV2	select the tools to counteract the danger of undermining the evidence prepare an incident report	L6SCB_SV2	assign roles in the process of securing evidence support technicians in and around the laboratory in accordance with procedures and technical needs after a security incident	L7SCB_SV2	minimise the potential risks to evidence manage a team performing evidence work in the computer forensics lab and in the field		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Response	Analysing collected evidence			L4SCB_SV3	assess the quality and reliability of evidence using specific systems and solutions to support automated assessment use a variety of systems and data to extract information and transport it	L5SCB_SV3	receive groups of evidence into the laboratory perform the procedure for receiving a partial or complete image from a digital storage medium qualify evidence or groups of evidence use technical solutions to increase the efficiency of processing evidence	L6SCB_SV3	analyse the evidence obtained, including with the use of specialised tools	L7SCB_SV3	manage a team performing analytical work	P8SCB_SV3	search for and analyse non-standard evidence develop new methods for the correct extraction of data develop a new solution for the correct extraction of data
		Responding to events and incidents	L3SCB_SV4	identify the components of an event cooperate with the person involved in an incident	L4SCB_SV4	respond to events in accordance with procedures, response standards, incident handling plans identify the correlations between two events verify the completeness of incident handling plans	L5SCB_SV4	modernise procedures, response standards in reaction to an incident communicate the incident to stakeholders, including management, customers, external bodies analyse and respond to incidents involving individual systems coordinate incident response activities prepare and present an incident handling report	L6SCB_SV4	develop plans, procedures, scenarios for security incident response develop automated incident response tools	L7SCB_SV4	develop security incident response standards identify system development paths that minimise the potential impact of incidents		
		Cybersecurity laboratory, including digital forensics	L3SCB_SV5	use the basic tools of a cybersecurity laboratory including digital forensics	L4SCB_SV5	select a workstation appropriate to the issue or objective of the investigation	L5SCB_SV5	plan the scope of the investigation taking into account the specificities of the cybersecurity laboratory, including digital forensics conduct an investigation using tools appropriate to the evidence collected prepare a report on the investigation performed	L6SCB_SV5	identify and assign specific roles to persons in the laboratory in the area of cybersecurity, including digital forensics verify the correct use of tools by personnel in the cybersecurity lab, including digital forensics	L7SCB_SV5	simulate a security incident to verify the performance of the system under investigation in a cybersecurity lab, including digital forensics, and minimise the potential consequences	L8SCB_SV5	develop new technical and procedural solutions to optimise the lab's performance in the area of cybersecurity, including digital forensics

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
knows and understands:														
KNOWLEDGE	Recovery	Data backups	L3SCB_KVI1	the types of data backups	L4SCB_KVI1	the construction and limitations of data media the methods and systems for making backup copies	L5SCB_KVI1	the principles of building data backup centres						
		Operational continuity model			L4SCB_KVI2	the construction and limitations of the operational continuity model the methods of implementing the operational continuity model	L5SCB_KVI2	the methods of developing an operational continuity model tailored to the needs of the organisation the potential effects of an incident on the functioning of the operational continuity model						
is able to:														
SKILLS	Recovery	Identifying operational continuity issues	L3SCB_SVI1	identify an incident by type	L4SCB_SVI1	assess the severity of the threat	L5SCB_SVI1	respond to the incident in accordance with internal procedures make changes in case of a failure to restore the system monitor the correct operation of backup systems	L6SCB_SVI1	develop and implement procedures for switching to backup systems				
		Assessing an incident	L3SCB_SVI2	replicate an incident	L4SCB_SVI2	replicate the incident to verify operating procedures	L5SCB_SVI2	analyse an incident and its effects	L6SCB_SVI2	develop structural solutions in response to an incident that has occurred	L7SCB_SVI2	recommend and initiate the implementation of structural changes		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
				is able to:										
SKILLS	Recovery	Reconstructing the operational continuity model	L3SCB_SVI3	identify the vulnerabilities of the operating model in the context of the incident that has occurred	L4SCB_SVI3	develop proposals for technical changes in response to the incident that has occurred	L5SCB_SVI3	analyse the situation in the context of the incident that has occurred and draw conclusions develop an optimal sequence of corrective actions taking into account the specificity of the organisation or systems correct the action model	L6SCB_SVI3	modify action models taking into account the conditions of the organisation and the incident that has occurred	L7SCB_SVI3	develop new action models taking into account the conditions of the organisation and the incident		
		Reproducing operational continuity	L3SCB_SVI4	monitor the indicators of the operational control systems and the automatic execution of backups check that backups are correct restore backup copies	L4SCB_SVI4	monitor the switchover of IT systems to servers in the CPD backup monitor the point in time when digital systems regain full service	L5SCB_SVI4	recommend devices and software for making backup copies develop backup retention policies develop an operational continuity plan	L6SCB_SVI4	critically analyse the backup policy solutions in use implement changes in backup solutions resulting from policy evaluation take a tactical approach in adapting operational continuity	L7SCB_SVI4	implement changes in backup solutions resulting from a trend analysis take a strategic approach in adapting the operational continuity plan		
		Verifying contractual provisions	L3SCB_SVI5	identify the contractual provisions affecting the operational continuity of the systems	L4SCB_SVI5	verify the compliance of contractual provisions with measures to ensure systems security execute contracts, including OLAs and SLAs monitor the implementation of contractual provisions, including OLAs and SLAs	L5SCB_SVI5	recommend contractual provisions, including OLAs and SLAs, to support operational continuity assurance						

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
		knows and understands:												
KNOWLEDGE	**Cybersecurity audit as part of security management**	Cybersecurity audit principles	L3SCB_KVII1	the objectives and scope of a cybersecurity audit the types of documentation needed to prepare and perform a cybersecurity audit	L4SCB_KVII1	cybersecurity audit procedures the principles for classifying organisations the key differences between sectors, industries, types of facilities where a cybersecurity audit is conducted the tools used in a cybersecurity audit the requirements of remaining security requirements, including information security, physical security	L5SCB_KVII1	the recommendations from sector-specific bodies as a reference for an audit the overarching requirements for auditing entities the impact of audit tools on the object under analysis and its operational continuity	L6SCB_KVII1	the impact of audit tools on the stability of operating complex systems	L7SCB_KVII1	the impact of audit tools on the integrity of sub-components operating within complex systems the principles of designing audit tools	L8SCB_KVII1	the principles of designing specialised audit tools and their directions of development
		Managing an audit team			L4SCB_KVII2	the roles within an audit team due to fundamental differences in the sectors	L5SCB_KVII2	the roles within an audit team due to specific intra-sectoral differences	L6SCB_KVII2	the roles within an audit team due to specialist differences the basic principles of audit team management	L7SCB_KVII2	the principles of audit team management taking into account the complexity of the organisation and the audit's impact on it	L8SCB_KVII2	the directions of development of audit methods

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is able to:								
SKILLS	Cybersecurity audit as part of security management	Preparing a cybersecurity audit			L4SCB_SVII1	verify that the formal requirements of the organisation's policies are met prepare the documents needed for a cybersecurity audit identify the risks in the audited area	L5SCB_SVII1	identify the resources necessary to conduct an audit in the area being audited verify the organisation's compliance with legal and formal requirements, taking into account the nature of its activities and its infrastructure and devices verify compliance with norms, standards and good practices analyse the results of previous audits, including post-audit recommendations come to agreement on the cybersecurity audit plan with the organisation	L6SCB_SVII1	verify that the organisation fulfils the legal and formal obligations of the main requirements relating to its classification develop a cybersecurity audit plan, including sampling prepare the set of tools for an audit	L7SCB_SVII1	modify the set of tools needed to perform a specific cybersecurity audit	L8SCB_SVII1	design audit ecosystems and the tools to perform an audit in industries where the cybersecurity audit is a new activity
		Audit qualification procedures	L3SCB_SVII2	collect and verify the project documentation, subcontractor documentation, as well as facility operating instructions for compliance with the specified requirements (DQ)	L4SCB_SVII2	verify the correspondence of the project documentation, subcontractor documentation, and operating instructions with their actual implementation in the facility (IQ) prepare a discrepancy report	L5SCB_SVII2	verify that the installed or modified devices, software or system operates in accordance with the baselines of the functional groups and systems (OQ)	L6SCB_SVII2	verify that the combined functional groups properly create a specific generation process and deliver a specific product or intermediate product at a specific time and place in the facility (PQ)	L7SCB_SVII2	tailor audit activities to the specialised requirements of specific organisations		

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
								is able to:						
SKILLS	Cybersecurity audit as part of security management	Conducting an audit	L3SCB_SVII3	distinguish between activities for audit, control and assessment activities	L4SCB_SVII3	conduct audit tasks in accordance with the programme secure evidence	L5SCB_SVII3	analyse audit findings and propose solutions use cybersecurity audit tools as intended prepare a security audit report prepare a control report	L6SCB_SVII3	prepare a security audit report with recommendations on non-conformities and areas to optimise define the scope of individual actions resulting from an audit and assign the actions to be performed to individual organisational units	L7SCB_SVII3	transfer knowledge after a cybersecurity audit be flexible in applying new, necessary audit activities in the course of an audit, including the selection of an adequate sample	L8SCB_SVII3	design new audit activities
		Post-cybersecurity audit activities					L5SCB_SVII4	assess the implementation of recommendations by the audited entity following an audit assignment	L6SCB_SVII4	implement findings and recommendations from a cybersecurity audit	L7SCB_SVII4	implement and oversee the implementation of major changes resulting from a cybersecurity audit	L8SCB_SVII4	design solutions after having conducted a cybersecurity audit
								is ready to:						
SOCIAL COMPETENCE	Work standards	Shaping attitudes in the area of cybersecurity	L3SCB_SCVIII1	take responsibility for how products and services are used	L4SCB_SCVIII1	follow cybersecurity policies and procedures for products, services and organisations	L5SCB_SCVIII1	conduct informational activities to increase cyber resilience in the use of products and services	L6SCB_SCVIII1	promote and communicate activities to increase cyber resilience	L7SCB_SCVIII1	promote and shape appropriate attitudes in the area of cybersecurity	L8SCB_SCVIII1	create role models for attitudes in the area of cybersecurity
		Ethical standards					L5SCB_SCVIII2	comply with professional ethics in cyberspace promote ethical principles in cyberspace	L6SCB_SCVIII2	resolve ethical dilemmas relating to the provision of cybersecurity				

CATEGORY	SECTORAL DETERMINANT	COMPETENCE SERIES	SQF CB CODE	LEVEL 3	SQF CB CODE	LEVEL 4	SQF CB CODE	LEVEL 5	SQF CB CODE	LEVEL 6	SQF CB CODE	LEVEL 7	SQF CB CODE	LEVEL 8
						is ready to:								
SOCIAL COMPETENCE	Work standards	Responsibility			L4SCB_SCVIII3	consciously comply with cybersecurity policies and procedures, taking into account the possible consequences of unreliable performance	L5SCB_SCVIII3	face the consequences of unreliable performance or non-compliance with cybersecurity policies and procedures	L6SCB_SCVIII3	promote an attitude of responsibility for cybersecurity assurance processes	L7SCB_SCVIII3	co-create norms/ standards of behaviour promoting quality in the area of cybersecurity promote a culture of quality in the area of cybersecurity	L8SCB_SCVIII3	shape a culture of quality in the area of cybersecurity
						is ready to:								
SOCIAL COMPETENCE	Communication and cooperation	Communication			L4SCB_SCIX1	communicate with a wide range of stakeholders, including those unfamiliar with sector-specific terminology, in a way they can understand	L5SCB_SCIX1	communicate in high-stress, high-risk situations, including security incidents communicate to peers their roles and responsibilities in the organisation's cybersecurity processes	L6SCB_SCIX1	present and justify the principles of the cybersecurity system to managers, taking into account the scope of their responsibilities	L7SCB_SCIX1	communicate in the international community, taking into account cultural differences		
		Relations, behaviour, responses			L4SCB_SCIX2	cooperate closely and effectively with stakeholders in the tasks of ensuring cybersecurity act appropriately under stress	L5SCB_SCIX2	is ready for changes in the technical and organisational solutions for the cybersecurity system adapt in the changing conditions of the cybersecurity sector	L6SCB_SCIX2	make decisions under changing, non-routine conditions in the event of a security incident, under conditions of incomplete information, high risk				
		Internet privacy and anonymity			L4SCB_SCIX3	use social networking sites in a way that maintains anonymity and privacy	L5SCB_SCIX3	manage the information about oneself in the internet						

Glossary of terms used in the Sectoral Qualifications Framework for Cybersecurity

TERM	DEFINITION
AIM network	Part of the automated infrastructure management (AIM) system, a solution that provides illustration, management, analysis and planning functions.
Anomaly	Behaviour (event) not in line with procedures, standards adopted in the organisation.
API	Application Programming Interface – a programming interface, which is a set of rules, protocols and tools used to build and interact with software and applications. It defines how applications or system modules should communicate with each other, defines the functions available for use, the rules for their operation and indicates the data necessary for their execution. It also defines rules to enable secure data transfer, e.g., by implementing authentication (user identity verification) and authorisation (granting of rights).
Authentication	Verification of the identity of a person, application or system. It verifies that the entity attempting to gain access to a resource is who they say they are. The authentication process may involve the use of passwords, certificates, biometrics (such as fingerprints or facial recognition) or other methods.
Authorisation	The process of verifying a user's or system's prerogative to determine whether a person, application or device has the right to access specific resources or functions of an information system. Authorisation is one of the key elements of access control and aims to ensure that only authorised individuals or systems are granted access to the resources or data they are allocated.
Blue Team	A team dedicated to defensive operations. Its role is to respond to attacks, threats, monitor network traffic and take action if an attack attempt is detected.
Branch	One of the areas of a sector, e.g., heating branch (energy sector), dietary supplements branch (pharmaceutical sector), etc.

Buffer overflow	Vulnerability involving an attempt to write more data to a memory buffer, exceeding its size.
Cloud solutions	Modern services involving the provision by specialised entities (providers) of computing power, disk space, development environment or finished applications. The user does not need to have a licence to use the applications or invest in disk space, and can make full use of the functionality of this paid service. The biggest advantages of cloud solutions are cost reduction, constant availability of resources, the ability of distributed teams to work, standardisation, flexibility and the adaptation of services to current needs.
CMDB	Configuration Management Database – a database containing information about assets and the relationships between them.
Cryptoanalysis	The field of knowledge concerned with transforming secret (encrypted) information into open (unencrypted) information without needing a decryption key.
Cryptography	The field of knowledge encompassing methods of encryption, i.e., the transformation of plain text information into secret information (cipher text). A cipher text is unintelligible to the recipient without a decryption operation, which requires the possession of additional, usually secret, information, i.e., a decryption key.
Cybersecurity	Activities, policies and procedures to maintain the continuity of an organisation's operations by protecting systems, networks, data, their users and other entities from unauthorised access, use, disclosure, disruption, modification or destruction as well as the ability to recover operational continuity after an incident.
Cyber threats	Cyber threats are any potential situation, event or activity that could harm, disrupt or otherwise adversely affect systems, services, products or their stakeholders.
Data	Facts recorded, processed and transmitted by the sender in the form of a message that are not structured, processed or combined in accordance with the purpose and objectives of the recipient.
Data carrier	A device used to collect, store, process and transmit data. The devices can be internal (e.g., hard drive) and external/portable (e.g., memory stick, memory card, external drive or CD).

Data information security	A set of security tools and procedures that broadly protect confidential information from misuse, unauthorised access, disclosure, modification, control, disruption or destruction.
Decompilation	The process of translating an executable file into a higher order form (source code).
Desktop application	Programs that are installed and run directly on a device, e.g., desktop computer, laptop, tablet, smartphone. No internet access is required for their operation.
Detection phase	Preparing and implementing appropriate actions to identify the occurrence of events affecting cybersecurity.
Directory service	A directory service is a specialised database allowing for the storage, processing and mapping of relations between the objects present in it. These objects are typically users, applications, computers, servers and other computer devices. Directory services allow hierarchical groups of objects to be constructed and facilitate their management (e.g., managing permissions of individual groups). One of the most popular directory service standards is ITU-T X.500, implemented as the Lightweight Directory Access Protocol (LDAP). One of the most popular commercial directory service solutions is Active Directory.
DLP system	Data loss/leakage prevention (DLP) is a system to detect and prevent data leakage.
DQ	Design Qualification – verification of the design documentation, subcontract documentation and facility operating instructions to ensure that the requirements contained therein are in line with the actual state.
DQL, DML, DCL libraries	Libraries containing the SQL language syntax definition: DQL (Data Query Language), DML (Data Manipulation Language), DCL (Data Control Language).

Environment	The totality of the conditions under which an entity operates in the space of information processing and exchange established by information and communication systems, together with the links between them and relationships with users, characterised by challenges (opportunities and risks) and threats to the achievement of the adopted objectives.
Event	Behaviour in information systems, e.g., logging into a computer. An event can occur in accordance with procedures and standards or be non-compliant. In the latter case, the event is called an anomaly.
Evidence (volatile/ non-volatile)	Evidence can help reconstruct attacks, identify vulnerabilities and provide proof to identify perpetrators or prove that unauthorised actions have been committed. Volatile evidence in the area of cybersecurity refers to information or traces that may only exist for a short period of time. Examples are temporary log files, network connection sessions, cached data that may contain important information about attacks or unauthorised activities. Due to their impermanence, the collection and analysis of these volatile materials are crucial for understanding attacks and taking appropriate corrective action. Non-volatile evidence in the area of cybersecurity is that which is permanent and can exist for a long period of time. This includes, for example, data backups, system status snapshots, archived log files and security event recordings.
Exploit	An off-the-shelf tool, usually made available in the form of a script or source code, to take advantage of a specific vulnerability.
Forensic artefact	Any information left on information and communication systems by a user (including terminal equipment, servers, computer networks, etc.) whose actions are the subject of a forensic investigation. Collected digital traces constitute digital evidence.

Format string	Actions that exploit the erroneous way of passing arguments to functions that operate on strings of characters. The aim is to write and apply a program that, by taking advantage of the erroneous way in which arguments are passed, allows a string to be pasted in the appropriate field so as to smuggle dangerous code into a poorly secured application.
Hash, hashing	The process of creating a shortcut (hash) using a one-way shortcut function. Example hash generated using the MD5 hash function for the phrase "SQF CYBER" is "e9ea2a5425f062c8c5b003c525a2dc2d"
IaaS	Infrastructure as a Service – one of the models, along with SaaS (Software as a Service) and PaaS (Platform as a Service), of cloud computing services in which computing resources are hosted in the cloud. The service provider hosts the physical infrastructure, software and network at a specified bandwidth.
IACS model	Industrial Automation and Control Systems (IACS) model – refers to industrial automation equipment and control systems.
Identification phase	Preparing and implementing appropriate actions to identify and assess the occurrence of risks affecting cyber security.
Incident	An unwanted and/or unexpected cybersecurity event or set of events that has or may have an adverse effect on the security of information systems.
IoT	Internet of Things – the concept of using devices that are not typically computers (for example, household electronics) to build a network of devices that collect and process data and communicate with each other via a computer or other network.

IP address	IP addresses allow devices that are on the same or different networks to communicate with each other. IPv4 addresses are 32-bit addresses, represented in decimal notation with dots, e.g., 192.168.1.0. IPv6 addresses are 128-bit addresses, represented in hexadecimal notation with colons, e.g., 2a01:612f:1047:9710:e9e0:ca9a:586b:dd04. There are two methods of assigning IP addresses on a network interface: dynamic and static. Dynamic addresses are assigned by the DHCP server from the available address pool, while static IP addresses are assigned manually.
IQ	Installation Qualification – a documented check and confirmation that an installed or modified device, software or system complies with the approved design, manufacturer's recommendations or user requirements.
IT system	Information Technology – computer systems, networks and software for processing information. It typically consists of a networked computer or computers, software and peripherals: printers, scanners, mouse, keyboard, etc.
MAC address	Each network card has a unique 48-bit MAC address encoded in the card, represented in hexadecimal notation. Also known as the physical address. The Ethernet MAC address has two parts. The first 24 bits of the address represent the unique identifier of the organisation. This is the vendor or manufacturer part of the address, e.g., 00-60-2F. The second 24 bits are assigned by the provider and unique within its identifier, e.g., 3A-07-BC. The full address notation consisting of both parts is 00-60-2F-3A-07-BC. In addition to identifying devices, addresses can be used for communication between network interfaces on the same network.
Malicious software	Malicious software, also known as malware, is a type of software created with the intent to cause harm, steal information or conduct other illegal activities on a computer, network or devices. Malware is produced by cybercriminals for the purpose of financial gain, harming others or obtaining confidential data.
Mobile applications	Software installed and run on mobile (portable) devices, e.g., smartphones, tablets. This is publicly available software with a touch interface, designed for use on mobile devices.

Network	An interconnection of devices to exchange data among them. The devices communicate with each other via transmission media, using appropriate communication protocols.
Object	In the field of cybersecurity, the term 'object' can refer to various concepts and aspects. Depending on the context, object in cybersecurity can have the following meanings: **Data object:** In the context of data protection and privacy, an object can be a collection of information, a document or a file that contains sensitive data, such as customers' personal data or trade secrets. Data objects are an important target for protection against cyber attacks and data breaches. **Object of attack**: In the field of cybersecurity, an attack object refers to a target on which an attacker attempts to conduct an attack or breach. This can be a specific computer system, network, application or device. **Monitoring object**: In the context of security monitoring, a monitoring object can be a specific resource or activity in an IT system that is tracked to detect anomalies or suspicious activity. For example, a monitoring object could be network traffic, event logs or changes in system configuration. **Access control object**: In access management and access control for IT resources, an object can be a user, application or device that attempts to access specific resources. Security systems can assess whether an object has permission to access specific resources and whether this is authorised. **Object of analysis**: In threat analysis and incident response, the object of analysis can be data, logs or traces that are examined to understand the nature of an attack or incident. This could include malicious code analysis, network traffic anomaly detection, etc. **Risk management object**: In cyber risk management, these objects are the risk factors that can affect the security of an organisation. These could be systems, applications, people, processes or technologies that are assessed for potential threats and incident impacts.

OLA and SLA	A service level agreement (SLA) specifies the minimum level at which a provider will deliver particular services to a customer. An operational level agreement (OLA) defines the internal obligations among the operational providers of a given level of services. The purpose of this agreement is to guarantee the level of service agreed to in the OLA, mainly maintenance and development.
OQ	Operational Qualification (OQ) – documented verification and confirmation that an installed or modified device, software or system is operating correctly over the entire range of assumed operational conditions.
OSI model	Its full name is ISO OSI RM (International Organisation for Standardization Open Systems Interconnection Reference Model) – a standard describing the structure of ICT network communications divided into seven abstraction layers, such as physical, data link, network, transport, session, presentation and application.
OT system	Operational technology (OT) system – all equipment and systems (software) used to manage and monitor operations in production and industrial environments. Its main purpose is to provide support aimed at improving production efficiency and operational safety.
OWASP top10	Document published by the Open Worldwide Application Security Project (OWASP) containing the 10 most relevant vulnerabilities for web applications. The document is updated regularly.
PaaS	Platform as a Service – one of the models, along with IaaS and SaaS, of a cloud computing service in which the provider provides a development or software platform.

Penetration test	Penetration test (pentest) – a computer system security test for detecting vulnerabilities (weaknesses) of that system by attempting to replicate actions which might be performed by an attacker during an actual computer attack. Penetration tests can be conducted manually by a tester or in a semi-automated manner. They can use ready-made or specially prepared exploits, i.e., methods of exploiting vulnerabilities present in computer systems in order to perform an action desired by an attacker, most often the execution of a program prepared by the attacker or an increase in the attacker's privileges. A characteristic feature of penetration tests is that they do not just stop at finding vulnerabilities, but attempt to exploit them (to see if it is possible to 'break into' the system). Penetration tests can include activities in the form of physical security tests (getting a tester into an area protected by access control, e.g., a protected building), as well as socio-technical activities.
Phishing	A form of cyber attack that attempts to deceive or defraud internet users with sensitive information such as passwords, credit card numbers, personal details or other sensitive data. A phishing attack is usually conducted by cybercriminals who pretend to be an otherwise trustworthy source in order to mislead their victims and get them to divulge their confidential information.
PQ	Performance Qualification (PQ) – documented checks and confirmations that equipment and ancillary installations combined into a functional whole, can operate efficiently and repeatedly in accordance with the approved processing method and specifications.
Programming	The process of producing and further developing computer programs by formulating instructions that a computer can understand and execute. Programming is a fundamental part of computer science and involves the development of algorithms, i.e., sequences of logical steps that determine the actions a computer should perform.

Protection phase	Preparing and implementing appropriate safeguards to ensure correct service delivery and product operation.
Recovery phase	Analysing the incident, preparing and taking appropriate actions to implement emergency plans and restore functions or services that have been disrupted as a result of a cybersecurity incident.
Redteaming	A set of activities undertaken by a red team to simulate an attack on a specific organisation or part of its structure. Redteaming is aimed at checking the security level of an organisation and the correct operation of its security systems, both IT (e.g., anti-virus systems, data leakage prevention, firewalls, etc.), technical (access control systems, video surveillance) and organisational (properly prepared, implemented and followed security policies and procedures). Redteaming uses methods known from, but not limited to, penetration testing, physical security testing and social engineering testing. It is usually an activity more extended in time, scope and used techniques than penetration testing. Typically, the objective of redteaming is to gain access to a specific resource (e.g., to steal some information) or to reach a location under access control.
Response phase	Preparing and implementing appropriate actions to respond and react to a detected cybersecurity incident. This is a short-term and ad hoc action.

Reverse engineering	Reverse engineering/back engineering – all activities leading to the recovery of source code instructions from the compiled machine code (usually available in the form of executable files of analysed programs). Reverse engineering also makes it possible to reconstruct and determine the requirements and design solutions of the analysed software, operations performed, communication protocols used and algorithms applied. Reverse engineering can be conducted in order to audit the security of the analysed applications, to eliminate security features applied by software developers (e.g., copy blocking, system activation checking) or to try to develop one's own solution based on someone else's work. Reverse engineering may also involve devices (e.g., computer hardware) and communication protocols.
SaaS	Software as a Service – one of the models, alongside IaaS and PaaS, of a cloud computing service. The service provider hosts the customer's software.
Scanning	An activity that, after examining ports, IP addresses, hosts and networks, identifies active devices, recognises services and operating systems that are running and provides information about events that have occurred, e.g., vulnerabilities that have arisen or potential threats. Scanning also helps to recognise the network topology and configuration of accessed devices and identify open ports.
Script	A short computer program or set of instructions used to perform specific actions or tasks in an IT environment. Scripts can be used both for security purposes and for other aspects of system management or process automation. As a general rule, scripts are not compiled and do not require this to function.
Sector	One of the areas of the economy, e.g., energy, pharmaceuticals, etc. A sector is divided into branches.
Security copy	A set of data that, in the event of loss (e.g., virus attack, accidental deletion), will allow the original data to be restored.

Sniffing	Activities monitoring the flow of information on a network and analysing this information.
SOAR system	Security orchestration, automation and response (SOAR) system – three elements (orchestration, automation and response to incidents) working together to find and stop attacks. Orchestration is the bringing together of various internal and external tools in one central location to consolidate data and streamline processes through automation. Automation is the programming of tasks with appropriate procedures so that they are performed automatically. Response is reacting appropriately to possible threats and incidents. SOAR systems make it possible to respond more quickly and accurately to possible incidents and reduce the number of potential work safety problems.
SOC	Security Operations Center – a 24/7/365 service consisting of the operation of ICT systems and security experts. It allows hired specialists to analyse ICT assets from the point of view of their security and respond to any incidents that may arise.
Social engineering	Social engineering – the act of influencing people, the practical application of deception through the use of psychological means and methods of manipulation aimed at eliciting specific information or inducing the performance of specific actions. The aim of such action is the unauthorised acquisition of confidential or otherwise unavailable information. The basic methods of social engineering include, e.g., persuasion, manipulation and the intensification of fear.
Source code	Detailed instructions written by a programmer and understood by a programmer using a given programming language, the execution of which by the computer leads to the presentation of the results of operations on the available data.

SQL Injection attack classes	SQL Injection attacks rely on the exploitation of programming errors, mainly in scripting languages (PHP, ASP, etc.). These bugs consist of a lack of filtering the input data used for dynamically generated SQL queries, thus making it possible to alter all or part of the query to the database system. Exploiting the application's vulnerability to SQL injection attacks can lead to the disclosure of database content or its modification.
SSRF	Server-side request forgery (SSRF) is an exploit occurring when a web application retrieves data from external resources without validating the URL provided by the user. This allows an application to be forced to send a crafted payload (request) to an unexpected destination, even if it is on the local network or protected by a VPN, firewall or has an active ACL.
SSTI	Server-side template injection (SSTI) is an exploit allowing remote code execution through the preparation of suitably crafted input (payload) using the native syntax specific to the used template engine.
Supply chain	A network of actors involved in the creation, distribution and sale of products or services. It encompasses all stages of the process, from the sourcing of raw materials, production, warehousing, transport and sales, to the delivery of the product to the final customer.
System	An arrangement of two components working together, hardware and software, to achieve a goal. The system is made up of several layers: hardware, operating system, utilities, application programmes and the people who use it.
Vulnerability	A property of an information system, including an asset or security weakness, that can be exploited by cyber threats.
Web (Internet) applications	Browser-run programs that, through a designed interface, are intended to provide the user with a specific service provided by a server.

XSS attack classes	Cross site scripting (XSS) attacks involve injecting a piece of JavaScript code or other scripting language that can be run in the user's browser. As a result, the attacker has the ability to execute arbitrary scripting code in the browser, allowing the user's session cookies to be stolen and, consequently, their entire session to be intercepted.
XXE attack classes	XML external entities (XXE) attacks are conducted when parsing an XML document supplied from an external source. This is similar to an SQL Injection attack in that it takes place when processing XML containing references to external sources that will be loaded into the XML content.