Competency Pool

Here, we provide a list of competencies generated during the competency model analysis. By summarizing the coded segments, we formed thick descriptions for each competency. Table 1 shows the competencies. Note that we did not perform this step for the entire set of professional competencies. Rather, we focused on the first ten professional competencies of each knowledge area. For the non-professional competencies, a full is provided. For better readability, gender sensitive language has been omitted.

Table 1: List of generated competencies. For every competency, a description is provided. Furthermore, category frequencies for each competency (CF) are given.

#	Competency	CF	Description
			List of Personal Competencies
1	Lifelong Learning & Professional Development	4	The cyber security professional undertakes a variety of efforts to maintain and develop his competencies. He is committed to developing himself and improving his knowledge and skills. He shows interest in lifelong learning, can anticipate development needs and takes appropriate action.
2	Initiative	4	The cyber security professional is able to take initiative and may go beyond routine tasks.
3	Integrity	4	The cyber security professional acts according to moral principles and has a strong work ethic. The professional complies with the law and policies of the organization, is trustworthy and contributes to maintaining the integrity of the company.
4	Self-responsibility	3	The cyber security professional takes responsibility for his own decisions, mistakes, actions, and when needed also for the action of groups or teams.
5	Professionalism	3	The cyber security professional is able to present a professional image of himself and the company. He has a positive attitude towards his own work and maintains a private lifestyle that does not negatively affect his work at the workplace.
6	Flexibility	3	The cyber security professional acts flexibly and adapts to new situations. He is able to deal successfully with change and is open to new ideas.
7	Independence	2	The cyber security professional is able to work independently and develop his own working style. The professional is also able to work effectively under minimal supervision.
8	Dependability & Reliability	2	The cyber security professional acts dutifully. He acts predictably, fulfills obligations conscientiously and completes tasks on time. He/she is punctual and complies with organizational rules and guidelines.
9	Conscientiousness	2	The cyber security professional pays attention to detail, performs work thoroughly and handles tasks conscientiously. He makes sure that everything has been taken into account and is able to recognize and correct errors.
10	Persistence	2	The cyber security professional is able to work on a task with perseverance despite setbacks. Even under unfavourable circumstances, he is able to stick to a task and puts in extra effort to achieve goals on time.
11	Achievement Motivation	2	The cyber security professional is motivated to exceed standards and expectations. He has confidence in his abilities and is confident to succeed in the future.
12	Stress Tolerance	1	The cyber security professional is able to deal effectively with stressful situations (e.g. emergencies, deadlines, dangerous situations). He acts calmly and prudently in stressful situations.
13	Willingness	1	The cyber security professional shows a high level of commitment. He also works on tasks that may not excite him.
14	Self-control	1	The cyber security professional is able to control himself in complex stressful situations. He maintains composure and keeps his emotions in check. He is able to deal with criticism, accept it and learn from it.
15	Enthusiasm	1	The cyber security professional is enthusiastic about cyber security tasks and activities.
16	Stamina	1	The cyber security professional is able to exert himself for longer periods of time without tiring. He also manages repetitive tasks (e.g. data entry) without signs of fatigue.
17	Resilience	1	The cyber security professional is able to deal sensibly with pressure. He remains calm and optimistic in emergency situations. The cyber security expert is able to recover quickly from setbacks.
			List of Social Competencies
1	Teamwork	7	The cyber security professional is able to cooperate with others to achieve common goals. He sees himself as a team member and takes on the role assigned to him. He is able to identify the strengths and weaknesses of the team and encourages and supports others.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
2	Leadership	6	The cyber security professional is able to take on a leadership role. He adapts his leadership style to the circumstances, achieves effect and is interested in the growth of others. He gives constructive feedback and encourages others.
3	Communication	6	The cyber security professional is able to correctly interpret verbal and non-verbal parts of communication and to react accordingly. He listens actively and can communicate thoughts effectively. He adapts his communication style to the recipient.
4	Relationship Management	5	The cyber security professional makes efforts to develop and shape effective and productive relationships. He is able to maintain relationships and establishes a high level of credibility and trust with others.
5	Conflict Management	3	The cyber security professional is able to resolve conflicts and prevent negative consequences. He deals with differences in a constructive way and is able to withstand them. He is able to conduct constructive negotiations to find common solutions.
6	Empathy	3	The cyber security professional is empathetic, can put himself in the place of others and shows empathy towards others. He is interested in the problems of others and strives to help others.
7	Presentation Skills	2	The cyber security professional has strong presentation skills and is able to present content effectively and persuasively to an audience.
8	Diversity	2	The cyber security professional respects and values diversity. He is able to deal responsibly with big and small differences and is open-minded towards cultural diversity, gender identities and other characteristics.
9	Persuasion	2	The cyber security professional argues logically and convincingly and thus influences the views of others. He is able to present thoughts and ideas convincingly.
10	Fairness	1	The cyber security professional treats others fairly and generally acts fairly. He makes understandable decisions that are fair to all.
			List of Methodological Competencies
1	Analytic Thinking	5	The cyber security professional thinks logically. He analyzes, interprets and compares information, deriving rules and relationships. He is able to think inductively and deductively and, through analytical thinking, to successfully manage the work.
2	Problem Solving	4	The cyber security professional is able to identify problems and generate, evaluate and implement solutions. Based on what he has already learned, he develops and evaluates alternative solutions and decides on a solution approach.
3	Creative Thinking	4	The cyber security professional has a good imagination and is able to develop creative and innovative ideas and solutions. He is able to develop innovative methods and finds new approaches.
4	Decision Making	4	The cyber security professional is able to make decisions in ambiguous or poorly defined situations.The professional is able to assess the consequences of the decision taken.
5	Planning Skills	3	The cyber security professional designs, prioritizes and plans tasks, so that they are completed on time. The professional manages time well and develops, plans and implements strategies to achieve goals.
6	Perceptual Speed	2	The cyber security professional is able to understand and learn things and aspects quickly. He is able to quickly recognise details in different sources of information.
7	Knowledge Management	2	The cyber security professional obtains information using, for example, a computer. He is able to search, find and retrieve information. He practices source criticism, organizes information and uses an information management system.
8	Computational Thinking	1	No description available due to lack of coded material that gives insight into the content of this competency
9	Strategic Thinking	1	The cyber security professional is able to think strategically and formulates effective strategies.
10	Systemic Thinking	1	The cyber security professional is able to see the big picture and understands the parts of a system as a whole.
11	Spatial Orientation	1	The cyber security professional is able to orientate himself spatially. He understands relational spatial concepts and uses a map for orientation.
12	Learning Skills	1	The cyber security professional is able to use learning techniques effectively to acquire new knowledge and skills. He also uses other opportunities (e.g. feedback) to improve himself.
13	Design Thinking	1	The cyber security professional uses design thinking methods to guide stakeholders through the inspiration, brain storming and implementation phases.
			List of job-specific Skills
1	Technology Watching	7	The cyber security professional monitors emerging technology trends and developments. He conducts cost-benefit analysis and evaluates the trends and developments with regard to their relevance for the company. He develops innovative solution approaches for integrating new technologies into existing systems.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
2	Research	6	The cyber security professional understands scientific rules, principles and methods. He is able to apply scientific methods to solve problems and generate knowledge. He develops research questions, collects and evaluates data and publishes scientific papers.
3	Customer Service & Technical Support	5	The cyber security professional works with customers and clients to assess their needs, provide assistance, and troubleshoot (technical) issues and incidents. He implements customer support policies, standards and norms. He develops user manuals and advises on infrastructural upgrades.
4	Organizational Awareness & Business Skills	5	The cyber security professional understands the organization's mission, structure, the organizational strategies and functions. He is knowledgeable about the organization's position in the marketplace and the internal and external factors that affect the organization. He understands the business objectives and acts to support them.
5	Language Literacy	5	The cyber security professional is able to read with comprehension. He critically examines various documents and recognizes gaps and inconsistencies. He writes and composes documents and texts that are free of errors, logically structured and tailored to the target audience. He speaks and communicates verbally clearly and concisely.
6	Project Management	5	The cyber security professional is capable of managing a project. He plans, manages and coordinates the project and all necessary resources. He reacts to problems and informs all parties involved on an ongoing basis.
7	Mathematics	4	The cyber security professional is able to select and apply appropriate mathematical and statistical methods to solve a problem. He has basic mathematical knowledge and skills and higher mathematical knowledge (e.g. modeling and simulation techniques). He translates practical problems into mathematical expressions.
8	Information & Knowledge Management	4	The cyber security professional manages information and considers organizational policies when distributing knowledge. He manages and administers processes and tools that enable content to be documented, identified and accessed. He generates, preserves, innovates and disseminates business knowledge using appropriate tools.
9	Procurement Management	4	The cyber security professional is able to plan, execute and evaluate the procurement and purchasing of IT products, including IT security products. He ensures that the supplier is trustworthy and performs management tasks during the procurement process. He evaluates the effectiveness of the procurement process in meeting information security requirements.
10	Fundamental IT User Skills	4	The cyber security professional uses computers, databases, software applications and automated systems to solve problems. He is familiar with basic computer science terms and basic software applications.
			Physical Security
1	Physical Security Controls	6	The cyber security professional is able to apply various physical security controls to mitigate risk. He is able to protect organizations, physical facilities, data, people and equipment. He understands various deterrent, preventative and investigative controls and develops policies and procedures to mitigate physical threats.
2	Physical Security Design	3	The cyber security professional designs security plans related to physical security and environmental security, including security testing and contingency plans. He integrates physical security concepts into test plans, processes and exercises. He reviews construction projects to ensure physical security features are included.
3	Evaluation of Physical Security	2	The cyber security professional evaluates and assesses the overall effectiveness of physical and environmental security policies and controls, the effectiveness of security control testing and the effectiveness of performance measurement systems. He recommends improvement proposals as appropriate.
4	Physical Threat & Vulnerability Assessment	2	The cyber security professional conducts threat and vulnerability assessments to identify physical and environmental risks and vulnerabilities. If necessary, he updates the appropriate security controls.
5	Physical Security Management	2	The cyber security professional performs management activities in the area of physical security. He consults with security personnel in other areas to ensure a holistic approach to security. He obtains all necessary resources required to operate a security program. He ensures that change and improvement actions are implemented as needed.
			CyBOK Introduction
1	Fundamental Concepts	6	The cyber security professional understands and applies the security concepts of integrity, confidentiality and availability. He is able to determine whether and to what extent a breach of the security properties has occurred. He is aware of the societal dimension of cyber security and the importance of protecting data and information systems.
2	Security Architecture	5	The cyber security processional plans and designs security architectures and implements various security solutions. He embeds security principles into the architecture design to mitigate risks and defines security specifications of components. He understands the security issues of different technologies and their impact on the security architecture.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
3	Information Assurance	4	The cyber security professional understands the information assurance principles of integrity, confidentiality, availability, authentication and non-repudiation and can successfully apply them in a variety of contexts. He is able to protect data and information systems and maintain security properties.
			Physical Layer & Telecommunications Security
1	Protection of Telecommunications Systems	2	The cyber security professional develops countermeasures to protect telecommunications systems from unauthorized access and interception. He is able to limit the loss of confidentiality by using emission security principles. He is aware of various jamming techniques and their effects.
2	Telecommunications	2	The cyber security professional has fundamental knowledge in the field of telecommunications systems. He knows and understands different architectures and typologies as well as the associated components and protocols.
			Cyber-Physical Systems Security
1	Critical Infrastructure	2	The cyber security professional is aware of the cyber threats that threaten the security of a country's critical infrastructure and knows relevant protective measures, including legal measures.
2	Operational Technology Architecture	1	The cyber security professional understands the risks associated with OT architectures and takes countermeasures to mitigate risks. In addition, he has basic and specialized knowledge of OT architectures.
3	Cyber-Physical Systems & IoT	1	The cyber security professional knows and understands the specific cyber security challenges associated with cyber-physical systems and IoT. He is aware of the peculiarities of cyber-physical systems and the resulting implications with regard to cyber security.
4	Embedded Computers	1	The cyber security professional understands the application of various specialized computer systems used to control devices (e.g. motor vehicles and helicopters) and is proficient in the appropriate programming languages.
			Hardware Security
1	Hardware Testing	3	The cyber security professional is able to test different types of hardware. He verifies the integrity, availability, efficiency and functionality of the hardware system and assesses the adherence to compliance rules.
2	Secure Hardware Design	3	The cyber security professional is able to create hardware designs that meet cyber security requirements. He ensures that the various requirements, such as security, functionality and quality, are appropriately balanced.
3	Hardware Problems	3	The cyber security professional is able to troubleshoot hardware issues. Furthermore, he has basic and specialized knowledge in the field of hardware.
			Network Security
1	Network Defense	15	The cyber security professional designs, maintains, installs and applies a range of network defense systems, including firewalls, intrusion detection systems (IDS), network monitoring, network hardening, network access controls and grid sensors to detect and respond to threats and protect networks and network traffic. He detects potential conflicts between systems and reports daily on network events.
2	Network Design	5	The cyber security professional understands network design processes and associated security objectives and operational goals. He is aware of potential trade-offs between objectives. He develops network designs and network design guidelines. He takes responsibility for key aspects of network design within an organization.
3	Network Protocols	5	The cyber security professional uses secure protocols to protect data and ensure secure communication. He knows the secure equivalents (e.g. SSH, SFTP, SLL) of the insecure protocols and can use them successfully.
4	Network Vulnerabilities	4	The cyber security professional monitors, identifies, evaluates, mitigates and patches network vulnerabilities. He is aware of various vulnerabilities that are specific to network infrastructures. He ensures that solutions are implemented to eliminate or mitigate network vulnerabilities.
5	Network Skills 4		The cyber security professional configures various network devices (e.g. switches and routers), diagnoses network connectivity issues and integrates new systems into existing network architectures. In addition, he has a broad knowledge of network technology.
6	Wireless Network Security	3	The cyber security professional is familiar with the key principles and concepts of wireless network security. He is aware of a wide variety of security problems that can arise in conjunction with wireless networks.
7	Network Security Evaluation	3	The cyber security professional evaluates network security, identifies risks and recommends appropriate countermeasures. He evaluates the achieved effects of policies and security controls and prepares a report regarding the performance of network security.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
8	Network Security Management	3	The cyber security professional is able to establish network security programs that are in alignment with the organization's vision and goals. He manages all resources necessary to establish and preserve the program. He defines the scope of the program and ensures that all compliance regulations are met.
9	Network Security Strategy & Policy	2	The cyber security professional develops and implements network security strategies and policies that are in compliance with various standards, regulations and laws.
10	Network Administration & Maintenance	1	The cyber security professional monitors the network to ensure optimal levels of network performance and minimization of downtime. He is able to detect, isolate and resolve network faults. Furthermore, he is able to optimize network performance.
			Authentication, Authorisation & Accountability
1	Authentication & Authorisation	10	The cyber security professional creates authentication and authorization systems that allow users to access data based on assigned privileges and permissions. He implements appropriate access controls and permissions, understands the relationship between authentication and authorization and favors multi-factor authentication.
2	Identity & Access Management	9	The cyber security professional uses identity management solutions and manages user accounts and access rights. He is able to grant the right people the right access and to deny access to unauthorized people. He understands the need to delete expired accounts and change passwords regularly.
			Distributed Systems Security
1	Distributed Systems	4	The cyber security professional knows and applies the principles, concepts and tools underlying distributed computing systems. He can assess the security implications and risks of distributed systems.
2	Cloud Security	3	The cyber security professional is familiar with security concepts concerning cloud solutions and can apply them successfully. He ensures that security requirements are implemented in cloud services. He knows various vulnerabilities, risks and threats that specifically affect cloud services and recommends security models and controls to mitigate risks.
3	Digital Currencies	1	The cyber security professional implements digital currency extensions using relevant scripting languages. He identifies security issues in the implementation of existing cryptocurrencies and is able to design e-commerce applications.
			Operating Systems & Virtualization Security
1	Understanding of Operating Systems & Virtualization	7	The cyber security professional is familiar with various virtualization technologies and concepts and their advantages. He analyzes virtualization concepts with regard to relevant security aspects. He is familiar with current operating systems and can handle file systems efficiently.
2	Database Administration	4	The cyber security professional uses, manages and evaluates database tools. He handles database configurations, reconfigurations and installations. He monitors and optimizes the performance of databases.
3	Secure Operating Systems	2	The cyber security professional is able to design operating systems that meet cyber security requirements. He is familiar with the security features and functions of operating systems and applies a range of security controls (e.g. hardening) to mitigate risks.
			Cryptography
1	Encryption	7	The cyber security professional knows the various application fields (e.g. data encryption, hard disk encryption) of encryption technologies. He applies appropriate encryption methods to protect data in motion and at rest and ensures that data remains confidential.
2	Cryptographic Understanding	3	The cyber security professional knows and grasps core concepts of cryptography and key management, is familiar with the ideas of information theory and the key cryptographic concepts (e.g. symmetric and asymmetric encryption, PKI, etc.).
			Secure Software Lifecycle
1	Software Testing	11	The cyber security professional identifies test objects, selects appropriate software testing techniques (e.g. module tests, integration tests, system tests) and develops, implements and executes test cases. He tests software to verify quality and compliance and decides on the execution of automated software tests.
2	Secure Design	11	The cyber security professional uses secure design patterns and follows recommended design principles to create secure systems. He understands, evaluates, compares and applies a set of secure design principles (e.g. open design, isolation, mediation, least privileged). He performs threat modeling and identifies the attack surface of systems. He is able to incorporate various security strategies (e.g. defense-in-depth, access control mechanisms, encryption of sensitive data) into the design and ensures a balance between security, functional and quality requirements.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
3	Secure Development	11	The cyber security professional considers security requirements during the development of a system and implements and updates secure systems, products and components. He defines and implements secure development standards and practices. He selects test strategies and verifies the extent to which the system meets security requirements. He implements processes to ensure that the required level of security of a system is maintained throughout its life cycle. He uses version management systems during the development of systems and documents the development processes.
4	System Requirements	10	The cyber security professional identifies, analyzes and designs functional and non-functional requirements and specifies the security requirements of a system. He consults with customers to identify functional requirements and translates these requirements into technical solutions. He performs initial threat modeling and identifies risks.
5	Security Testing	9	The cyber security professional develops guidelines for security testing, creates test plans, defines test items, determines the scope of testing, prepares the security test and implements and performs security testing. He is able to evaluate test results and decides if countermeasures need to be initiated. He performs code reviews to identify vulnerabilities.
6	Software Configuration Management	7	The cyber security professional plans and prepares software configuration management activities. He designs data and code repositories, develops and manages software configuration management libraries and develops a software configuration management plan. He performs software configuration management activities and follows the software configuration management plan. He develops software release plans and performs software releases.
7	Software Test Planning	7	The cyber security professional develops and implements software test plans, including module test plans and integration test plans. He defines success and failure criteria for various software testing techniques, determines completion criteria for software testing and defines the objectives of the test. He identifies all stakeholders involved and organizes the test team.
8	Patch Management	6	The cyber security professional corrects vulnerabilities and implements patches. He distinguishes between patches and updates and is aware that patches themselves can produce new vulnerabilities and problems. He performs manual updates and patches and automates patches and updates for specific sub-areas.
9	Software Testing Infrastructure	5	The cyber security professional is able to select, document and implement appropriate test tools needed during the software testing process. He decides on the type of documentation and is able to develop, select and implement test environments.
10	Software Testing Measurement & Defect Tracking	5	The cyber security professional collects and stores data from the test and performs root cause analysis. He evaluates and analyzes the results of the software test. He identifies and performs necessary corrective actions, if required. He reports the results, evaluates the effectiveness of the test and decides on further actions (e.g. additional testing).
			Software Security
1	Prevention of Software Vulnerabilities	10	The cyber security professional practices defensive and secure programming and uses secure programming languages to prevent the introduction of software vulnerabilities. He is aware of the consequences associated with disregarding the rules for secure and defensive programming. He is able to develop new guidelines for safe programming and to review and approve guidelines.
2	Detection of Software Vulnerabilities	6	The cyber security professional is able to select and apply appropriate static and dynamic analysis methods to detect software vulnerabilities. He uses static and dynamic analysis methods to identify vulnerabilities in software applications and recommends countermeasures as needed. He develops protocols and other measures to help mitigate risks and reduce exploitable software vulnerabilities.
3	Software Security Evaluation & Vulnerability Assessments	5	The cyber security professional conducts security evaluations of software systems. He evaluates software by analyzing the design documentation and code to identify potential vulnerabilities. He tests whether and to what extent these vulnerabilities can be exploited. He conducts vulnerability and threat assessments, prepares reports of findings and recommends countermeasures as needed.
4	Programming Skills	3	The cyber security professional uses a number of programming languages to solve problems. He knows well-known programming languages and their fields of application.
5	Application Security Controls	3	The cyber security professional continuously ensures that the software application security controls have been implemented correctly and are demonstrating effectiveness. He writes reports (e.g. POA&M) regarding the security controls that have not been implemented correctly.
6	Software Security Assessment Process	2	The cyber security professional collects and monitors metrics for the security assessment process, following specific standards.
			Web & Mobile Security

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
1	Web & Mobile Defense	6	The cyber security professional is able to secure web and mobile applications and defend them against known attacks. He is able to implement security controls for mobile devices and test them for effectiveness. He protects web servers and takes appropriate measures to ensure that user input does not affect server-side processes.
2	Secure Web Usage	4	The cyber security professional is aware of the risks associated with social media and can initiate appropriate countermeasures. He is aware that surfing on dubious websites can have negative effects on privacy and security.
3	Web & Mobile Vulnerabilities	1	The cyber security professional is familiar with various vulnerabilities, threats and risks that affect mobile devices in particular.
4	Server Attacks	1	The cyber security professional is able to perform buffer overflow attacks and cross-site scripting attacks against a server.
			Forensics
1	Digital Forensics	12	The cyber security professional collects, processes, preserves, analyzes and presents forensic evidence to support security vulnerability mitigation and/or criminal, intelligence or law enforcement investigations. He is able to secure the crime scene and identifies evidence in the most effective manner and in accordance with guidelines so that there is minimal disruption to business and the evidentiary content is preserved.
2	Computer Forensics	7	The cyber security professional is able to solve cyber crimes and security breaches using forensic methods. He is able to recover data. He examines recovered data and uses forensic analysis to examine file systems. He is able to create forensically sound duplicates of evidence and ensures that the original evidence is not inadvertently modified in any way.
3	Network Forensics	6	The cyber security professional is able to investigate network security breaches using forensic methods. He determines the extent to which network security policies have been violated, assesses the consequences and secures evidence as needed. Furthermore, he is able to reconstruct a malicious attack based on network traffic.
4	Criminal Investigations	4	The cyber security professional is able to secure crime scenes. He collects and secures evidence that can be used to prosecute computer crimes. He is able to determine the extent to which a security incident constitutes a violation of law and responds accordingly. He assists law enforcement agencies and explains details as needed.
5	Cloud Forensics	1	The cyber security professional is aware that forensic analysis of cloud systems have particular demands. He is able to propose and successfully apply various analysis methods.
6	Evaluation of Forensic Activities	1	The cyber security professional reviews all documentation related to forensic processes and outcomes for accuracy, applicability and completeness. He evaluates the effectiveness, adequacy and accuracy of the forensic team's analysis processes and assesses the fitness of personnel. He is able to suggest appropriate improvement actions as needed based on the evaluation processes.
7	Forensic Program Management	1	The cyber security professional manages all resources necessary to operate a forensic laboratory and program. He builds a forensic team, oversees the forensic program and ensures that necessary innovations, changes and improvements are implemented.
8	Mobile Forensics	1	The cyber security professional is able to perform forensic analysis of mobile devices. He is able to create an inventory of the files on a mobile device and use forensic tools specifically designed for mobile operating systems.
			Adversarial Behaviours
1	Characterisation of Adversaries & Defence	5	The cyber security professional knows and identifies the various tactics, techniques and methods of adversaries. He is able to draw conclusions regarding the motivations of adversaries based on analysis. He formulates strategies to defend against actions by state-sponsored attackers, hackers, activists, organized crime and other adversaries.
2	Cyber Threat Analysis	2	The cyber security professional is able to identify and assess the capabilities and activities of cyber criminals and foreign intelligence agencies using a variety of tools. He supports law enforcement and counterintelligence activities through the production of intelligence.
3	Social Engineering	1	The cyber security professional is aware of the threats and dangers posed by social engineering attacks. He is able to expose various methods of social engineering, such as pretexting or phishing.
			Malware & Attack Technologies
1	Malware Detection	8	The cyber security professional is able to detect malware. He performs virus scans, ensures that antivirus systems are functioning properly and debugs systems to determine the presence of malware. When performing analysis, he considers the benefits and limitations of behavioral and signature-based antivirus technologies. He is aware that malware can circumvent security systems through deception.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
2	Malware Analysis & Defence	6	The cyber security professional is able to analyze the behavior, capabilities, interactions, intentions, features and characteristics of malicious software and threats. He is also able to develop and successfully apply defense and mitigation strategies and techniques to combat malware. He performs static and dynamic analysis and isolates and removes malware.
3	Awareness of Attacks	4	The cyber security professional is familiar with the attack vectors used by intruders, the various stages of an attack and different classes of attacks used to compromise systems.
			Security Operations & Incident Management
1	Incident Management	18	The cyber security professional takes precautionary measures and ensures that well-trained staff, tools and diagnostic equipment are available to deal with emergencies. He defines and implements processes and procedures for incident detection and investigation. He is able to identify security incidents and responds to them in a timely manner to restore normal operations as quickly as possible. He makes immediate efforts to mitigate the damage, assess the impact, remediate and resolve the incident. He evaluates and improves incident management as needed.
2	Vulnerability Assessment	14	The cyber security professional knows various principles, methods and tools for conducting vulnerability assessments. He performs vulnerability assessments using appropriate methods and tools to identify weaknesses and gaps in the system. He recommends and develops appropriate countermeasures based on the test results.
3	Intrusion Detection & Analysis	13	The cyber security professional monitors network and system activity to detect potential intrusion and other anomalous behavior. He analyzes information, derives appropriate countermeasures and provides escalation in case of emergency. He is able to distinguish attacks from normal user behavior on a network and understands the difficulties associated with zero-day attacks and the use of signature-based attack detection systems.
4	Security Audits	12	The cyber security professional plans, implements and conducts internal and external security audits to determine, if information systems and processes meet security criteria and, if security controls are implemented correctly and are operating according to expectations. He audits the extent to which legal and other requirements are met. He establishes audit plans and strategies and prepares for audits. He documents security audit findings and recommends corrective actions as needed.
5	Security Controls	11	The cyber security professional selects and implements security controls based on risk analysis to mitigate risks. He periodically evaluates the effectiveness and performance of the security controls and ensures that the security controls have been implemented effectively. He is able to monitor the use of security controls and develops strategies to monitor the effectiveness of security controls.
6	Penetration Testing	10	The cyber security professional coordinates, plans, implements and conducts penetration testing. He is able to assess vulnerabilities and their potential for exploitation by demonstrating how an adversary can either undermine the organization's security objectives or achieve specific adversary goals. He is able to identify deep risks associated with (exploitable) vulnerabilities. He prepares reports, communicates test results and recommends mitigation options based on the test results. He is aware of the difference between vulnerability assessments and penetration testing and is familiar with the opportunities and limitations of penetration testing.
7	Configuration Management	8	The cyber security professional identifies and determines all IT assets, determines their relationship to business processes and classifies assets in a configuration management database. He implements and manages the database and protects the confidentiality, availability and integrity of the database. He identifies, classifies and specifies configuration items and their relationships to each other. He defines naming conventions and attributes of configuration items. He regularly verifies that the information in the database is complete and that the configuration items are mapped correctly.
8	Backup & Recovery	8	The cyber security professional prepares for incidents, disasters and other problems by identifying ways and means of backing up and restoring data. He is able to back up data to storage media and is familiar with a range of storage media and solutions. He believes in the importance of reliable and efficient data backup and designs and develops backup and recovery processes.
9	Secure Operations & Service Delivery	8	The cyber security professional takes proactive steps to ensure a stable and secure application and ICT infrastructure and to avoid potential service interruptions wherever possible. He analyzes performance data and recommends measures to improve the reliability of services. He ensures secure configuration and maintenance of information, control, communications and security equipment and components. He is able to perform routine security operations such as patching, access rights management and vulnerability assessments.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
10	Continuous Monitoring	6	The cyber security professional develops and implements continuous monitoring processes and tools to assess risks on an ongoing basis. He is able to evaluate and integrate a continuous monitoring program into existing organizational security structures. He establishes situational awareness of risk levels through the use of data derived from continuous monitoring tools. He takes responsibility for the management and implementation of a continuous monitoring program.
			Privacy & Online Rights
1	Data Security	10	The cyber security professional is able to ensure data security and the availability, integrity, confidentiality and privacy of data on all media throughout the data lifecycle. He determines the appropriate level of protection for data, develops data security policies and procedures for collecting sensitive data and addresses privacy breaches when needed. He evaluates the effectiveness of various data security controls and takes appropriate action.
2	Technology & Privacy	3	The cyber security professional ensures that the privacy of individuals is preserved and not undermined through the use of technologies. He is aware of data security problems in relation to technologies. Furthermore, he monitors technological developments in the field of data protection and privacy.
3	Personal Information	2	The cyber security professional handles personal information responsibly. He understands the role and limitations of encryption technologies with regard to the protection of personal information. He is aware that there are major tensions and inherent conflicts between personal data protection and the security property of authenticity and non-repudiation.
4	Privacy Policies	2	The cyber security professional develops, implements and maintains an organization's privacy policies. He ensures that all newly developed products comply with privacy policies. He is able to establish an office to address complaints related to an organization's privacy policies.
5	Privacy Impact Assessment	2	The cyber security professional conducts privacy impact assessments to prevent privacy risks and to determine how personal information is collected, shared, used and preserved.
6	Privacy Management	1	The cyber security professional oversees data privacy programs. He responds to legal, regulatory, and organizational changes and revises the data privacy program when needed. He reviews all relevant security plans and ensures that privacy and information security activities are aligned.
7	Anonymity Systems	1	The cyber security professional is aware of the strengths and limitations of current anonymous communication and payment systems. He uses anonymity systems (e.g. Tor) to ensure anonymity.
8	Data Protection Management	1	The cyber security professional is able to develop and implement data protection management programs. He formulates a company's data protection strategy and ensures the effectiveness of the data protection management program.
			Law & Regulations
1	Legal & Regulatory Compliance	13	The cyber security professional ensures that the organization complies with information security and privacy laws, regulations, standards and policies. He establishes, manages and oversees an organization's information security compliance program. He evaluates and reviews the effectiveness of various compliance activities, conducts audits and updates company compliance policies as needed to ensure compliance with laws and regulations.
2	Legal & Regulatory Environment	10	The cyber security professional is familiar with the legal and regulatory environment in which the company operates. He knows the most important legal and regulatory instruments (e.g. the General Data Protection Regulation), observes legislative changes and trends and assesses the consequences for the company and cyber security in general. He is able to interpret laws and regulations and apply them to specific cases.
3	Intellectual Property & Licensing	4	The cyber security professional protects intellectual property and copyrighted information, does not violate intellectual property law and drafts rules in dealing with intellectual property. In addition, he is able to ensure that software is properly licensed before installation.
4	(Data-)Ethics & Integrity	4	The cyber security professional acts according to ethical principles, especially in the collection, use, storage and disposal of data. He can deal with ethical dilemmas and is convinced that those who can help are also obliged to help respectively should help. He follows legal and ethical principles in the creation and maintenance of software systems.
5	Contracts	3	The cyber security professional is able to negotiate and complete contracts. He reviews contracts to ensure that all compliance requirements are met.
6	Privacy & Organizations	1	The cyber security professional represents the organization's privacy interests, oversees the organization's privacy program and maintains relationships with external stakeholders dealing with privacy issues. He handles the organization's public relations regarding privacy.
			Human Factors

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
1	Cyber Security Awareness & Development	14	The cyber security professional ensures that information and cyber security awareness of all employees is strengthened and that other cyber security professionals expand their competencies. He is able to diagnose competencies of individuals and groups. He contributes to improving security awareness by providing supportive, interactive learning environments and using innovative teaching methods.
2	SA&E Policy and Content Development	11	The cyber security professional develops training guidelines and policies regarding cyber security awareness. He develops, designs, plans, elaborates and updates a wide variety of instructional materials, training programs, lessons and curricula. He assists other skill providers in the development of security awareness instructional materials and programs.
3	Personnel Security	8	The cyber security professional applies a set of personnel security controls to prevent and detect employee security breaches (e.g. misuse of information). He is aware of the inherent risk posed by employees and insiders and conducts background checks. He ensures that the selection and use of human capital contributes to overall security.
4	Security Awareness & Training Program Management	7	The cyber security professional recognizes when there is a need for security awareness and training programs. He is able to convince other stakeholders of the usefulness of such programs. He establishes security awareness and training programs and oversees, directs, assesses and maintains these programs. He ensures that such programs are consistent with the organization's business objectives and that relevant standards and requirements are met.
5	Evaluation of Security Awareness & Training Programs	6	The cyber security professional evaluates the effectiveness of the training program and verifies the extent to which the program covers all relevant and current topics. He evaluates and checks whether and to what extent the program complies with laws, regulations and company guidelines. He reviews course content for accuracy, completeness and timeliness and recommends changes based on findings.
6	Cyber Workforce Management	3	The cyber security professional performs a range of human resource management activities (e.g. performance management). He ensures appropriate and effective allocation and distribution of human resources. He creates standardized position descriptions based on established cyber job roles and develops and evaluates recruiting, hiring and retention processes. He creates, manages, implements and evaluates human resource management programs and ensures that the program meets relevant regulatory and organizational requirements.
7	Usable Security	2	The cyber security professional studies human behavior, capabilities and limitations. He uses these insights when creating security systems to ensure effective use by humans. He understands the role of usability in creating security systems and mechanisms. He is able to design user interfaces for security systems and considers whether and to what extent security policies take the human factor into account.
			Risk Management & Governance
1	Risk Management	20	The cyber security professional implements risk management using various risk management policies and procedures. He develops risk management policies and controls with consideration of business requirements and risk assessments. He develops balanced approaches to identify and assess risks. He develops appropriate mitigation strategies to ensure required security at affordable cost. He decides on appropriate actions required to adjust security and address risks.
2	Risk Assessment	19	The cyber security professional performs risk assessments at regular intervals and after major changes. Based on the results, he recommends various security strategies to mitigate the identified risks. He is able to improve risk assessment processes and adapt them to different contexts. He informs the appropriate stakeholders about the identified risks and issues.
3	Business Continuity Management	12	The cyber security professional creates and tests continuity plans to ensure that an organization continues to function in the case of a catastrophic event. He develops and designs contingency plans and is able to implement and maintain business continuity management processes and functions. He evaluates business continuity management and recommends improvements as needed. He reviews test, training and exercise results to improve processes and recommend changes as needed.
4	Cyber & Information Security Policy	11	The cyber security professional develops and maintains organizational cyber and information security policies, standards and processes using recognized standards (e.g. ISO/IEC 27000 family, Security Policy Framework) as appropriate. He is able to apply cyber and information security standards and policies within an organization, program, project or operation. He incorporates new changes into policies and evaluates security policies.
5	Information Security Strategy	10	The cyber security professional develops, determines and establishes the organization's security vision, goals, strategy and initiatives to protect assets and mitigate risk. He is able to develop and implement an information security strategy.

Table 1: List of generated competencies (continue).

#	Competency	CF	Description
6	Disaster Recovery Plannning	9	The cyber security professional is able to design, develop and implement disaster recovery plans. He clarifies the recovery actions and backup processes in the disaster recovery plan, verifies the accuracy of the plans and organizes the dissemination and distribution of the plans.
7	Business Continuity Planning	9	The cyber security professional is convinced of the need for an business continuity plan and accompanies the design, development and implementation of business continuity plans. He is aware of how business continuity plans contribute to cyber and information security.
8	Disaster Recovery Management	8	The cyber security professional implements disaster recovery processes and capabilities and executes disaster recovery plans. He is able to ensure rapid recovery of data, systems and services in the event of a disaster.
9	Threat Assessment	6	The cyber security professional conducts threat assessments to identify security risks and to create a security risk profile. He determines the extent of the threat and recommends measures to mitigate risks.
10	Enterprise Security Architecture	5	The cyber security professional helps develop an enterprise information security architecture and works with enterprise architects. He is convinced that enterprise-focused security architectures help mitigate risk. He develops robust and fault-tolerant security measures that match the perceived level of risk.