Competency Model for Information and Cyber Security Professionals

Here, the competency model for information and cyber security professionals is presented. A graphical elaboration of the model is given in Figure 1. Table 1 provides key data on the competency model. Therein included is information on the uses, goals, and target groups of the model. The model itself is presented in Table 2. As indicated by Figure 1, the high-level structure is formed by the four competency classes. The professional competency class is further divided into several subareas, which provide a suitable structure for organizing the competencies.

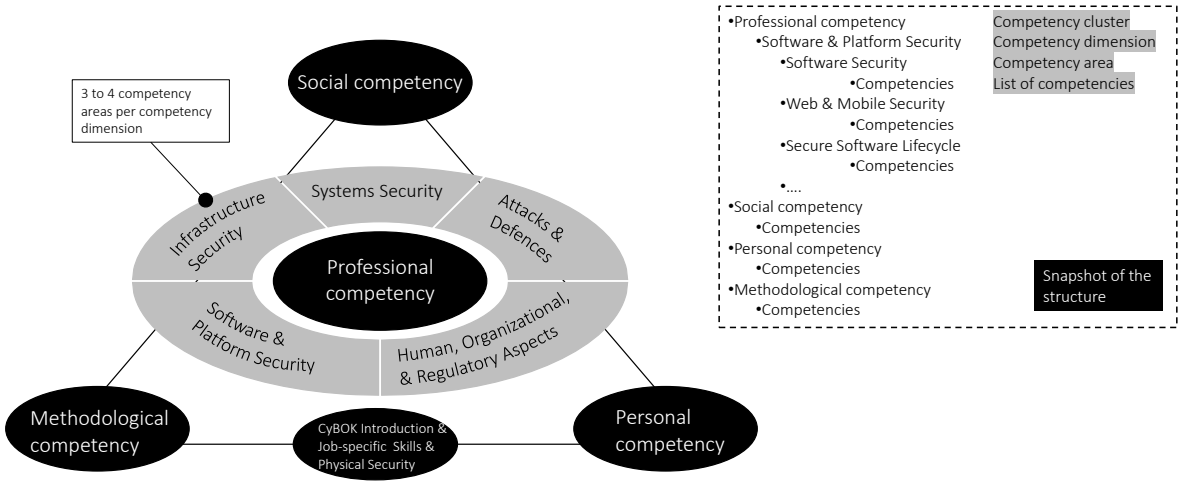


Figure 1: Overview and structure of the competency model for information and cyber security professionals.

Table 1: Description of the competency model.

Key Information of the Competency Model.	
Target groups	IT & cyber security experts, educational researchers, students, HR experts, curriculum developers, organizations
Goals	Ensuring a competent workforce; providing a flexible framework for different contexts; revitalizing and strengthen the training landscape; strengthening the profession; supporting organizations in HR management.
Uses	Learning & competency development; assessment; development & evaluation of qualification programs; recruitment & selection; performance management and many more uses that are included in the generated list of uses.
Competency classes / cluster	Professional, methodological, social and personal competency
Number of competency areas	24
Number of competencies	72
Defintion of the concept of competency	Competencies are the cognitive abilities and skills possessed by or able to be learned by individuals that enable them to solve particular problems, as well as the motivational, volitional and social readiness and capacity to use the solutions successfully and responsibly in variable situations [1, pp. 27-28].
Competency anatomy	The competency anatomy consists of the competency name, a definition, and between 2 and 6 behavioral indicators.
Behavioural indicators	Yes
Proficiency levels	The three sectors under each competency do not represent competence levels. Rather, they are used to organize the indicators.
Scope	The competency model for information and cyber security professionals includes competencies from all CyBOK knowledge areas and thus fully covers the domain of information and cyber security. Additionally, competencies from all four competency classes are included. Also, professional competencies beyond the security domain are incorporated.
Extendable	The competencies from the generated pool can be used as extensions.
Language	English

Table 2: The competency model for information and cyber security professionals.

Social Competency		
Teamwork		
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.		
Shows loyalty to the team.	Identifies with the team and its goals.	Uses a group approach to identify problems and develops solutions based on group consensus.
Accepts membership in the team and commits to the goals of the team.	Works as part of a team, contributing to the group's effort to achieve goals.	Chooses behaviors and actions that best support the team and accomplishment of work tasks.
Leadership		
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.		
Serves as a leader.	Creates and leads formal, informal or virtual teams and/or creates collaborative links with related teams.	Motivates others.
Leads small groups/teams with delegated authority for a limited range of tasks.	Adapts leadership styles to a variety of situations.	Provides technical leadership in a professional field, either within an organisation or across an industry sector.
Communication		
The cyber security expert is able to correctly interpret verbal and non-verbal parts of communication and react accordingly. He listens actively and can communicate thoughts effectively. He adapts his communication style to the recipient.		
Expresses information (for example, ideas or facts) to individuals or groups effectively, taking into account the audience and nature of the information (for example, technical, sensitive, controversial).	Applies active listening skills using reflection, restatement, questioning, and clarification.	Expresses relevant information appropriately to individuals or groups taking into account the audience and the nature of the information (e.g. technical or controversial).
Conveys information clearly, correctly, and succinctly.	Effectively uses eye contact and non-verbal expression.	Maintains open lines of communication with others.
Personal Competency		
Lifelong Learning & Professional Development		
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.		
Demonstrates an interest in personal and professional lifelong learning and development.	Seeks feedback from multiple sources about how to improve and develop.	Modifies behavior based on feedback or self-analysis of past mistakes.

Table 2: The competency model for information and cyber security professionals (Continue).

Recognises the value of Continued Professional Development (CPD) to the Information Security profession.	Regularly takes steps to improve and update own skills sets.	Maintains level of knowledge for professional certifications, accreditations and/or qualifications gained.
Initiative		
The cyber security professional is able to take the initiative and may go beyond routine tasks.		
Goes beyond the routine demands of the job.	Takes initiative in seeking out new work challenges and increasing the variety and scope of one's job.	Provides suggestions for innovative approaches to improve processes or tasks.
Displays a high level of initiative.	Takes initiative.	Seeks opportunities to influence events and originate action.
Integrity		
The cyber security professional acts according to moral principles and has a strong work ethic. The professional complies with the laws and policies of the organization, is trustworthy, and contributes to maintaining the integrity of the company.		
Displays strong moral principles and work ethic.	Behaves ethically.	Encourages others to behave ethically.
Displays high standards of ethical conduct and understands the impact of violating these standards on an organization, self, and others.	Understands that behaving ethically may go beyond what the law requires.	Uses company time and property responsibly.
Methodological Competency		
Analytic Thinking		
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.		
Possess sufficient inductive, and deductive reasoning ability to perform job successfully.	Critically reviews, analyzes, synthesizes, compares, and interprets information.	Draws conclusions from relevant and/or missing information.
Uses logic and reasoning to identify strengths and weaknesses of alternate solutions or approaches to a problem.	Identifies connections between issues.	Analyzes information and makes correct inferences or draws accurate conclusions.
Problem Solving		
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.		
Identifies the Problem.	Identifies the true nature of the problem and defines critical issues.	Integrates previously learned and externally obtained information to generate a variety of high-quality alternative approaches to the problem.

Table 2: The competency model for information and cyber security professionals (Continue).

Decisively chooses the best solution after evaluating the relative merits of each possible option.	Documents the problem and corrective actions taken and their outcomes and communicates these to the appropriate parties.	Develops a realistic approach for implementing the chosen solution.
Creative Thinking		
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.		
Generates innovative and creative solutions.	Uses original analyses and generates new, innovative ideas in complex areas.	Develops innovative methods of obtaining or using resources when insufficient resources are available.
Reframes problems in a different light to find fresh approaches.	Uses imagination to develop new insights into situations and applies innovative solutions to problems.	Entertains wide-ranging possibilities and perspectives to develop new solutions.
Professional Competency		
Job-specific skills		
Technology Watching		
The cyber security professional monitors emerging technology trends and developments. He conducts cost-benefit analyses 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.		
Explores latest ICT technological developments to establish understanding of evolving technologies.	Devises innovative solutions for integration of new technology into existing products, applications or services or for the creation of new solutions.	Exploits wide ranging specialist knowledge of new and emerging technologies, coupled with a deep understanding of the business, to envision and articulate the solutions of the future.
Provides expert guidance and advice, to the leadership teams in business and in technology, about potential innovations to support strategic decision-making.	Understands new and emerging IT and information security technologies.	Conducts research and identifies opportunities for new and emerging technology to support the business.
Research		
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.		
Understands basic scientific principles and uses appropriate technology.	Understands the scientific method (i.e. identify problem, collect information, form opinion and draw conclusions).	Understands overall intent and proper procedures for set-up and operation of equipment.

Table 2: The competency model for information and cyber security professionals (Continue).

Applies basic scientific principles and technology to complete tasks.	Formulates scientifically investigable questions, constructs investigations, collects and evaluates data and develops scientific recommendations based on findings.	Conducts original investigation in order to gain knowledge and understanding relating to Information Security.
Customer Service & Technical Support		
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.		
Provides services to end users by systematically identifying, classifying and troubleshooting technical issues and incidents that disrupt and impact their day-to-day business activities, within a specified timeframe.	Analyses issues or incidents encountered by users and conduct troubleshooting, and roll out upgrades.	Develops plans and retains accountability for maximising service quality, speed and availability in infrastructure administration and support activities.
Works with clients and customers to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations.	Provides end user information security support.	Coordinates and ensures end user support for all infrastructure applications and operations.
Physical Security		
Physical Security Controls		
The cyber security professional is able to apply various physical security controls to mitigate risk and 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.		
Explains the impact and proper use of environmental controls.	Explains the importance and application of physical security measures.	Protects an organization from natural or man-made threats.
Applies physical and environmental controls in support of physical and environmental security plans.	Develops countermeasures against identified risks and vulnerabilities.	Assesses effectiveness of physical and environmental security control testing.
Physical Security Design		
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.		
Develops a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions.	Integrates physical security concepts into test plans, procedures and exercises.	Reviews construction projects to ensure that appropriate physical security and protective design features are incorporated into their design.

Table 2: The competency model for information and cyber security professionals (Continue).

Develops criteria for inclusion in the acquisition of facilities, equipment, and services that impact physical security.	Identifies the physical security program requirements and specifications in relationship to enterprise security goals.	Compiles, analyzes and reports performance measures.
Evaluation of Physical Security		
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.		
Assesses and evaluates the overall effectiveness of environmental security policy and controls in coordination with the responsible organization and make recommendations for improvement	Assesses effectiveness of physical and environmental security control testing	Evaluates acquisitions that have physical security implications and report findings to management
Assesses the accuracy and effectiveness of the physical security performance measurement system and makes recommendations for improvement where applicable	Compiles, analyzes and reports performance measures	Assesses and evaluates the overall effectiveness of physical security policy and controls and makes recommendations for improvement
CyBOK Introduction		
Fundamental Concepts		
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.		
Distinguishes between data in use, data in motion (transit) and data at rest.	Explains the importance of information security, assurance and privacy to individuals, organizations, industries, and societies.	Explains concepts of Confidentiality, Integrity, and Availability (CIA).
Explains the concepts of confidentiality, integrity, and availability as applied to Information Systems Security.	Analyzes the trade-offs of balancing key security properties (Confidentiality, Integrity, and Availability).	Evaluates when the Confidentiality, Integrity and Availability (CIA) of information has been or could be violated with regards to providing trust of information.
Security Architecture		
The cyber security professional 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.		
Explains security issues and interdependencies related to various technologies and their impact on the security architecture of an organization.	Designs security architectures and controls.	Designs secure systems and define security specifications of components, integrating appropriate security controls.

Table 2: The competency model for information and cyber security professionals (Continue).

Designs a security blueprint and direct the design of a robust and coherent security architecture, based on a suite of security solutions and key design principles.	Establishes organisational guidelines and principles for the design of security architecture and controls, and drive the enhancement of organisation-wide security systems.	Integrates results regarding the identification of gaps in security architecture.
Information Assurance		
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.		
Explains information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication and non-repudiation.	Applies confidentiality, integrity and availability principles.	Explains how information assurance principles and methods apply to software development.
Explains the importance of information assurance to individuals, organizations, industries and societies.	Protects information systems and data by ensuring their availability, authentication, confidentiality and integrity.	Demonstrates skill in determining how a security system should work and how changes in conditions, operations or the environment will affect these outcomes.
Infrastructure Security		
Physical Layer & Telecommunications Security		
Protection of Telecommunicationssystems		
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.		
Describes transmission methods and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	Develops processes and procedures for protecting telecommunications networks against unauthorized access and wiretapping (e.g., protected distribution systems, transmission encryption, locked telephone closets, etc.).	Develops processes and procedures for mitigating the loss of confidentiality of SUI or classified information by utilizing TEMPEST, emanations and Technical Surveillance Countermeasures (TSCM).
Telecommunication		
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.		
Demonstrates knowledge of communication methods, principles, and concepts.	Describes the capabilities of different electronic communication systems and methods.	Explains basic concepts, terminology, and operations of a wide range of communications media.
Cyber-Physical Systems Security		
Critical Infrastructure		
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.		

Table 2: The competency model for information and cyber security professionals (Continue).

Identifies local specialized system requirements (e.g. critical infrastructure systems that may not use standard IT for safety, performance and reliability).	Explains concerns regarding the protection and safeguarding of critical infrastructures, both governmental and commercial, including power, transportation, banking and telecommunications systems.	Discusses key security laws and policies, global trade practices and other efforts to protect and maintain cyber infrastructures.
Cyber-Physical Systems & IoT		
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.		
Makes meaning of the terms CPS and IoT and why they are often used interchangeably and identify definitions that indicate the differences between them.	Recognizes the protocols and networks typically used to connect CPS and IoT devices to networks.	Describes how security mechanisms are used to address IT challenges that may not be viable in the world of CPS or IoT.
Designs, creates and deploys a IoT device using open source and low-cost computing platforms.	Describes how the handling and storage of data delivered by IoT devices offers challenges to security and privacy.	Demonstrate several security issues and challenges of collaborative data acquisition in IoT.
Operational Technology Architecture		
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.		
Explains typical OT architecture.	Differentiates between IT and OT architectures and the operation of these architectures.	Explains the typical communications network options and communications protocols used in OT architectures, with their relative pros and cons.
Identifies the principal drivers of OT systems, particularly process safety and system availability.	Recognizes the specialized system requirements of OT systems.	Understands the risks associated with operational technology (OT) systems and is able to identify practical mitigation measures to manage these risks.
Hardware Security		
Hardware Testing		
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.		
Tests hardware.	Tests hardware security problems pertaining to the organisation's computing environment.	Tests dedicated cyber defense hardware.
Analyzes the results of hardware testing.	Checks system hardware availability, functionality, integrity and efficiency.	Tests, evaluates and verifies hardware to determine compliance with defined specifications and requirements.
Secure Hardware Design		

Table 2: The competency model for information and cyber security professionals (Continue).

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.		
Designs hardware to adequately address cyber security requirements.	Builds cyber defense hardware.	Ensures that hardware designs balance functional, service quality, security, systems management and sustainability requirements.
Hardware Problems		
The cyber security professional is able to troubleshoot hardware issues. Furthermore, he has basic and specialized knowledge in the field of hardware.		
Troubleshoots hardware security problems pertaining to the organisation's computing environment.	Diagnoses faulty system/server hardware.	Performs repairs on faulty system/server hardware
Network Security		
Network Defense		
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.		
Recognizes security policies and select the network technology and equipment necessary to implement security measures.	Identifies network access control mechanisms (e.g., access control list).	Describes basic network hardening techniques.
Explains computer network defense tools, including open source tools and their capabilities.	Understands the purpose and basic features of a firewall, Intrusion Detection System (IDS), and Intrusion Protection System (IPS).	Maintains and updates the security system controlling the incoming and outgoing network traffic.
Network Design		
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.		
Designs the security architecture for network implementation.	Explains network design processes, to include understanding of security objectives, operational objectives and trade-offs.	Provides feedback on network requirements, including network architecture and infrastructure.
Takes responsibility for major aspects of network specification and design within the organisation.	Produces network design policies, philosophies and criteria covering connectivity, capacity, interfacing, security, resilience, recovery, access and remote access.	Translates logical designs into physical designs.
Network Protocols		

Table 2: The competency model for information and cyber security professionals (Continue).

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.		
Explains computer networking protocols.	Understands Voice over Internet Protocols (VoIPs).	Explains common communications protocols and how to apply security to them, e.g., IPSEC, SSL, TLS.
Understands and use protocols to provide reliable, ordered, and error-checked delivery of information between applications running on hosts communicating over an IP network.	Understands essential security protocols.	Explains use of secure communications protocols.
Systems Security		
Authentication, Authorisation & Accountability		
Authentication & Authorisation		
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.		
Describes major access control systems and their function.	Explains digital rights management.	Explains key authentication, authorization and access control principles and methods.
Demonstrates knowledge of processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access.	Applies appropriate access controls and privileges to an organisation's computing environment.	Creates authentication and authorization system for users to gain access to data based on assigned privileges and permissions.
Identity & Access Management		
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 deny access to unauthorized people. He understands the need to delete expired accounts and change passwords regularly.		
Manages accounts, network rights, and access to systems and equipment.	Validates the identity of individuals to verify access approval and level.	Administers accounts, network rights and access to systems and equipment.
Monitors activity to ensure that only authorized access is taking place.	Grants users appropriate access to IT resources and prevents access by non-authorized users.	Shows the concept of identity management and how it is important.
Distributed Systems Security		
Distributed Systems		
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.		

Table 2: The competency model for information and cyber security professionals (Continue).

Explains distributed computing concepts.	Summarizes the security implications and risks for distributed IT systems.	Discusses the trade-off between utility and risk of cloud computing, file sharing, and peer-to-peer services.
Cloud Security		
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.		
Recognizes vulnerabilities, threats and risks that are distinct to cloud computing servers.	Demonstrates why organizational accountability for data and system security still exists in a cloud service, delivery model.	Recommends what safe guards and security models should be in place to reduce organizational risk (e.g. consent/notice requirements, data classification).
Uses security tools and design techniques to ensure security is built into cloud services.	Contrasts the security benefits and risks of cloud storage systems.	Differentiates between public, hybrid and private clouds.
Digital Currency		
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.		
Compares and evaluates different approaches/implementations of digital currencies.	Suggests and implements digital currency extensions using relevant scripting techniques (colored coins paradigm).	Provides a thorough security analysis of digital currency implementation.
Operating Systems & Virtualization Security		
Understanding of Operating Systems & Virtualization		
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.		
Understands virtualization concepts, features, benefits and considerations.	Explains virtualization technologies and virtual machine development and maintenance.	Demonstrates familiarity with Windows/Unix/Android, iOS and Windows Mobile ports and services.
Demonstrates familiarity with Windows command line.	Identifies file system implementations.	Demonstrates knowledge of Linux/UNIX operating systems and the underlying source codes.
Database Administration		
The cyber security professional uses, manages, and evaluates database tools and handles database configurations, reconfigurations, and installations. He monitors and optimizes the performance of databases.		
Implements database systems.	Identifies, evaluates and manages the adoption of appropriate database administration tools and processes, including automation.	Contributes to the setting of standards for definition, security and integrity of database objects and ensures conformance to these standards.

Table 2: The competency model for information and cyber security professionals (Continue).

Manages database configuration including installing and upgrading software and maintaining relevant documentation.	Monitors database activity and resource usage.	Develops and maintains procedures and documentation for databases.
Secure Operating Systems		
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.		
Describes basic operating system hardening techniques.	Demonstrates familiarity with the security features and functions of common operating systems.	Designs operating systems to adequately address cybersecurity requirements.
Cryptography		
Encryption		
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.		
Explains the concept of public key infrastructure (PKI). Explains use of encryption technology, e.g. PKI, hard drive encryption, data encryption and encryption-at-rest.	Explains symmetric key rotation techniques and concepts. Compares encryption for data at rest and data in motion.	Describes encryption methodologies. Makes sense of block-level encryption, file-level encryption and application-level encryption for encrypted storage.
Cryptographic Understanding		
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.).		
Explains the core concepts of cryptography and cryptographic key management concepts.	Demonstrates knowledge of information theory.	Exhibits comprehension of the terms encryption, decryption, key, public key cryptography, symmetric cryptography, algorithm, key length, key escrow, key recover, key splitting, random number generator, nonce, initialization vector, cryptographic mode, plaintext, cipher text, S/MIME, PGP, IPsec and TLS.
Software & Platform Security		
Secure Software Lifecycle		
Software Testing		
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.		
Identifies test objectives.	Selects appropriate testing/demonstration techniques.	Designs, implements, and executes test cases.

Table 2: The competency model for information and cyber security professionals (Continue).

Performs manual test activities (in other words, data entry, test case execution and so forth).	Designs and executes unit test cases.	Identifies automated testing opportunities.
Secure Design		
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.		
Models threats and associated risks of new and modified systems.	Identifies the attack surface of new and modified systems.	Analyzes design constraints, analyzes trade-offs and detailed system and security design, and considers life cycle support.
Undertakes threat modelling tasks.	Designs software applications to adequately address cyber security requirements.	Follows recommended design principles to create secure systems (such as providing multiple layers of protection, using access control mechanisms, and encrypting sensitive data).
Secure Development		
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.		
Recognises the benefits of addressing security during system development.	Lists some of the tools, products and practices that contribute to secure development.	Contributes to the development of secure systems.
Defines and/or implements secure development standards and practices including, where relevant, formal methods.	Develop cyber security or cyber security-enabled products.	Explain the importance of integrating security requirements into SDLC.
Software Security		
Prevention of Software Vulnerabilities		
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 secure programming and to review and approve guidelines.		
Describes secure coding practices and defensive programming techniques.	Explains concepts and techniques for secure software coding and defensive programming.	Recognizes major software security concerns (buffer overflow, X-site scripting, SQL Injection, etc.) and coding and management techniques to mitigate them.

Table 2: The competency model for information and cyber security professionals (Continue).

Develops processes and procedures to mitigate the introduction of vulnerabilities during the engineering process.	Performs processes and procedures to mitigate the introduction of vulnerabilities during the engineering process.	Practices secure coding practices.
Detection of Software Vulnerabilities		
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.		
Detects programming errors / defects by utilizing effective means such as debug technique or debugger.	Exhibits several common defects, bugs and logic flaws in software.	Demonstrates basic knowledge of static and dynamic analysis to assist in the identification of vulnerabilities.
Applies knowledge of static and dynamic analysis to identify vulnerabilities.	Uses static analysis methods to identify security vulnerabilities.	Creates or proposes new methods for recognizing security vulnerabilities.
Software Security Evaluation & Vulnerability Assessments		
The cyber security professional conducts security evaluations of software systems. He evaluates software by analyzing the design documentation and programming 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.		
Performs a security evaluation of software based on the procedure stipulated by ISO/IEC 15408.	Contributes to the security evaluation of software.	Applies recognised evaluation methodologies, tools and techniques, developing new ones where appropriate.
Applies vulnerability assessments to determine if the software/system being assessed is sufficiently secure within tolerances.	Conducts assessments of software system vulnerabilities.	Reviews vulnerability assessment findings to quantify and prioritize vulnerabilities in a system.
Web & Mobile Security		
Secure Web Usage		
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.		
Explains the risks associated with social media and the countermeasures available to address them.	Describes methods for secure use of social media.	Tells a story about dangerous places on the web and how surfing one of them can have a negative impact on privacy or security.
Web & Mobile Defense		
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.		

Table 2: The competency model for information and cyber security professionals (Continue).

Demonstrates knowledge of methods to protect web services.	Develops processes, procedures, and identifies minimum security controls for External Information Systems and portable/mobile devices.	Uses accepted standards to ensure that user input on web pages does not affect server-side processes.
Secures a web or mobile application and defends against common attacks.	Recognizes "security containers" and identifies their limitations and usability failings with respect to mobile devices.	Describes how authentication, secure certificates and secure communication can be used in web sessions.
Web & Mobile Vulnerabilities		
The cyber security professional is familiar with various vulnerabilities, threats, and risks that affect mobile devices in particular.		
Recognizes vulnerabilities, threats and risks that are distinct to mobile devices.	Contrasts client-side with server-side security issues.	Compare the benefits with the risks of a 'bring your own device' (BYOD) program.
Attacks and Defences		
Forensics		
Digital Forensics		
The cyber security professional collects, processes, preserves, analyzes, and presents forensic evidence to support security vulnerability mitigation and 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.		
Describes types of digital forensics data and how to recognize them.	Investigates suspected attacks and manages security incidents.	Sets policies and standards and guidelines for how the organisation conducts digital forensic investigations.
Conducts investigations to correctly gather, analyse and present the totality of findings including digital evidence to both business and legal audiences.	Can describe the basic principles of digital forensics and recognises the capability of forensics to support investigations.	Presents evidence as appropriate, acting as an expert witness if necessary.
Computer Forensics		
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.		
Identifies which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Describes the use of computer forensics to prevent and solve information technology crimes and security breaches.	Preserves electronic evidence.

Table 2: The competency model for information and cyber security professionals (Continue).

Performs forensic analysis on computer systems, and make recommendations for remediation.	Extracts a memory dump from a running computer.	Creates a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes.
Network Forensics		
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.		
Examines potential security violations to determine if the network environment security policy has been breached, assesses the impact and if appropriate preserves evidence.	Maintains current knowledge on network forensic tools and processes.	Performs forensic analysis on networks and makes recommendations for remediation.
Compares active and passive approaches to network forensics.	Employs surveillance mechanisms to discover network intrusion.	Performs a network inventory.
Adversarial Behaviours		
Characterisation of Adversaries & Defence		
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.		
Formulates strategies to defend against the actions of state-sponsored attackers, hackers, hacktivists, organized crime, industrial and international cyber espionage, advanced persistent threats, supply chain and insider cyber threats.	Identifies threat tactics and methodologies.	Identifies cyber threat tactics and methodologies.
Identifies common adversary tactics, techniques and procedures (TTPs) in assigned area of responsibility.	Monitors and reports changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Establishes a threat intelligence strategy and directs analysis and integration across various sources to present a robust view on threats, perpetrators, motivations and modus operandi.
Cyber Threat Analysis		
The cyber security professional is able to identify and assess the capabilities and activities of cyber criminals and/or foreign intelligence agencies using a variety of tools. He supports law enforcement and/or counterintelligence activities through the production of intelligence.		
Using cyber means, identify and assess the capabilities and activities of cyber criminals or foreign intelligence entities.	Produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	Collects intelligence and actively identifies cyber-threats and counterintelligence information.

Table 2: The competency model for information and cyber security professionals (Continue).

Social Engineering		
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.		
Illustrates how to recognize phishing and spear phishing.	Tells a story about how a social engineering attack can be designed using data posted on social media.	
Malware & Attack Technologies		
Malware Detection		
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.		
Makes sense of the role and limitations of signature-based and behavioral-based anti-virus technology.	Contrasts the roles of prevention, deterrence and detection mechanisms.	Contrasts host-based and network-based intrusion detection systems.
Performs virus scanning on digital media.	Ensures that anti-malware systems are operating correctly.	Demonstrates skill in identifying malware.
Malware Analysis & Defence		
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.		
Enables and conducts analysis of malicious threats, to examine their characteristics, behaviours, capabilities, intent and interactions with the environment as well as the development of defence and mitigation strategies and techniques to effectively combat such threats.	Performs static, dynamic or behavioural analysis on malicious codes and threats, debug malware and thwart malicious attacks.	Examines malicious threat behaviour and capabilities, and circumvent anti-analysis mechanisms, recommending techniques to block malicious code and attacks.
Establishes an enterprise threat defence and mitigation strategy, incorporating new techniques to combat threats and attacks.	Analyzes identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Applies knowledge of static and dynamic analysis to identify malware.
Awareness of Attacks		
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.		
Describes general attack stages.	Describes different classes of attacks.	Recognizes potential IT security threats and risks, including common attacks and methods used to compromise systems.
Security Operations & Incident Management		

Table 2: The competency model for information and cyber security professionals (Continue).

Incident Management		
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.		
Contributes to incident management.	Identifies and classifies incident types and service interruptions to build the knowledge system.	Manages incidents and monitors compliance with incident management policies and procedures.
Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact.	Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure.	Takes appropriate action to report incidents as required by procedure and, where applicable, legislation, in order to avert any effect from it.
Vulnerability Assessment		
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/or develops appropriate countermeasures based on the test results.		
Inspects vulnerabilities using the appropriate methods and tools.	Evaluates the test results, and if that reveals any problems, then works out measures in cooperation with project stakeholders and so produces improvement.	Explains vulnerability assessment tools, including open source tools, and their capabilities.
Explains the proper use of vulnerability scanning for vulnerability assessments.	Demonstrates knowledge of vulnerability identification techniques and tools.	Conducts vulnerability assessment to reveal vulnerabilities or lapses in the existing systems or security mechanisms.
Intrusion Detection & Analysis		
The cyber security professional monitors network and system activity to detect potential intrusion and other anomalous behavior. He analyzes information and 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.		
Monitors network and system activity to identify potential intrusion or other anomalous behaviour.	Analyses the information and initiates an appropriate response, escalating as necessary.	Uses security analytics, including the outputs from intelligence analysis, predictive research and root cause analysis in order to search for and detect potential breaches or identify recognised indicators and warnings.
Applies and maintains intrusion detection systems.	Designs several rules for a network-based intrusion detection system that will protect against specific known attacks.	Demonstrates familiarity with Intrusion Detection System (IDS) tools and applications.
Human, Organizational, and Regulatory Aspects		
Privacy & Online Rights		

Table 2: The competency model for information and cyber security professionals (Continue).

Data Security		
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.		
Undertakes a comprehensive review of the company's data and privacy projects and ensures that they are consistent with corporate privacy and data security goals and policies.	Develops data security policies using data security standards, guidelines, and requirements that include privacy, access, retention, disposal, incident management, disaster recovery and configuration.	Specifies data and information classification, sensitivity, and need-to-know requirements by information type.
Develops sensitive data collection and management procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes).	Addresses alleged violations of data security and privacy breaches.	Assesses the effectiveness of enterprise data security policies, processes, and procedures against established standards, guidelines, and requirements, and suggest changes where appropriate.
Technology & Privacy		
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 and monitors technological developments in the field of data protection.		
Demonstrates knowledge of identifying and protecting privacy data and sensitive information.	Explains the privacy issues associated with cloud computing.	Makes sense of the impact of IT systems on privacy.
Assures that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information.	Monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.	Evaluates the role of privacy issues within IT as it relates to organizations.
Personal Information		
The cyber security professional handles personal information responsibly. He understands the role and limitations of encryption technologies with regard to the protection of personal data. He is aware that there are major tensions and inherent conflicts between personal data protection and the security property of authenticity or non-repudiation.		
Makes sense of the terms Personal Information, Personally Identifiable Information, De-Identification, Anonymization, Pseudonym, Masking and Unmasking.	Describes how the Fair Information Practices apply to personal information and how online entities collect and use personal information.	Classifies several categories of personal information according to privacy and disclosure risk.
Contrasts policies for collecting, processing, storing, sharing, and disposing of personal information.	Illustrates the role and limitations of encryption for protecting personal information.	Makes sense of policies and technologies for isolating personal data from enterprise data.
Law & Regulation		

Table 2: The competency model for information and cyber security professionals (Continue).

Legal & Regulatory Compliance		
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.		
Defines the enterprise information security compliance program.	Recognises and reports non-compliances with applicable legislation and regulation	Establishes an enterprise information security compliance performance measures program.
Understands the importance of compliance and possess awareness of laws and regulations.	Applies known compliance considerations, laws and policies to a project.	Ensures that the organisation complies with legal and regulatory requirements.
Legal & Regulatory Environment		
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.		
Understands the legal and regulatory environment within which the business operates.	Can describe the major legislative and regulatory instruments relevant to Information Security (e.g. Data Protection Act, General Data Protection Regulation (GDPR), privacy, healthcare, ISO/IEC 27000 family) and legislation and regulation relevant to own work.	Can explain the principal requirements of major legislation and regulations relevant to Information Security, and those legal and regulatory instruments relevant to own work.
Analyses changes in legislation or regulation and assesses impact on own or client organisation.	Advocates organization's official position in legal and legislative proceedings.	Interprets and applies laws, regulations, policies, standards or procedures to specific issues.
Intellectual Property & Licensing		
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.		
Determines whether not to violate intellectual property right of other organization.	Investigates intellectual property rights protection and registers the rights.	Establishes a handling rule to preserve intellectual property.
Explains software licensing agreements and the importance of ensuring that software is properly licensed prior to performing installation.	Understands the concept of an End User License Agreement (EULA).	Differentiates between open source and proprietary licenses.
Human Factors		
Cyber Security Awareness & Development		

Table 2: The competency model for information and cyber security professionals (Continue).

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 the competencies of individuals and groups. He contributes to improving security awareness by providing supportive, interactive learning environments and using innovative teaching methods.		
Provides learning and development to improve technical skills and/or security awareness.	Provides briefing/training sessions to individuals and groups.	Uses specialist knowledge and skills to advise, guide and coach individuals.
Leads or supports the assessment of individual and group competence, identifying skills needs and skill gaps.	Performs a needs assessment to determine skill gaps and identify personnel in roles requiring training based on mission requirements.	Delivers awareness and training to intended audiences based on identified needs and within mandated time frames.
SA&E[1] Policy and Content Development		
The cyber security professional develops training guidelines and policies regarding 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.		
Contributes to the development of training content.	Develops security education materials.	Develops the policy for the cyber security training and awareness program.
Defines the goals and objectives of the cyber security awareness and training program.	Develops a workforce development, training, and awareness program plan.	Designs a continuing education program.
Personnel Security		
The cyber security professional applies a set of personnel security controls to prevent and/or 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.		
Makes sense of the limits of a background check in screening an organization's employees.	Establishes personnel security rules and procedures to which external suppliers (e.g. vendors, contractors) must conform.	Coordinates within the personnel security office, or with Human Resources, to ensure that position sensitivity is established prior to the interview process, and that appropriate background screening and suitability requirements are identified for each position.
Coordinates within the personnel security office, or with Human Resources, to ensure background investigations are processed based on level of trust and position sensitivity.	Reviews, analyzes and adjudicates reports of investigations, personnel files, and other records to determine whether to grant, deny, revoke, suspend or restrict clearances consistent with organizational requirements, national security and/or suitability issues.	Assesses the relationships between personnel security procedures and organization-wide security needs and makes recommendations for improvement.

[1]SA&E stands for Security Awareness & Education

Table 2: The competency model for information and cyber security professionals (Continue).

Risk Management & Governance		
Risk Management		
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 an affordable cost. He decides on appropriate actions required to adjust security and address risks.		
Articulates the different forms of threat to, and vulnerabilities of, information systems and assets; and manage the risks.	Advises management on information risk across a business unit or organization.	Evaluates findings from threat assessments, IT Health Checks and vulnerability testing tools.
Formulates risk management plans to mitigate identified cybersecurity/IA weaknesses.	Decides on appropriate actions required to adapt security and address risk exposure.	Assesses effectiveness of the risk management program and implements changes where required.
Risk Assessment		
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.		
Conducts risk assessments and produces treatment plans for low impact risks.	Produces or contributes to risk assessments for Information Systems taking into account information assets, threats, vulnerabilities, business impacts and likelihood.	Produces risk assessments for complex systems.
Performs basic risk assessments for small information systems.	Conducts security risk assessments for defined business applications or IT installations in defined areas and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls.	Can describe the concepts and principles of risk assessment.
Business Continuity Management		
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.		
Identifies information, assets and business processes that are critical for business continuity.	Works closely with those responsible for business continuity to input into the development and testing of recovery plans.	Leads definition and testing of the continuity plan for all knowledge and information services.

Table 2: The competency model for information and cyber security professionals (Continue).

Identifies the available continuity and recovery strategies for the entity's operations that will meet the recovery time objective and recovery point objectives identified during the Business Continuity Planning process.	Explains the concept of business continuity.	Understands the importance of keeping business functions and computing processes on-going and how to recover from an outage or equipment failure.

References

[1] Weinert, F. E. Vergleichende Leistungsmessung in Schulen - eine umstrittene Selbstverständlichkeit. In *Leistungsmessung in Schulen*, F. E. Weinert, Ed. Beltz, Weinheim, Germany, 2001, pp. 17–32.