Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model

DANIEL BENDLER, University of Innsbruck, Austria
MICHAEL FELDERER, University of Innsbruck, Austria and Blekinge Institute of Technology, Sweden

Competency models are widely adopted frameworks that are used to improve human resource functions and education. However, the characteristics of competency models related to the information security and cybersecurity domains are not well understood. To bridge this gap, this study investigates the current state of competency models related to the security domain through qualitative content analysis. Additionally, based on the competency model analysis, an evidence-based competency model is proposed. Examining the content of 27 models, we found that the models can benefit target groups in many different ways, ranging from policymaking to performance management. Owing to their many uses, competency models can arguably help to narrow the skills gap from which the profession is suffering. Nonetheless, the models have their shortcomings. First, the models do not cover all of the topics specified by the Cybersecurity Body of Knowledge (i.e., no model is complete). Second, by omitting social, personal, and methodological competencies, many models reduce the competency profile of a security expert to professional competencies. Addressing the limitations of previous work, the proposed competency model provides a holistic view of the competencies required by security professionals for job achievement and can potentially benefit both the education system and the labor market. To conclude, the implications of the competency model analysis and use cases of the proposed model are discussed.

CCS Concepts: • **Security and privacy**; • **Social and professional topics → Computing education**; **Employment issues**;

Additional Key Words and Phrases: Cybersecurity education, competency model, competency, workforce development, skills gap

1 INTRODUCTION

Recent security breaches [37] point to the inherent danger that cyberspace poses. Given the ongoing risks posed by malware and other threats, the growing sophistication of the threat landscape, and the expansion of the attack surface [36], cybersecurity professionals represent an indispensable resource for protecting assets. The security industry, however, is suffering from a global workforce deficiency [26, 38, 56]. Because the shortage in competent security experts is putting public and private organizations at risk [56], narrowing the skills gap is imperative.

In this context, the lack of capacity and capability of the cybersecurity workforce has fueled efforts by governments, education systems, and companies to advance cybersecurity education. Countries such as the United States, Australia, New Zealand, and France have launched cybersecurity strategies addressing cybersecurity education (e.g., strengthening educational programs) [10, 88]. Likewise, companies have begun to foster recruitment and workforce development (e.g., by offering training and certification opportunities) [54]. To increase efforts, higher education institutions have started to offer stand-alone security programs and programs including security

Authors' addresses: Daniel Bendler, daniel.bendler@student.uibk.ac.at, University of Innsbruck, Technikerstrasse 21a, Innsbruck, Austria, 6020; Michael Felderer, michael.felderer@uibk.ac.at, University of Innsbruck, Technikerstrasse 21a, Innsbruck, Austria, 6020, Blekinge Institute of Technology, Valhallavägen 1, Karlskrona, Sweden, 37141.

1946-6226/2022/12-ART $15.00
https://doi.org/10.1145/3573205

content [17, 88], introduce novel maintenance measures to keep curricula up to date [65], and revise curricula to include competency-based education [103].

Moreover, the notion of competency, often referred to as the integration of knowledge, skills, and attitudes necessary for successful task performance [5], is gaining popularity in cybersecurity education [88, 103]. Professional associations, such as the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM), are endeavoring to push the concept of competency as the currency of educational outcomes [22], and universities are striving to shift to competency-based education [103]. To incorporate the notion of competency into educational settings, organizations and universities are using competency models to specify professionals' competencies. Educational institutions recognize competency models as useful tools for the development of competency-based curricula and training [21, 51, 66]. Similarly, public and private organizations are utilizing competency models to improve and align competency-based human resource (HR) functions, including workforce development and training [20, 32, 117]. However, despite the merits of competency models in education and training and their widespread use in practice, a systematic cybersecurity competency model analysis has thus far been lacking. To bridge this gap, this study investigates the current state of competency models related to the security domain and also proposes a competency model that addresses the limitations of existing ones.

The remainder of the paper is organized as follows. After presenting the theoretical background and related work in Section 2, Section 3 outlines the methods used to analyze the existing work and construct a new evidence-based competency model. Subsequently, Section 4 presents the findings of the analysis and Section 5 describes the proposed competency model. In Section 6, the implications of the findings and use cases of the model are discussed. The paper concludes with remarks in Section 7.

2 BACKGROUND AND RELATED WORK

In this section, we outline the theoretical background and related work of our study. Section 2.1 discusses the information security and cybersecurity domains and introduces the Cybersecurity Body of Knowledge (CyBOK) [94]. Sections 2.2 and 2.3 explain the concept of competency and competency models. Section 2.4 presents related work and includes studies analyzing competency models, which are also the subject of the present work. Additionally, Section 2.4 includes job advertisement analyses that shed light on the competency profile of a cybersecurity expert.

2.1 Information Security and Cybersecurity

Information security and cybersecurity can be differentiated by considering the origin of the threats and the assets that are to be protected [112]. While competing definitions exist, information security can be understood as an ongoing process [83] concerned with the protection of analog and digital information, its security properties, and the information technology (IT) that stores valuable data from intentional and unintentional threats that arise from physical and virtual sources [2, 57, 112, 119]. In contrast, cybersecurity is a computing-based approach [60] that focuses on the protection of information systems (e.g., hardware and software), the information stored on them, and non-information-based assets (e.g., humans and society) that are vulnerable to intentional or unintentional threats originating from cyberspace [53, 112]. IT security referring to the protection of information systems can be seen as a subset of both information security and cybersecurity [112].

From the perspective of security, assets have security properties assigned, including confidentiality, integrity, availability, authentication, authorization, and nonrepudiation [39]. These security properties are defined as follows [2, 23]. Confidentiality refers to the ability to ensure that information is not disclosed to unauthorized individuals, processes, or devices. Integrity ensures that information is not maliciously or unintentionally modified or altered. Availability ensures that information is accessible by authorized individuals when required. To establish whether a claim of identity is true, authentication is used. Implemented using access controls, authorization decides what an authorized entity can or cannot do. Lastly, nonrepudiation is achieved when the people taking action cannot successfully deny that they have done so [2].

In recent years, several efforts [46, 60, 95] have been made to collect, systematize, and codify the foundational information security and cybersecurity knowledge in a body of knowledge (BOK). Given that cybersecurity is a broad and interdisciplinary field, different bodies have different foci. For the competency model analysis, we have selected the CyBOK [94], because it (i) is an up-to-date body, (ii) has a strong focus on cybersecurity [124], and (iii) consists of a reasonable number of knowledge areas that allow for a fine-grained content analysis that is neither too abstract nor too specific. The CyBOK is a comprehensive body of knowledge with a more technical focus than other BOKs, such as the Certified Information Systems Security Professional BOK or the Cybersecurity Curricula 2017 [124]. The CyBOK's purpose is to codify foundational knowledge and serve as a guide for cybersecurity knowledge. The CyBOK's basis is formed by 19 knowledge areas (KAs) that are grouped into five broad categories [94]. Table 1 provides a brief definition of each area.

Table 1. Overview of the 19 KAs and five broad categories (adapted from [94, p. 5])

	Human, organizational, and regulatory aspects
Risk management & governance	Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation
Law & regulations	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare
Human factors	Usable security, social and behavioral factors impacting security, security culture and awareness, as well as the impact of security controls on user behaviors
Privacy & online rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
	Attacks and defenses
Malware & attack technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches
Adversarial behaviors	The motivations, behaviors, and methods used by attackers, including malware supply chains, attack vectors, and money transfers
Security operations & incident management	The configuration, operation, and maintenance of secure systems, including the detection of and response to security incidents and the collection and use of threat intelligence
Forensics	The collection, analysis, and reporting of digital evidence in support of incidents or criminal events
	Systems security
Cryptography	Core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these, and the protocols that use them
Operating systems & virtualization security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualization, and security in database systems
Distributed systems security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centers, and distributed ledgers
Authentication, authorization, and accountability	All aspects of identity management and authentication technologies and architectures and tools to support authorization and accountability in both isolated and distributed systems
	Software and platform security
Software security	Known categories of programming errors resulting in security bugs and techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems
Web & mobile security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models
Secure software lifecycle	The application of security software engineering techniques in the whole systems development lifecycle, resulting in software that is secure by default
	Infrastructure security
Network security	Security aspects of networking and telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security
Hardware security	Security in the design, implementation, and deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness
Cyber-physical systems security	Security challenges in cyber-physical systems, such as the Internet of things and industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures

Table 1. Overview of the 19 KAs and five broad categories (adapted from [94, p. 5])

Physical layer & telecommunications security	Security concerns and limitations of the physical layer, including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference

2.2 About the Concept of Competency

Competency is a widely adopted concept in cognitive, social, and educational science [63] and has been introduced in psychology as a counterterm to intelligence [50, 81]. Theoretical views, national context, and application area influence the concept's meaning [110], and different approaches to conceptualizing competencies coexist [33, 71, 114]. For instance, Schippmann et al. [99] revealed that experts' answers to the question of what a competency is vary. Given its different meanings, some authors have referred to the term as a "*fuzzy concept*" [109]. Nonetheless, the concept promises to help to bridge the gap between education and the labor market [71, 90, 109].

Which components should be included in the competency construct is an ongoing debate. Focusing on a narrow notion of competency, Klieme and Leutner [64] defined competency as a context-specific, cognitive performance disposition, thereby reducing the concept to specialized cognitive prerequisites [49, 50]. In contrast, the computing curricula 2020 report went beyond the cognitive realm and defined competency as *"composed of K-S-D dimensions observed within the performance of a task"* [22, p. 47]. According to this notion, competency integrates knowledge, skills, and dispositions that are causally related to the accomplishment of a task [41]. The integration of cognitive and noncognitive components into a complex competency system is also frequently found in the concept of action competency [64, 114]. For example, the German Qualifcations Framework Working Group [45] defined competency as *"the ability and readiness to use knowledge, skills, personal, social, and methodological competencies and to behave in a considered, individual, and socially responsible manner"* [45, p. 17]. In this paper, we adopt a holistic approach to competency and refer to the definition of Weinert [116, pp. 27-28]: 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. This notion of competency implies that competencies are comprised of *"all those cognitive, motivational, and social prerequisites"* [115, p. 51] that are necessary for achievement. Specifically, this holistic approach to competency integrates cognitive and noncognitive components into a complex system of knowledge, skills, attitudes, and cognitive abilities [114]. Although not explicitly stated, knowledge is a component of Weinert's definition [62]. Here, knowledge refers to the mastery of core concepts and topics acquired through learning [74, 114, 120]. Cognitive abilities refer to general intellectual abilities that are less learnable [69, 114]. Relying on [22] and [45], we define skill as the proficient application of knowledge to successfully meet demands in a particular action context. The construct described as "motivational, volitional, and social readiness and capacity" refers to attitudes respectively dispositions [41] and bridges the gap between the mere ability to do something and the actual behavior [89]. Dispositions are affective by nature and can be understood as tendencies toward a certain behavior and the sensitivity to know how and when to engage in a task [89]. In this sense, the affective component is what transforms the mere ability to act into appropriate action [1]; it establishes the connection between what a person can do (ability) and what a person does do (action) [41]. Lastly, the internal structure of the competency is derived from the structure of the task, with the task unfolding and framing the purpose and meaning of competency. The task serves as a crystallization point of competency (i.e., the task renders competencies concrete and visible) [90, 115].

For analytical and organizational reasons, competencies can be categorized into competency classes [34, 77, 104]. By default, competency classes can be differentiated according to task or demand [33, 34]. If the subject's action relates to other people or groups of people (the task), it is a question of social competencies. Personal competencies refer to tasks concerned with oneself (e.g., self-control in stressful situations), and professional competencies pertain to domain-specific and work-related tasks. Methodological competencies are somewhat different, as their task application is more general. Here, we refer to methodological competencies as personal qualities that apply to a broad range of tasks (e.g., problem-solving). Depending on the task, the relative emphasis of the competency components varies [41]. Thus, some competencies are strongly knowledge-focused, while others are more skill- or disposition-focused.

2.3 Competency Models

The concept of the competency model has been defined in three ways: First, the term can refer to the modeling of the internal structure of competency in general terms, specifying personal qualities, such as dispositions and skills, as competency components [41]. Second, there are competency structure and level models used to model the dimensionality and differentiate between the levels of proficiency of a concrete competency, such as foreign language competency or programming competency [6, 64, 67]. Third, competency models, as understood in this paper, refer to organized catalogs or lists of competencies required by individuals to achieve goals, meet demands, and perform effectively in a specific role within a(n) job, job family, organization, industry, or process [20, 32, 75, 78, 79]. Specifically, the term "competency framework" is also frequently used in the literature to refer to a structured competency collection [3, 30, 34].

Because models can contain a large number of competencies [34], organization becomes crucial. To organize competencies, different structures have been proposed [106], including hierarchies [32, 108] and typologies [45, 52, 104]. For instance, models by the Employment and Training Administration [32] organize competencies into stacked tiers that form a hierarchically structured pyramid shape. In contrast, the "KompetenzAtlas" [52] classifies competencies based on a competency class typology. Regardless of the underlying structure, competencies constitute the core of a competency model, and models often record competencies in detail. A competency usually consists of (i) a label or title highlighting the name of the competency, (ii) a detailed description of the competency in behavioral terms, and (iii) proficiency levels or behavioral indicators outlining how a competency unfolds in action [20, 97]. Grouping behavioral indicators into proficiency levels (e.g., novice, intermediate, and expert) facilitates the application of competency models in many HR activities, including performance management, appraisal systems, and workforce development [98, 106]. Owing to their many applications, competency models can be considered the backbone of an organization's competency management [97]. To maximize the benefits of using competency models, many models are highly tailored to an organization's context and strategy, use organization-specific language and are graphically elaborated [20].

2.4 Related Work

Against the backdrop of a lack of qualified workers and with the aim of tackling the workforce shortage, several studies have examined competency models to provide input for the preparation of cybersecurity programs. For instance, Manson et al. [76] asked faculty experts to assess the content of several standards, including the IT Security Essential Body of Knowledge (EBK) [150]. According to the results, the EBK's competency area "data security" was considered most important, whereas "strategic security management" was deemed least important [76]. To determine industry priorities regarding the competencies of entry-level professionals, Whitman [118] asked participants to rate the competencies of the Cybersecurity Competency Model [153]. Results showed that all competencies were in demand, although some were more favored than others. Moreover, the preference for specific competencies did not vary between organization size and industry [118]. With the aim of informing curriculum development, Armstrong et al. [4] and Jones et al. [61] investigated the relative importance of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework's knowledge, skills, and abilities (KSAs)[1] [140] that are listed under specialty areas within the "protect and defend" category. In sum, the most important KSAs common to two or more specialty areas dealt with networks, vulnerabilities, threats, and programming [61], and nontechnical skills were rated highly important for achievement [4]. Next, several studies have compared competency models to identify differences and similarities. From these efforts, we can see that models can vary in several ways, including in the treatment of nonprofessional competencies (e.g., methodological, social and personal competencies), the number of competencies [15], the basic structure [84] and the concepts referred to [40]. Another line of studies has analyzed the content coverage of models and whether predefined characteristics have been met. Using the CyBOK knowledge areas to map the content of several frameworks, Hallett et al. [48] found that the NICE Framework, while not exhaustive, covers most knowledge areas, with "security operations and incident management" and "risk management and governance" being the most emphasized. Focusing on the analysis of the e-Competence Framework (e-CF), Plessius and Ravesteyn [91] showed that the e-CF [132] covers the IT domain to a great extent and fulfills many quality criteria. Miloslavskaya and Tolstoy [82] analyzed four models in terms of their applicability to the Internet of things (IoT) and cloud areas and found that the NICE Framework best fulfills the requirements. To inform a possible drafting of an e-competency framework for Malta, Camilleri [19] analyzed the usability of existing e-competency frameworks in Europe. Findings shed light on best practices regarding usability. Examining three models (e.g., e-CF) in terms of user expectations, Brown and Parr [15] found that models did not fully comply with user expectations, such as utility, portability, and simplicity. Moreover, all three models lacked automation features, limiting their usefulness in advanced skill management tasks [15]. Elsewhere, Brown [14] discussed the issue of backward compatibility between the Skills Framework for the Information Age (SFIA) 7 [145] and 6. Another study [25] examined the applicability of the e-CF 3.0 and SFIA 6 to the profile of a data scientist and concluded that both models adequately represented the profile. Lastly, relating to our investigation are studies extracting competencies from cybersecurity and information security job advertisements. From these efforts, we can draw the conclusion that it is not only professional competencies that are in demand but also methodological, social, and personal competencies [13, 92, 93]. Reducing the competency profile of the cybersecurity workforce to professional competencies is therefore an invalid process.

3 RESEARCH METHOD

This section presents the research method of the study and provides information on the search and selection process, the data analysis method, and the construction and validation procedure of the newly developed competency model. We also compile a maintenance and replication package [9] that contains the dataset and general maintenance advice.

3.1 Research Goal and Questions

To achieve consistency between goals, research questions, and metrics, the Goal–Question–Metric paradigm [7] has been used. The goal of this study is:

- *to analyze the current state of competency models related to the information security and cybersecurity domains and to build a competency model for these domains.*

The goal leads to two research questions (RQs):

RQ1 Which competency models for cybersecurity and information security are available and what are their characteristics?

RQ2 Can we use existing competency models to build a new security competency model, and which components and properties should characterize the new model?

[1] KSA stands for knowledge, skills, and abilities and is another way of conceptualizing competencies [69].

To answer the research questions, we collected, analyzed, and synthesized evidence for several metrics:

- annual number of publications, citation frequency, nations' producing models, publication type of the sources;
- competencies and their frequencies, competency classes and their frequencies, competency definition, number of proficiency levels, covered CyBOK categories and knowledge areas in addition to their frequencies; and
- completion of competency models in terms of content coverage, competency model uses and their frequencies, target groups, and a competency model based on existing models.

The search and selection of sources, the data analysis, and the construction and validation process for the new competency model are described in Sections 3.2, 3.3, and 3.4, respectively. The competency model analysis results answering RQ1 are presented in Section 4, and the new competency model that provides answers to RQ2 is presented in Section 5.

3.2 Searching and Selecting Sources

The search process and source selection are critical to our research, as they lay the foundations for all of the results. To optimize the search process and source selection, we adopted recommended strategies stated in the guidelines of systematic and multivocal literature reviews [43, 122].

3.2.1 Search Process. We decided to collect sources that provided a stand-alone cybersecurity competency model and models that integrate security content to obtain all cybersecurity and information security competencies and other relevant information. Therefore, not only did we search competency models for cybersecurity, but we also searched models from related fields, such as software engineering and information systems. Before the search, determining the source types was crucial. Regarding publication types, two forms were distinguished: formally published literature and grey literature (GL) [43]. While competing definitions exist [100], GL usually refers to *"literature that is not formally published in sources such as books or journal articles"* [72, Chap. 6]. Although the inclusion of GL in secondary studies is gaining momentum [44] and may be beneficial, for example, to avoid publication bias [105], the inclusion should not be taken lightly and should follow rigorous decision-making. To systematically decide whether to include GL, we applied the question-based checklist provided by [43]. As the sum of the "yes" answers was four out of seven, we chose to include GL. After the decision, we generated search terms. As recommended by [122], we expanded the search terms to include synonyms, alternative spellings, and related concepts. Note that we included "curriculum" as a search term to identify curricula encompassing competency models. The search was limited to the 1990-2020 period. From March 13, 2020, to May 15, 2020, search phrases with Boolean operators were used to identify formally published literature and GL in databases (see Table 2).

To narrow down the search space, relevance rankings (e.g., using Google's PageRank algorithm) of the databases were determined, and only the first 50 pages were examined. This action limited the search space and set a stopping criterion [43]. Typically, the collection of results and the application of inclusion and exclusion criteria are divided into separate steps. For this study, the selection criteria were already applied during the search process. Garousi and Mäntylä [44] also favored this strategy, as it reduces the number of irrelevant sources. After finalizing the initial pool, we utilized forward and backward snowballing methods in the search process [73, 122]. The references of the collected literature were studied (backward snowballing), and the citing literature was determined using the citation tracking functions of Google Scholar and Web of Science (forward snowballing). After checking for inclusion, these methods allowed us to obtain two additional sources [141, 151].

Table 2. Search phrases and databases used to find either formally or informally published models

#	Category	Search terms	Databases for formally published literature	Databases for GL
1	Stand-alone security competency models	(“Cybersecurity” OR “Cyber Security” OR “Information Assurance” OR “IT Security” OR "Information Security") AND (“Competency Model” OR “Skills Framework” OR “Competency Framework” OR “Competence Framework” OR "Curriculum" OR "Competency" OR "Competence" OR "Capability" OR "Skills")	Web of Science, IEEE Xplore, ACM Digital Library, Google Scholar	Google, OpenGrey, arxiv
2	Competency models integrating security concepts	(“Information Technology” OR “Software Engineering” OR “Information Systems” OR “ICT” OR "Computer Science" OR "Computer Engineering") AND (“Competency Model” OR “Skills Framework” OR “Competency Framework” OR “Competence Framework” OR "Curriculum" OR "Competency" OR "Competence" OR "Capability" OR "Skills")	Web of Science, IEEE Xplore, ACM Digital Library, Google Scholar	Google, OpenGrey, arxiv

3.2.2 Source Selection. Source selection deals with defining and applying inclusion and exclusion criteria to identify relevant sources for answering research questions [43]. Similarly to [44], we only defined inclusion criteria, as these criteria already indirectly excluded irrelevant sources. In addition, we used some quality assessment criteria because GL requires special treatment. First, we applied inclusion criteria to the title and the abstract. Subsequently, we applied the criteria to the body of content. Table 3 shows the inclusion criteria and some sources that were excluded. For clarification, we selected sources that solely contained a competency model and sources in which the competency model was only one element among many (e.g., in curricula). Additionally, we included any accompanying material to which no selection criteria were applied (e.g., material of the e-CF [131, 133]). Figure 1 presents the entire search and selection process.

Table 3. Inclusion criteria

#	Type of criteria	Inclusion criteria	Excluded
1	Content	The publication contains a stand-alone security competency model or a model integrating security concepts (i.e., a list of competency descriptions, behavioral indicators, or related concepts).	[31, 34, 85, 102]
2	Content	The competency model describes competencies that practitioners or graduates of a tertiary program should possess.	[96]
3	Language	The literature is in English or German.	
4	Access	The full text can be accessed.	[11, 35]
5	Bibliographic information	The producer (author, institute, organization, etc.) and the date of publication are indicated.	[58]
6	Bibliographic information	The source was published online during the time frame 1990 to 2020.	

3.2.3 Final Pool. When finalizing the pool, we arrived at 29 sources, 27 of which were competency models or material encompassing a model and two of which were additional sources that constituted supplementary material [131, 133]. Of the 29 sources, 13 models were stand-alone information security and cybersecurity competency models [127, 130, 135, 136, 138, 140, 141, 148–151, 153], and 14 competency models [125, 126, 128, 129, 132, 134, 137, 139, 142–147, 152] were frameworks that integrated cybersecurity content and related to adjacent domains, such as software engineering.

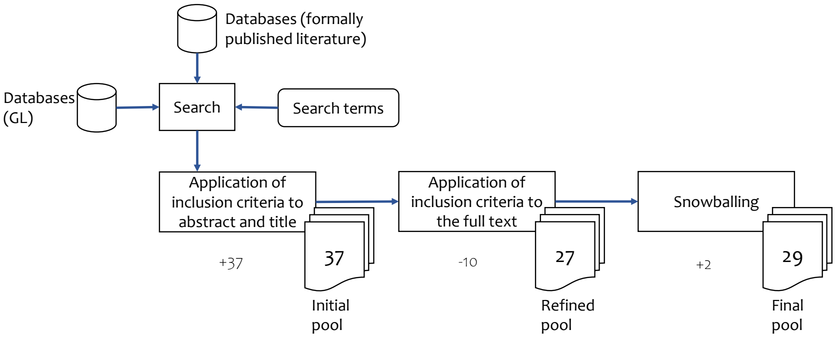
Databases (formally published literature)
Databases (GL)
Search
Search terms
Application of inclusion criteria to abstract and title
Application of inclusion criteria to the full text
Snowballing
+37
37
Initial pool
-10
27
Refined pool
+2
29
Final pool

Fig. 1. The search and selection process

3.3 Data Analysis

To evaluate the content of the 29 sources, we performed a qualitative content analysis (QCA) using MAXQDA.[2] QCA is a qualitatively oriented, category-based method that systematically condenses qualitative material, reduces complexity, and deciphers the meaning of qualitative data [70, 80, 101]. QCA does so by assigning text passages (coding units) to categories of a category system [101]. Several forms of QCA exist, and a decision regarding a specific technique depends on the project's research questions. For this study, we favored a content structuring QCA [70, 80]. A content structuring QCA allows for specific topics to be filtered out of the material and summarized [80]. The category system used in this method usually consists of deductive and inductive categories [70]. We derived some of our deductive categories by transforming the metrics (see Section 3.1) into categories. Additionally, competency classes (e.g., social, methodological, personal, and professional competencies), as well as the five CyBOK categories and 19 CyBOK knowledge areas [94] (see Table 1), were converted to categories that, together, formed a theoretically derived hierarchical category system.

When constructing a coding manual [80], we defined the categories and underpinned them with illustrative coding examples. Where required, coding rules were added to support coding decisions [101]. Additionally, we determined appropriate content analytical units (coding unit, context unit, and recording unit) for each research question. When coding competency statements, for example, we coded text snippets that clearly stated what an individual should be able to do. Thus, we coded competency statements such as *"develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process."* After coding the material with the main categories, subcategories were derived using inductive category formation, a strategy to derive categories from material [80]. This way, we developed a deductive-inductive, hierarchically structured category system that served as the basis for answering our research questions.

3.4 Building and Validating the New Competency Model

To build the competency model, we chose an empirical rather than theoretical approach [12] and followed best practice recommendations [20, 79]. The 27 models served as the data basis upon which we developed the new model, and the competency model analysis (see Section 3.3) served as the method for deriving the structure and content of the model. The developed category system already represented the structure of the competency model (i.e., it categorized the competencies according to competency clusters and dimensions). Thus, by converting the category system to a competency model, we obtained the structure of the model. Determining the granularity

[2] MAXQDA is a software for coding and analyzing qualitative data. Coding the material using MAXQDA makes the process of analysis more efficient and accurate. MAXQDA 2020 was used in this study.

of the competency model was another critical step in the construction process. Granularity concerns not only the number of competencies included but also the level of detail of each competency [20]. For the model to be exhaustive, we included a large number of competencies, namely 72. When determining the detail of a competency, we followed recommended guidelines [20, 79] and constructed a basic competency anatomy for every competency. Up to six behavioral indicators were selected to anchor the definitions [97]. Because of the coding process, competency categories were already assigned to behavioral indicators. We extracted the indicators and added them to the respective anatomies. In doing so, we avoided the frequently mentioned criticism of *"using empty, overly general phrases or a listing of meaningless buzzwords"* [102, p. 398].

The next step in the development process was to check and ensure curricular validity [59]. This validation step examined the extent to which the model's content corresponded to the curricular content. Other competency modeling studies [67, 68] have also regarded this step as essential. Because we are familiar with the cybersecurity education landscape in Austria and consider it representative, we used the Austrian information security and cybersecurity curricula as our basis. The collection process resulted in 10 curricula [154–163] that were analyzed according to content structuring QCA [70, 80]. To check curricular validity, we used the competency model as a deductive coding scheme. During the first coding session, similarly to [12], we found that the richness in detail of the content of the curricula varied, with many curricula only stating titles, topics, and content knowledge. Consequently, the corpus included many implicit competencies. Hence, we refined our coding rules to fit the data. In addition, whenever competency candidates not previously captured by the category system emerged, a new competency category was inductively developed [80].

4 COMPETENCY MODEL ANALYSIS

This section presents the results of the competency model analysis. First, the bibliographic and demographic results are given. Subsequently, the results regarding the content of the models are presented qualitatively and quantitatively.

4.1 Demographic and Bibliographic Aspects

Figure 2 shows the cumulative number of sources per year. In 2006, the first competency model containing security content emerged. Since this emergence, interest has steadily increased, peaking in 2017 and 2019. Excepting in 2009, competency models were released regularly, resulting in a continual supply of such models. As regards the publication type, most sources constituted GL (23). Only some of the models (6) were formally published. As shown in Figure 3, the GL published in this area surpassed the formally published literature many times.

In the next step, we examined which countries have produced the most competency models. To rank countries based on the number of models, we extracted the countries of the universities to which the authors belonged. If several authors from several different countries had developed a model, one credit for each country was assigned. Figure 4 shows the top countries in terms of the releasing of competency models. According to Figure 4, the United States significantly outnumbered the rest of the countries. Noticeably, only 17 countries contributed to the growing body of competency models. Moreover, international collaborations seemed to be the exception, as only two models were developed through collaboration.

To evaluate the influence of models in terms of citation count, we extracted the respective information from Google Scholar and Web of Science. Of particular interest was the relationship between the citations for each article and articles' years of publication. Showing the relationship, Figure 5 indicates that the actual citation count of the models depended on the database used. In effect, Google Scholar reported higher citation counts than Web of Science, while Web of Science indexed more models than Google Scholar. Contrary to expectations, recently published models were more influential than earlier work. Based on data from Google Scholar, the NICE

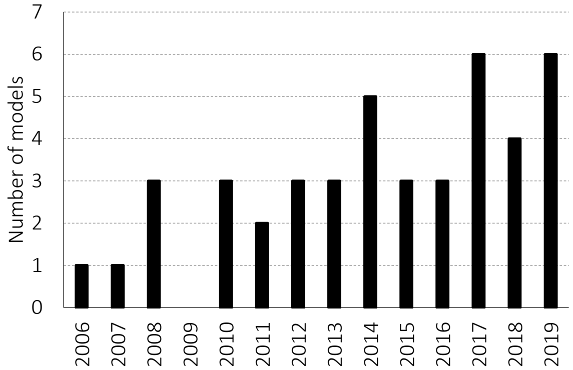

Fig. 2. Cumulative number of competency models per year. The Figure 2 contains the release dates of all versions of one model.

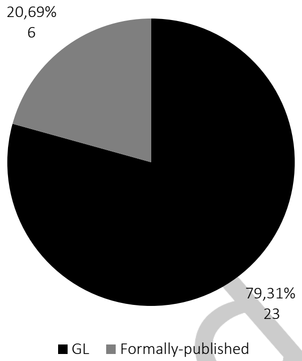

Fig. 3. Number of sources per type

Framework [140] led the list of the most influential models and was followed by the models of [142] and [147]. Concerning data provided by Web of Science, the model developed by [142] was cited the most.

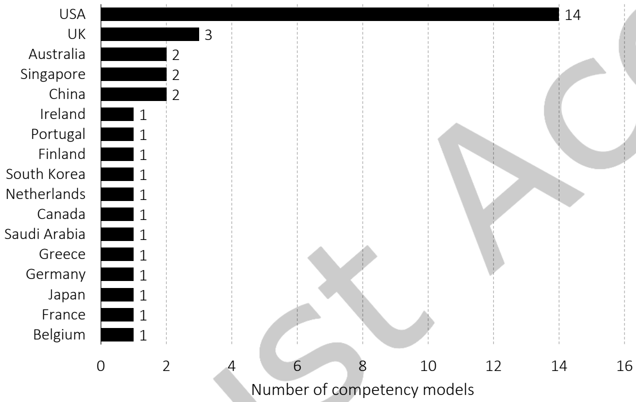

Fig. 4. Top countries based on authors' university affiliation

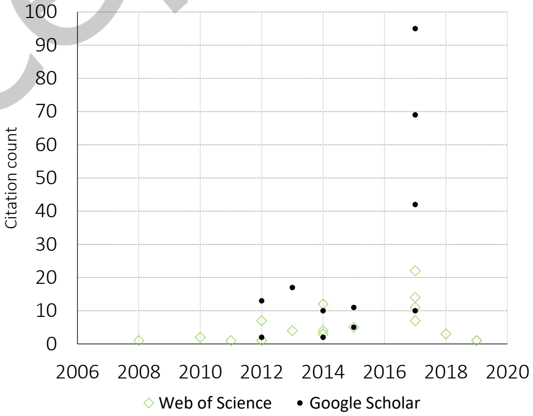

Fig. 5. Citations versus year. Each point represents a competency model.

4.2 Usages and Target Groups

We developed 18 categories describing the usages and applications of the competency models. According to the results, competency models provide several uses, ranging from performance management to policymaking. Table 4 provides an insight into the results, as well as descriptions and frequencies for all usages. As Table 4 indicates, the category "learning and competency development" led the list of the most frequently coded usages and was followed by the categories "assessment" and "development and evaluation of qualification programs."

Subsequently, several target groups were identified, including job seekers, technical professionals, HR experts, qualification providers, and students. To understand how target groups can use competency models, we investigated the relationships between the target groups' subcategories and the subcategories of usage by looking for co-occurrences. The findings indicate that most target groups can use competency models in several ways. Although market researchers and legislative bodies constitute target groups, the examination did not find any concrete use for these groups. Considering these findings, Table 5 presents a matrix that relates target groups to usages.

Table 4. Detailed description of use options (CF=category frequencies)

#	Category	CF	Description	Example(s) of coded segments
1	Learning and competency development	19	Competency models can help several target groups to develop competencies, set learning goals, and identify means to accomplish and evaluate these goals. Using competency models aids competency development in alignment with market needs and recognized standards. Furthermore, models support organizations and companies in aligning company strategy with competency development.	*"Within this context, the e-CF can also support: ICT professionals to show them what to be learnt and possible learning paths"* [131, p. 41]; *"The e-CF has [...] supported the alignment between the company's competence development and its business strategy"* [131, p. 11].
2	Assessment	16	Competency models support the application of assessments. Basically, two kinds of assessments can be distinguished: self- and external assessments. The self-assessment process can take place on an individual or organizational level. External assessments refer to the assessments of employees by a third person.	*"This Software Assurance (SwA) Competency Model was developed to create a foundation for assessing [...] the capability of software assurance professionals"* [135, p. VII]; *"It provides individuals with a framework for self-assessment [...]"* [126, p. 3].
3	Development and evaluation of qualification programs	16	Developing and evaluating qualification programs is a common application of competency models. Two kinds of qualification programs can be distinguished: educational and certification programs. With regard to the development of educational programs, models can be used to build entire competency-based curricula, develop concrete modules, develop learning materials, and plan lessons. One main advantage of using competency models is that the programs are tailored to market needs, which improves students' employability. Furthermore, models can be used to evaluate and validate existing programs.	*"The competencies outlined in the EBK become the basis for training 'modules' that can be fit into the specific course curriculum for each of the Department-defined key roles [...]"* [150, p. 4]; *"aligning curriculum to industry/employer needs and improving employability"* [145, p. 7]; *"For example, the core IT learning outcomes can be used by colleges to conduct periodic program reviews with the intent of validating their existing IT courses, certificates, and degrees, as well as to create new IT curriculum"* [134, p. 8].
4	Career management	13	Competency models can be used to manage careers. Job seekers and students can use models to discover industry-valued competencies. Competency models can be the starting point to exploring common job roles in cybersecurity. Technical experts can inform themselves about different career paths. Furthermore, models help to develop career pathways.	*" [...] to help job seekers and students understand which cybersecurity work roles and which associated Knowledge, Skills, and Abilities are being valued by employers for in-demand cybersecurity jobs and positions"* [140, p. 3]; *"provides guidance on a viable career pathway from entry-level data protection executives to regional data protection senior management roles"* [141, para. 1].
5	Recruitment and selection	11	Using competency models for recruitment and selection is beneficial to organizations. Not only is the use of models helpful in improving the efficiency and effectiveness of the process, but it is also helpful in developing competency-based selection criteria.	*"The Cyber Security Capability Framework is a tool that can be used in recruitment and selection"* [148, p. 9]; *"The opportunities for improving the efficiency and effectiveness of recruitment processes by adopting the European e-Competence Framework are significant"* [133, p. 15].
6	Job/role profiles and job ads	10	Competency models can be used to develop and improve job and role descriptions, as well as job advertisements. Models help to clarify the tasks, competencies, and responsibilities of a certain position and specify the sought-after competencies in job advertisements. A major advantage of using competency models is that the job/role profiles and job advertisements do not have to be built from scratch. Rather, the already developed competencies can be used as "building blocks" [131, p. 38] to create profiles.	*"The European e-CF describes competence and can be used in a variety of applications where consistency of competence language is required. These include job descriptions, role profiles [...]"* [131, p. 15]; *"Improve position descriptions and job vacancy announcements selecting relevant KSAs and Tasks, once work roles and tasks are identified"* [140, p. 3].

Table 4. Detailed description of use options (CF=Category frequency)

#	Category	CF	Description	Example(s) of coded segments
7	Guide to qualification programs	9	The qualification landscape is complex. Competency models can act as a guide to qualification programs, including education and certification programs. Competency models help to find the appropriate qualification programs to develop the appropriate competencies through suitable programs or to close competency gaps. For companies and specialists, this assistance is also important from a financial point of view because disinvestment can be avoided. Noticeably, some online tools acting as guides to qualification programs use the models as a basis.	*"Consequently, individuals can see opportunities for personal growth aided by the European e-CF and also select appropriate training programmes"* [131, p. 37]; *"Selecting appropriate educational programs and so on"* [137, p. 23]; *"addition, practitioners can use a competency model to provide guidance in selecting academic programs and training classes"* [125, p. 145].
8	Analysis of workforce and competency gaps	7	This category deals with two kinds of gaps: competency and workforce gaps. The qualitatively oriented competency gap analysis deals with the question of which competencies are currently available and which ones are required (in the future). Conversely, the quantitatively oriented workforce gap analysis can determine the gap between the workforce demand and supply. The analysis is not an end in itself. Instead, the analysis is followed by an effort to narrow the diagnosed gaps through appropriate training or hiring. The model by [125] is especially noteworthy, as it provides dedicated gap analysis worksheets.	*"Identifying competence gaps for future requirements is a significant application of the e-CF "* [131, p. 10]; *"The first spreadsheet (SWECOM Staffing Gap Analysis Worksheet) is for use by managers, human resources personnel, and others who analyze available and needed skills within an organizational unit"* [125, p. 25]; *"Assessment data can be combined to determine an organisational view of the skills capability that the organisation has and its skills needs, this characterises the 'skills gap' and by using a recognised framework it is less open to misinterpretation"* [145, p. 14].
9	Communication	6	Competency models not only help to improve communication within a company, but also communication between policymakers, qualification providers, HR experts, and the IT sector in general. An essential instrument for the establishment of improved communication is a common language. In fact, many models can be used to establish a common language.	*"Using the NICE Framework as a fundamental reference will improve the communication needed to identify, recruit, and develop cybersecurity talent"* [140, p. 2]; *"SFIA gives individuals and organisations a common language to define skills and expertise in a consistent way"* [145, p. 5].
10	(Strategic) personnel planning	5	Many models state their usefulness for personnel planning in general. Using competency models can assist organizations and companies with (strategic) personnel planning. Drafting and implementing plans related to workforce planning can be facilitated by competency models. Furthermore, competency models support the planning and anticipation of organizations' future personnel needs.	*"Referencing the NICE Framework will help organizations to accomplish strategic workforce planning [...]"* [140, p. 8]; *"The competencies identified may be used in such agency efforts as workforce planning [...]"* [127, para. 3].
11	HR development	4	By employing competency models, organizations and companies can improve human resource development. For instance, competency-based development plans aligned with organizations' goals can be drafted and implemented.	*"Organizations or sectors can use the NICE Framework to [...] define or provide guidance on different aspects of workforce development"* [140, p. 10].
12	Performance management	3	Using competency models can support organizations' performance management. In effect, models state their general supportive power regarding performance management without going into detail.	*"The competencies identified may be used in such agency efforts as performance management"* [127, p. 2].
13	Policymaking	2	This category emphasizes that competency models can be effective and useful tools for policy initiatives. For instance, the Netherlands used the e-CF [132] to develop its national e-skills strategy and Estonia used the e-CF as the basis for occupational qualification standards.	*"The examples from the European level, Estonia, the Netherlands and Ireland show how the e-CF can serve as a useful basis for policy making for the ICT workforce in different environments"* [131, p. 53].
14	Reward and compensation	2	Using competency models to reward and compensate employees is another useful application area. Included in this category are specific measures to implement reward and compensation mechanisms, such as job family models, job grading, and job evaluation. In essence, competency models can form the basis for such instruments.	*"It is essential that individuals and service providers are recognised for their performance, whether through salary and benefits, bonus schemes or feedback and SFIA can form the basis of such mechanisms"* [145, p. 15].
15	Talent management	2	Two models [145, 151] indicate that line managers and HR professionals can use them for talent management. Furthermore, this category covers succession planning, which is mentioned by SFIA [145].	*"Developing succession plans"* [145, p. 9]; *"[...] can be used to establish a baseline for the DHS Cybersecurity Workforce Initiative (CWI) and inform [...] talent management activities for cybersecurity roles across DHS"* [151, p. 4].
16	Instruction	1	This category deals with the possibilities offered by competency models in terms of the creation of group-specific instructional materials to support cybersecurity professionals.	*"A technology provider can then create appropriate support materials to assist members of the cybersecurity workforce in the proper configuration and management of their products"* [140, p. 14].

Table 4. Detailed description of use options (CF=Category frequency)

#	Category	CF	Description	Example(s) of coded segments
17	Developing models and mapping	1	In addition to using existing models, models can be used to create new models. Furthermore, models can be used to map qualifications and career pathways, for instance.	*"Creating discipline-specific competency frameworks aligned to a global standard"* [145, p. 10].
18	Organization design and target operating model	1	Designing and validating organizational structures and target operating models is another application area of competency models.	*"SFIA can be used to design and validate proposed organisation designs and target operating models"* [145, p. 11].

Table 5. Relationship between target groups and competency model usages

	Organizations & companies	Technical professionals	HR experts	Qualification providers	Managers	Students	Certification providers	Educational experts	Job seekers	Authorities	Policymakers	Consultants	Professional bodies	Leaders
Learning and competency development	X	X			X	X								
Assessment	X	X	X	X										X
Development and evaluation of qualification programs				X				X		X				
Career management	X		X			X		X	X					
Recruitment and selection	X		X											
Job/role profiles and job ads	X		X		X									
Guide to qualification programs	X	X	X		X	X	X							
Analysis of workforce and competency gaps	X	X	X			X						X		
Communication	X	X	X	X	X			X		X	X	X		
(Strategic) personnel planning	X		X		X									
HR development			X											
Performance management			X											
Policymaking											X			
Reward and compensation	X		X											
Talent management			X		X									
Instruction	X													
Developing models and mapping													X	
Organization design and target operating model												X		

4.3 CyBOK Categories and Knowledge Areas

As previously mentioned, the CyBOK [94] consists of 19 knowledge areas grouped under five categories. To evaluate the content of competency models, we transformed these categories and knowledge areas into a deductive category system and applied the system to the material. After the coding process, the categories were quantitatively evaluated. Figure 6 shows the category frequencies of the five CyBOK categories. The category "human, organizational, and regulatory aspects" topped the list of the most frequently coded knowledge areas and was followed by the CyBOK category "attacks and defenses." The categories "infrastructure security" and "systems security" were the least frequently named topics. Evaluating the codings quantitatively, we discovered an imbalance in terms of content. In fact, the competency models analyzed favored less technical content.

To further analyze the models' content, we conducted a simple configuration according to [70]. Figure 7 shows nine code configurations. Interestingly, the most frequent code configuration was formed by all five CyBOK

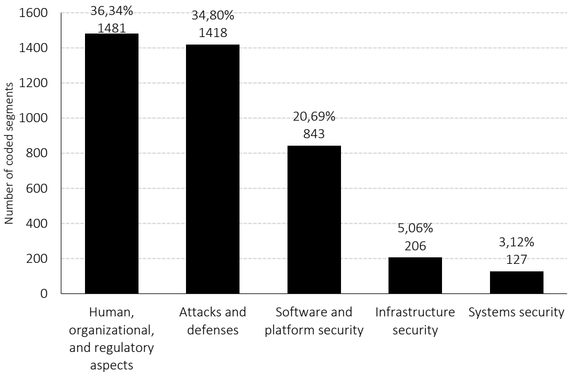

Fig. 6. Frequencies of the five CyBOK categories

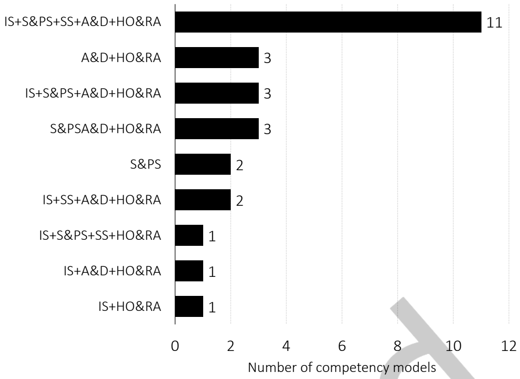

Fig. 7. Simple CyBOK code configurations. Abbreviations are used in the figure (HO&RA="human, organizational, and regulatory aspects"; IS="infrastructure security", etc.).

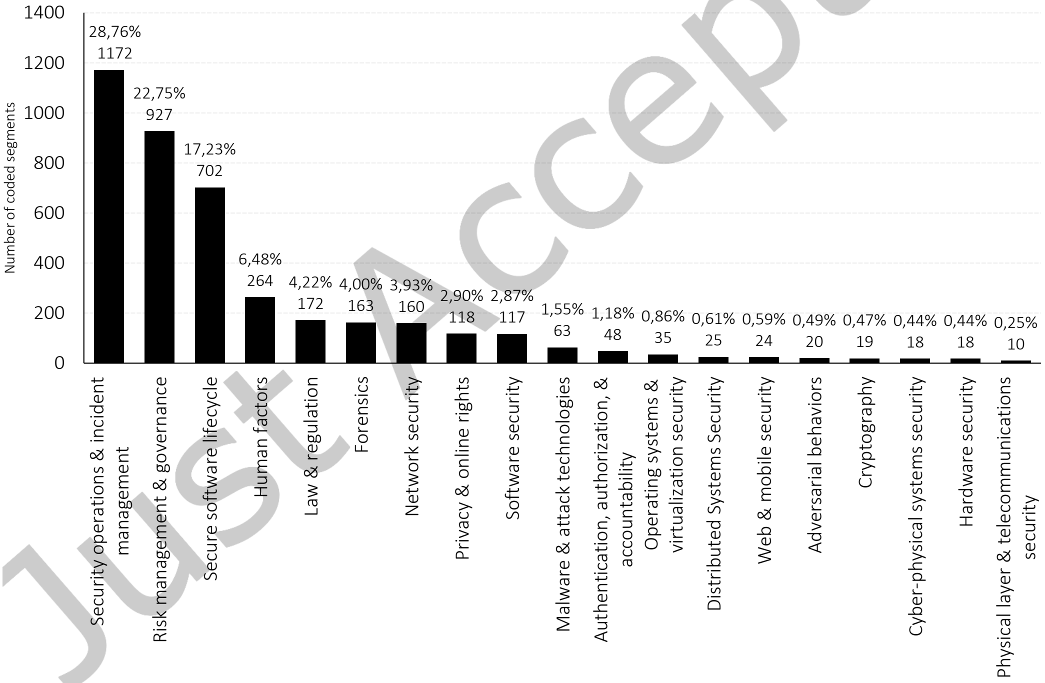

Fig. 8. Frequencies of the 19 CyBOK knowledge areas

categories. Put another way, many models included content covering a diverse set of knowledge and competencies, ranging from systems security to regulatory aspects. Excepting two models, most of the models included content related to at least two CyBOK categories. Moreover, the CyBOK category "human, organizational, and regulatory aspects" ran through all code configurations, excepting two. Similarly, most of the configurations, excepting three, contained the CyBOK category "attacks and defenses."

Separating the CyBOK categories into 19 knowledge areas allowed the content to be analyzed in more detail. After the coding process, the material was not only reduced to 19 categories describing the models' content from a bird's-eye view but also quantitatively evaluated. Figure 8 shows a bar chart revealing the category frequencies of the 19 CyBOK knowledge areas. The most frequently coded knowledge area was "security operations and incident management," which was followed by "risk management and governance" and "secure software lifecycle." Noticeably, the remainder of the categories occured to a considerably lesser extent. As with the five CyBOK categories, the quantitative evaluation of the 19 knowledge areas revealed an imbalance in terms of content coverage. By comparison, areas such as "risk management and governance" and "security operations and incident management" were emphasized much more than the more technically oriented areas, such as "hardware security" and "physical layer and telecommunications security."

4.4 Evaluation of Competency Models

Inspired by [91], we evaluated the competency models regarding content coverage. Assuming that the CyBOK knowledge areas represented the full range of possible cybersecurity topics, we used the 19 CyBOK categories as a deductive coding scheme to uncover the models' content coverage. Because models that integrate security content do not claim to be exhaustive, the evaluation process focused on stand-alone models. Table 6 presents the results of the evaluation. In Table 6, beginning with the oldest model, the models are ordered by date. It is to be noticed that Table 6 indicates the presence of a specific knowledge area, not the extent to which the models cover the knowledge area.

Table 6. CyBOK knowledge areas that are covered by information security and cybersecurity models

Release date	2008	2010	2011	2012	2013	2013	2014	2015	2017	2018	2019	2019	2020
Competency model reference	[150]	[148]	[127]	[151]	[135]	[149]	[130]	[144]	[140]	[138]	[153]	[136]	[141]
Physical layer & telecommunications security			X			X					X		
Cyber-physical systems security			X								X		
Hardware security		X	X						X				
Network security	X	X	X	X		X	X	X	X		X		
Secure software lifecycle	X	X	X	X	X	X	X		X	X	X		
Web & mobile security			X			X			X		X		
Software security	X		X	X	X	X	X	X	X	X	X		
Authentication, authorization, & accountability	X	X	X			X	X		X		X		
Distributed systems security			X								X		
Operating systems & virtualization security			X				X		X		X		
Cryptography			X			X	X		X		X		
Forensics	X	X	X			X	X		X	X	X	X	
Security operations & incident management	X	X	X	X	X	X	X	X	X	X	X	X	X
Adversarial behaviors				X					X		X		
Malware and attack technologies	X			X		X			X		X		
Risk management & governance	X	X	X	X	X	X	X	X	X	X	X	X	X
Privacy & online rights	X					X	X		X		X		X
Law & regulation	X	X	X		X	X	X	X	X	X	X		X
Human factors	X	X	X	X	X	X		X	X	X	X		
Number of covered knowledge areas	11	9	16	8	6	14	11	6	16	7	18	3	4
Number of missing knowledge areas	8	10	3	11	13	5	8	13	3	12	1	16	15

As shown in Table 6, none of the competency models were exhaustive (i.e., no model studied could be considered complete in terms of content coverage). Missing only one knowledge area, the Cybersecurity Competency Model [153] came closest to being complete. Additionally, the NICE Framework [140], as well as the Competency Model for Cybersecurity [127], omitted relatively few areas compared to other models, such as [136] and [141]. Consequently, some models offered a general view of cybersecurity, while others were better understood as specialized models. However, although models differed, all of the models contained content relating to the knowledge areas "security operations and incident management" and "risk management and governance." To a lesser extent, the knowledge areas "secure software lifecycle," "software security," and "human factors" also represented common ground. Lastly, each knowledge area was addressed by two models at least.

4.5 Definitions of the Concept of Competency and Proficiency Levels

In the next step, we coded all of the text passages that provided clarification on the concept of competency. Of the 27 models, only 10 actually defined the term explicitly; the rest refrained from doing so. To better understand the competency construct, we examined the characteristics of the coded passages. Inspection of Table 7 reveals that the term is associated with various features, ranging from learnability to measurability, yet no single coded definition of the competency construct contained all of the attributes listed in Table 7. Instead, the list serves as an overview of all of the possible characteristics that a definition of the term “competency” could provide. To further elaborate on the characteristic "gradual expression," we extracted the number of competency levels from each model. Table 8 shows that between two and seven competency levels were deployed to express different degrees of proficiency. Approximately half of the models did not group behavioral indicators into varying levels of proficiency.

Table 7. Characteristics of competency definitions

#	Characteristic	Example of coded segments
1	Learnability	*"Competency – A cluster of related knowledge, skills, and abilities that affects a major part of one’s job (a role or responsibility), [...] that can be improved through training, development, and experience"* [153, p. 4].
2	Contextualization	*"IT COMPETENCIES = (KNOWLEDGE + SKILLS + DISPOSITIONS) IN CONTEXT"* [147, p. 31].
3	Interplay of different attributes	*"The term competency represents the set of knowledge, skills, and effectiveness needed to carry out the job activities associated with one or more roles in an employment position"* [135, S. 3].
4	Measurability	*"Competency – A cluster of related knowledge, skills, and abilities, [...] that can be measured against well-accepted standards"* [153, S. 4].
5	Sustainability	*"Competence is a durable concept, [...] the e-CF remains durable requiring maintenance approximately every three years to maintain relevance"* [132, p. 5].
6	Gradual expression	*"Competency: the demonstrated ability to perform work activities at a stated competency level"* [125, S. 23].
7	Competency as a prerequisite for achievement	*"[...] the set of knowledge, skills, and effectiveness needed to carry out the job activities [...]"* [135, S. 3].

4.6 Competency Classes

A common way to categorize competencies is to use competency classes. After inductively constructing 240 competencies, we counted the competencies per competency class. As shown in Figure 9, the class "professional competencies" encompassing those competencies associated with the solution of domain-related technical problems was the largest general competency category. Examples of professional competencies are, inter alia, penetration testing, risk management, cloud security, and secure operating systems. While the analysis identified

Table 8. Competency levels and their frequencies

#	Number of competency levels	Number of models
1	2	1
2	3	2
3	4	1
4	5	5
5	6	3
6	7	1

a large set of professional competencies, only a few competencies were assigned to the classes "methodological competencies" (e.g., problem-solving), "social competencies" (e.g., teamwork), and "personal competencies" (e.g., self-control). Since only 13 methodological, 10 social, and 17 personal competencies were identified in the analysis, it can be stated that competency models included a limited variety of nonprofessional competencies required by security experts.

Subsequently, we conducted a simple code configuration [70] to analyze the relationship between competency classes and models. By performing a simple configuration, code combinations can be examined. In other words, code configurations provide information about which competency classes are present in the respective competency models. Inspection of Figure 10 reveals that of the 27 models, most models only included professional competencies (18). Conversely, only a small number of models (4) covered the complete range of competency classes. Moreover, all of the other possible code configurations were addressed by two models at most. Consequently, methodological, social, and personal competencies for security professionals were not only underrepresented compared to professional competencies in terms of variety but also seldomly covered in competency models in general.

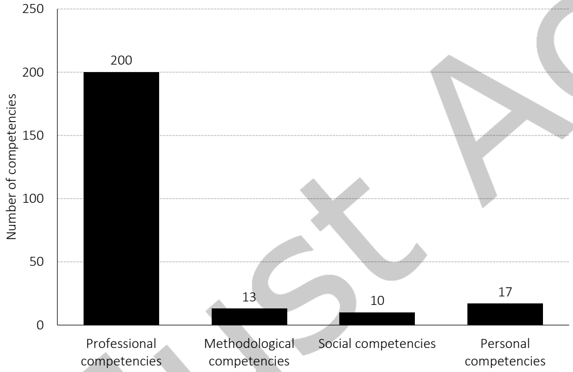

Fig. 9. Frequencies of competency classes

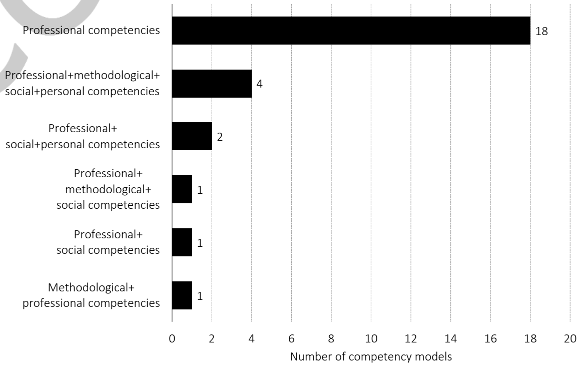

Fig. 10. Simple competency class configurations

4.7 Competencies

The analysis identified a unique set of 240 competencies. To elaborate on the competency descriptions for each of the 240 competencies, we conducted a category-based evaluation [70]. In essence, we listed all material under one category and summarized the material's meanings in a few sentences. When formulating the descriptions, we ensured that all definitions followed the same sentence structure and expressed the competency in an observable manner. Constructing all competencies based on this approach led to the formation of a competency pool, which can be found on Zenodo [8]. It is worth mentioning that the competencies extracted from the models did not prescribe any technologies to be used. Table 9 provides examples of competencies with their respective descriptions and associated knowledge areas. For instance, with regard to the competency "network defense," cybersecurity experts should be able to design, maintain, install, and apply a range of network defense systems. As regards the competency "secure design," experts should be able to apply different design principles and perform threat modeling. Regarding the competency "malware analysis and defense," security professionals are required to analyze different features of malicious software and combat malware.

To identify the category frequencies of each competency, we conducted a quantitative evaluation. By calculating category frequencies, a list of the 20 most frequently coded competencies could be produced. Inspection of Figure 11 reveals that while no competency was shared by all 27 models, the competency "risk management" topped the list of the most coded competencies and was followed by the competencies "risk assessment" and "incident management."

Table 9. Competency definitions

#	KA	Competency	Description
1	Network security	Network defense	The cybersecurity professional designs, maintains, installs, and applies a range of network defense systems, including firewalls, intrusion detection systems, network monitoring, network hardening, network access controls, and grid sensors to detect and respond to threats to protect networks and network traffic. The professional recognizes potential conflicts between systems and reports network events on a daily basis.
2	Software security	Prevention of software vulnerabilities	The cybersecurity professional practices defensive and secure programming and uses secure programming languages to prevent the introduction of software vulnerabilities. The expert is aware of the consequences associated with disregarding the rules on secure and defensive programming. The expert comments on and documents defensive programming practices and follows the rules of secure programming. He is able to develop new guidelines for secure programming and review and approve guidelines.
3	Secure software lifecycle	Secure design	The cybersecurity professional follows recommended design principles for creating secure systems and uses secure design patterns. The expert understands, evaluates, compares, and applies a number of secure design principles (e.g., open design, isolation, mediation, least privilege). The expert performs threat modeling and identifies the attack surface of the systems. The expert is able to incorporate various security strategies (e.g., defense in depth, access control mechanisms, and encryption of sensitive data) into the design and ensures a balance between security, functional, and quality requirements.
4	Malware & attack technologies	Malware analysis & defense	The cybersecurity professional is able to analyze the behavior, capabilities, interactions, intentions, features, and characteristics of malicious software and threats. The professional is also able to develop and successfully apply defense and mitigation strategies and techniques to combat malware. He performs static and dynamic analyses and isolates and removes malware.

Interestingly enough, the competencies listed were associated with only eight areas of expertise: "risk management and governance," "security operations and incident management," "network security," "human factors," "law and regulations," "forensics," "secure software lifecycle," and "software security." The remaining knowledge areas are not covered in Figure 11. Similarly, nonprofessional competencies, such as teamwork and stress tolerance, do not appear on the list. Consequently, the ranking of competencies shows that not only was the level of diversity of nonprofessional competencies lower than that of professional competencies but that their level of importance was too.

5 NEW COMPETENCY MODEL

This section introduces an evidence-based competency model for information security and cybersecurity professionals. The section presents the details of the design, which are followed by the results of the validation stage.

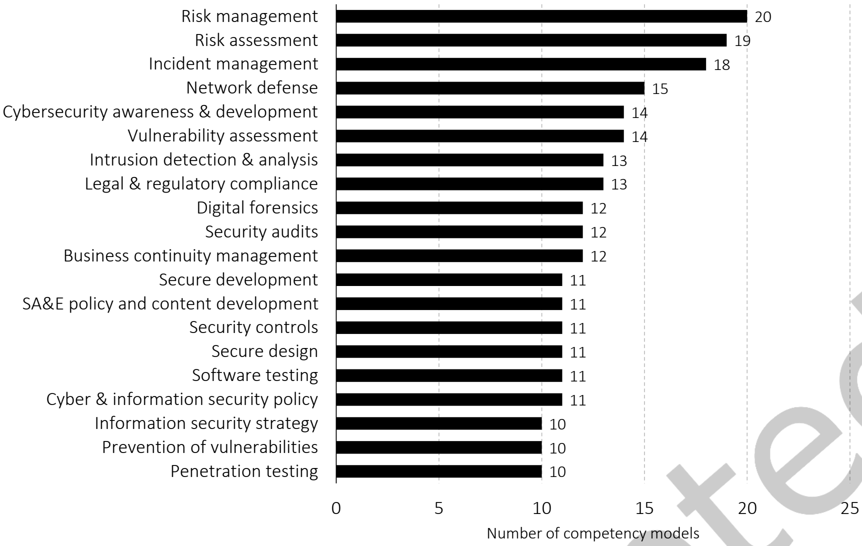

Fig. 11. Frequencies of the top 20 competencies

5.1 Competency Model for Information Security and Cybersecurity Professionals

By transforming the empirically developed category system into a competency model, we produced the competency model for information security and cybersecurity professionals, which is shown in Figure 12. The four competency classes serve as the high-level structure of the model. Unlike the nonprofessional competency classes, the professional competency class was divided into additional subcategories according to the structure of the CyBOK. As the CyBOK areas were insufficient to incorporate all of the identified competencies, we added three additional areas: physical security, job-specific skills, and CyBOK introduction. The latter refers to the foundational professional competencies of the security domain. The competency dimension of job-specific skills highlights the need for professional competencies beyond the security domain (e.g., technology watching). By design, the model incorporates not only professional competencies but also social, personal, and methodological competencies, thereby providing a holistic view of the competency profile of an cybersecurity expert. Furthermore, the model can be considered exhaustive, as the model's content covers all of the CyBOK knowledge areas. In that regard, the proposed model is unique. As previously shown, none of the existing models fulfill this criterion.

When constructing the model, we did not include all 240 competencies. Instead, we selected the three most frequently mentioned competencies per knowledge area from the generated pool. This approach is in line with the advice of the scientific literature, which recommends a manageable number of competencies [20, 75]. In sum, the model displays 72 competencies, which are underpinned with up to six competency indicators expressing the competency in action. While we set a size limit, we consider this model to be a minimal framework that is expandable. For example, additional competencies from the competency pool could be added to the model. Regarding the definition of the competency construct, the model refers to the definition of [116]. Due to limited space, the full model, an in-depth description, and key data are provided online [8].

5.2 Curricular Validation

Overall, the model proved to be applicable to the categorization of the curricular content of 10 Austrian security programs. When checking for curricular validity, we found that most of the content of the 10 Austrian curricula

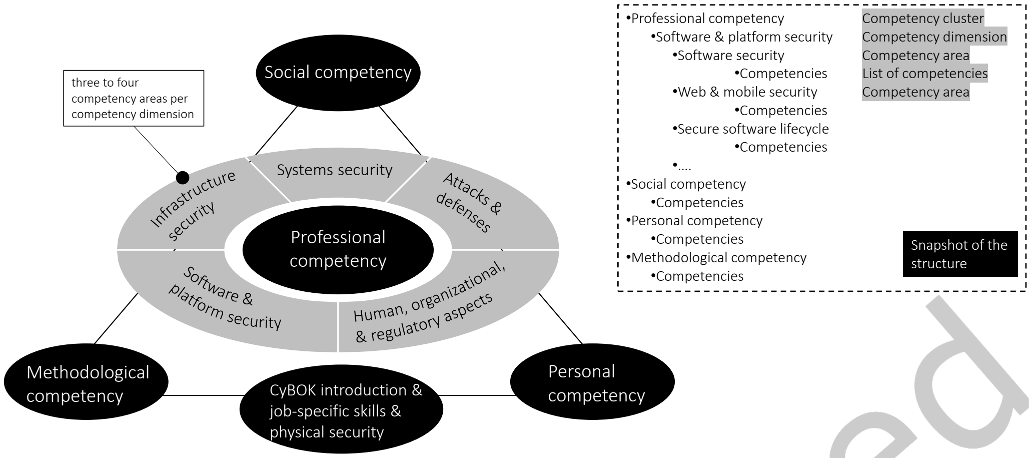

Fig. 12. The left part of the graphic shows the model from a bird's-eye view, while the dashed box outlines the internal structure of the model (i.e., how competencies are organized).

could be integrated into the competency model. Consequently, the competencies of our model matching with competency aspects of the curricula reflect a significant number of abilities that are thought to be relevant to information security and cybersecurity experts and can be considered as approved on that basis. Table 10 provides a brief overview of the coding results. However, 11 competencies of the competency model for information security and cybersecurity experts were not mentioned in the curricula (e.g., customer service and technical support, hardware testing, secure hardware design, personal information, and creative thinking). At the same time, it also became apparent that it was impossible to integrate all curricular content into the model immediately, and some of the competencies suggested in the curricula were missing from the proposed model. Hence, 25 new competencies had to be developed inductively to be able to integrate all of the curricular content. Table 11 provides an insight into some of the newly developed competencies. Concerning the competency areas and dimensions, the structure of the model proved to be sufficient to categorize the competencies emerging from the curricular analysis.

Table 10. Coding results of the validation stage

#	Competency	Coded segment(s)
1	Research	This course teaches students about the basic principles of scientific work in the field of applied computer science [155].
2	Network defense	Firewalling and packet filtering (stateless filtering and stateful packet inspection) [159]; students can select security components, such as firewalls, demilitarized zones and VPN gateways for the corresponding requirements and integrate them into existing networks [161].
3	Secure development	Students should learn the basic software engineering principles for the development of secure software systems [155]; secure software development UE [154]; the graduate of this module has detailed knowledge in dealing with security requirements during the entire software development process [158].
4	Prevention of vulnerabilities	At the end of the ILV, students can define, combine and use suitable data structures (in the C programming language) for storing and manipulating information in such a way that no security vulnerabilities occur [161]; secure coding [160]; they know basic methods of secure programming in C and can also apply them [157].
5	Risk assessment	The course teaches widely used approaches and techniques for identifying, analyzing, assessing, presenting and, communicating risks [161]; be able to independently conduct risk analyses or lead RA projects and be able to follow and help to shape future developments [158].
6	Legal & regulatory environment	Introduction to the basics of law (structure of the legal order/demarcation between public and private law) [161].

Table 10. Coding results.

#	Competency	Coded segments
7	Web & mobile defense	Mobile security [156]; hardening using HTTP Header [162]; students can identify the security mechanisms used in current mobile systems (e.g., Android, iOS) [157].
8	Teamwork	They are able to convincingly work in a team [156]; graduates of the Master's program must be able to work effectively in teams [163].
9	Cryptographic overview	Basics of applied cryptography [156]; the lecture covers basic concepts of cryptography, methods of classical cryptography [154].
10	Encryption	Theoretical and practical knowledge of symmetric and asymmetric cryptography and its most important procedures and algorithms [161]; basic procedures for encrypting and decrypting data [154].

Table 11. Inductively derived competencies during curricular analysis

#	Competency	Coded segment(s)
1	Self-reflection	Self-reflection [159]; the spectrum ranges from accompanying personality development to reflections [158].
2	Transferability	Transferability: Translating theoretical learning into practical action and at the same time recognizing the possibility and limits of application [161].
3	Economics & ethics	Ethics in economics [154].
4	Corporate culture	After successful completion, students are able to understand the importance of 'culture' for a company [162].
5	Physical layer	Electrotechnical basics for data transmission [161].
6	IoT security	Security in the IoT: threat model in the IoT, concrete attack scenarios, security concepts at organizational and technical levels for manufacturers, service providers, and consumers [158].
7	Embedded security assessment	Embedded security assessment [155].
8	Computer architecture	Boolean algebra, conceptual framework of computer architecture, components of modern computer systems, computer models (von Neumann, Harvard), RISC, CISC, memory hierarchies, memory addressing [157].
9	Data science skills	Sample design, statistical data collection planning, data selection [159].
10	Modeling malicious operations	Classify the attack techniques in the cyber kill chain (R) [162]; cyber kill chain (R), unified kill chain [162].

6 DISCUSSION

In this section, we highlight the contribution of our work and relate our results to previous efforts. Additionally, we discuss use cases of the proposed competency model. The section concludes with a reflection on the limitations of the study.

6.1 Discussion in the Context of Literature

To better understand the field of information security and cybersecurity competency modeling, we explored competency models' characteristics using a QCA. This study addresses the limitations of previous efforts. First, unlike related research, this study analyzes a broad array of competency models, namely 27. Previous research on competency modeling in the information security and cybersecurity domains and beyond [113] has focused on a smaller set of models, ranging from one model [14] to 14 models [111]. Second, this study adopts a systematic research method to uncover new, previously missed insights into competency modeling.

First, this study provides a complementary contribution to the discussion on the importance of cybersecurity topics. From this perspective, the competency models' creators consider "human, organizational and regulatory aspects" to be more important than knowledge about "systems security" and "infrastructure security." Diving deeper, we found that less technical content, such as "risk management and governance," was emphasized more than more technical areas, such as "cyber-physical systems security" and "hardware security." These results are in line with recent work. Mapping four curricula against the CyBOK knowledge areas, Hallett et al. [48] also noticed an overemphasis on the areas "risk management and governance" and "security operations and incident management" in comparison with more engineering-focused areas. Similarly, Cabaj et al. [17] analyzed cybersecurity master's programs and identified an increased interest in less technical content, such as human, societal, and organizational security. Nevertheless, from the results of other work, we can see that the discussion on the importance of topics continues to be a source of debate. For instance, the work by [86] highlighted the importance of privacy, ethics, operating system security, and the rooting of trust in hardware. However, the CyBOK knowledge areas covering these topics are underemphasized in competency models. Another piece of work [107] analyzing the content of 71 cybersecurity education papers suggested that human, societal, and organizational security are much less important than data security and connection security, for example. In contrast, the present study rather suggests the opposite. Hence, what constitutes the core topics remains controversial at this point.

Next, the findings regarding the competency classes suggest an imbalance that could have profound consequences. Studies analyzing job advertisements have agreed that employers value professional competencies, as well as social, personal, and methodological competencies [13, 87, 92, 93]. In addition, a recent review of the cybersecurity workforce's future has argued that the skill set of cybersecurity experts must consist of more than just technical skills [27]. However, social, methodological, and personal competencies are not only underemphasized in number but are also completely missing from many competency models. Consequently, most of the studied competency models paint an incomplete picture of the competencies required in the security domain. Indeed, if security professionals lack personal and social competencies, they may not be successful at work. As discussed by [27], lifelong learning is a valuable personal competency, and the absence of a commitment toward lifelong learning could render a security professional useless as the technology and threat landscape changes. Similarly, an inability to communicate complex security issues to nontechnical personnel and a lack of team playing skills reduce job performance [27]. Therefore, most of the analyzed competency models are only partially suitable for curriculum and workforce development, as they miss essential competency dimensions. Purely subject-oriented competency models must not be the only basis for curriculum and workforce development; they must be complemented by other sources.

The evaluation of the models' content coverage pointed to a similar problem. As some models provided a general view of the domain and others were better understood as specialist frameworks, curriculum designers must carefully select models for curriculum design. For instance, if a designer wishes to build a program providing a holistic view of the security domain and chooses [136] or [141] as the basis, they could achieve the opposite. Conversely, these models could meet expectations if a specialist focus were to be desired. As information about the content of models is crucial for the selection process, we believe that the information provided in Table 6 would facilitate decision-making.

In accordance with previous efforts [13, 15], our work suggests that more professional competencies are required in terms of variety than nonprofessional ones (e.g., methodological, social and personal competencies). In addition, our findings stress the importance of professional competencies. However, the analysis of job advertisements by [13] showed that teamwork was the most frequently sought-after competency of a security professional. In addition, the work of [118] and [93] underscored the importance of soft skills. The World Economic Forum's list of the top 10 most in-demand skills across industries also stressed the importance of nonprofessional competencies [121]. Nonprofessional competencies, however, do not appear in our top 20 list. However, concerning the importance of domain-specific professional competencies, our results comply, to a large extent, with the results reported in the literature. Similarly to our work, previous work has also suggested that competencies related to risk [13, 55, 93], networks [61, 93], incidents [13, 123], audits [13, 93], vulnerabilities [13, 61], and compliance [13] are among the most important competencies required by security professionals. In summary, while our results disagree with those of related work on the importance of nonprofessional competencies, the findings regarding the importance of professional competencies agree with those of the literature.

Furthermore, this study adds to the discussion on what characterizes a competent cybersecurity professional. First, unlike other efforts [13, 93], we underpinned the competencies with a thick description in an observable manner to provide clarification and avoid confusion. Second, we substantially expanded the set of competencies required in the industry and painted a more nuanced picture of the profession. However, the vast number of competencies could also be indicative of challenges for educational programs. Because a single program cannot promote all 240 competencies, curriculum designers must carefully select the competencies that are most important for security jobs [61].

Lastly, the findings suggest that competency models could help to tackle the skills gap. Given their uses related to competency development, workforce development, and curriculum design, competency models can help to address many of the pressing issues and challenges facing the cybersecurity education system and the labor market, including outdated curricula [18], the low responsiveness of the education system to changes in the cyber domain [10], the poor alignment between educational and industry requirements [28, 47], the insufficient communication between employers and educational institutions [26], the difficulties in hiring and retaining employees [55], the lack of investment in employees [26, 28], and the lack of clear career pathways [18]. Since competency models are applicable to the education system and the labor market, they can support the elimination of deficits with regard to supply and demand, which, in sum, are at the root of the shortage in skills [28]. With regard to employers, competency models, for example, can help to ensure and sustain the professional development of employees by facilitating the identification of skills gaps and ways to address them, supporting the identification of appropriate training opportunities, and providing a means to manage talent and plan succession. With regard to supply, competency models can support the construction and evaluation of educational programs. By mapping the curriculum against a competency model, curriculum designers can identify gaps and ways to address them. In addition, competency models can complement proactive, cost-effective curriculum maintenance strategies based on monitoring and integrating changes to certification schemes [65]. Competency models are frequently updated (e.g., the e-CF and the Cybersecurity Competency Model), and considering such updates can strengthen curriculum maintenance efforts. In terms of curriculum design, the models facilitate discussion among key stakeholders and provide a clear indication of what cybersecurity professionals should be able to do. Additionally, competency models help to advance the professionalization of individual security occupations. Because a spectrum of different cybersecurity occupations exists, Burley et al. [16] argued against oversimplified one-size-fits-all professionalization mechanisms and recommended tailored occupation-specific activities. When considering occupation-specific activities, competency models can be used to identify occupation characteristics (e.g., competency requirements) and deficits (e.g., competency gaps). Using competency models also addresses some of the disadvantages associated with professionalization activities, such as high barriers to entry based on credentials [16]. In fact, the notion of competency highlights a worker's actual capacity and job readiness in terms of competencies rather than formal achievements, which provides opportunities for people who have not undertaken formal training but have nevertheless developed competencies informally to enter the cybersecurity labor market [16, 71]. Therefore, we believe that the competency model analysis helps to address workforce issues, especially the qualitative aspects of the issues.

6.2 Application Scenarios

In this section, we wish to draw attention to the potential applications and uses of the competency model for information security and cybersecurity professionals. In principle, the model can be used in all application scenarios identified during the competency model analysis. However, here, rather than discussing all applications in detail, we focus on two important application scenarios and conclude by highlighting the model's ability to narrow the skills gap. Tailoring the model to the concrete context could be beneficial when using the framework. For example, organizations could pick competencies linked to their missions and goals [20]. Educational staff might wish to adapt the model to fit with the regional and national contexts or the institute's capacities.

Developing and evaluating qualification programs is one of the main applications of the competency model. The competencies of the model used to define programs' learning outcomes constitute in-demand abilities that are not technology-specific. Consequently, curricula based on those competencies not only align with industry needs but are also more sustainable than curricula focusing on specific tools, as they are less subject to technological advances [13]. Moreover, as pure knowledge is insufficient to meet industry expectations [103], educational programs must provide opportunities to develop competencies. To support competency development, educational experts must rethink the learning culture. Competencies cannot be traditionally taught and they can only be developed through hands-on experience in authentic learning environments [63]. Authentic learning environments and tasks can be constructed using the competency model's behavioral indicators. These indicators suggest how a competency unfolds in action and provide guidance for creating test items and learning tasks.

The nature of the learning task (well-defined versus ill-defined) and the learner's familiarity with the task are hypothesized to influence the integration process of knowledge, skills, and attitudes (e.g., low-road integration and transformative integration) [5]. Hence, designers should think carefully about the nature of the task. In addition to serving as a tool for the creation of new curricula and content, the competency model is helpful in analyzing existing programs. As outdated curricula are seen as one rationale for the shortages in the security workforce [29, 94], evaluating the currency of curricula is imperative. The proposed model provides a holistic and up-to-date view of the security domain, making the model particularly useful in evaluating educational programs.

Competency models form the basis for competency-based HR management in organizations. Competency-based HR management aims to inform and improve HR systems, including recruitment and selection systems [3]. Evidence has suggested that recruiting competent cybersecurity experts is challenging for organizations [29, 55]. Our model can help to improve the effectiveness and efficiency of recruiting and selecting talent inside and outside the organization. By using the model's competencies as building blocks for constructing job profiles, recruiters do not have to build profiles from scratch. Moreover, the competency model helps to build attractive job descriptions. Because the competencies have been defined and anchored with indicators to avoid misunderstandings, they are particularly useful in communicating an organization's needs and attracting candidates who fit the profile. However, when informally studying job advertisements, we found that many organizations do not use a structured process to convey the meaning of competencies. By using the model, organizations can avoid this problem. Additionally, the competencies can be used in competency-based interviews during selection. Again, the behavioral indicators are particularly useful for this process and should help HR experts to decide which candidate should be appointed to the job in question. Consequently, using the model reduces the risk of recruiting and selecting the wrong people, thereby helping to avoid increased costs.

Moreover, the competency model can facilitate other approaches to narrowing the skills gap. For example, some organizations do not exactly know which qualifications and certifications are required for a particular job [42]. By mapping the qualifications and certifications against the competency model, organizations can determine which competencies are actually covered by the educational programs and sort out those requirements and certifications in the job advertisements that do not fit the role. This way, organizations can avoid mismatches [42]. Similarly, by mapping external educational platforms against the model, organizations can compare their offerings and find the training that best fits employees' training needs. In doing so, organizations ensure cost-effective professional development and retain indispensable personnel. To satisfy workforce needs, the literature has also recommended the hiring of applicants with nontraditional backgrounds [26]. In this case, the competencies of the model are well suited to the assessment and validation of the person's abilities and support decision-making regarding the applicant's employability. With regard to education, using the model to align industry requirements with educational efforts facilitates the development of cybersecurity experts with sought-after competencies who successfully transition from an academic environment to the industry. To resolve the tension between education and training [24], which represents a long-standing issue in alignment efforts, educational designers can construct authentic learning environments through practical tasks, group work, or internships, for example, using the model's competencies. Lastly, the model can serve as a source of input for future competency-based cybersecurity curriculum guidelines and standards.

6.3 Limitations

The main issues related to threats to the validity of this article are an inaccurate category system and an incomplete dataset. Potential issues during the process of searching for and selecting sources can arise from limitations of the search terms, the databases used, and biases when applying inclusion and exclusion criteria. To minimize biases when applying inclusion criteria, we discussed controversial sources as a team and made consensus-based decisions. To minimize the risk of sources being missing, we used formal search terms and considered synonyms, which was followed by full forward and backward snowballing. Moreover, we used a wide range of databases to avoid issues resulting from the limitations of the search engines. The exclusive use of Austrian curricula to validate the competency model threatened external validity. The question concerns whether the curriculum corpus is up to date and covers all types of competencies. In that respect, we argue that the curricula contained enough information to map almost all of the competencies of the competency model. Hence, we are confident that the outcome of these processes constitutes a solid and inclusive basis.

Now, we wish to discuss the validity of the category system. Concerning inductive categories, signs of validity issues are high coding frequencies of residual categories, disproportionately high coding frequencies of subcategories, and disproportionate abstract categories [101]. The validity of the inductive categories is supported by the fact that no residual categories were used. Furthermore, disproportionately high frequencies for one subcategory within a main category were absent in most cases. However, in cases where they were not absent, we are confident that it was not a sign of an undifferentiated category but rather an empirical finding. This assumption is supported by the sheer number of inductive categories, which also indicate appropriate abstraction and differentiation. For evaluation, the second author, who was familiar with the study's objectives and the procedure of content analysis, reviewed the category system so that the coding frame could also be considered valid from an expert's perspective. Hence, we consider the validity of the category system as approved.

7 CONCLUSION

This work focuses on analyzing competency models related to the information security and cybersecurity domains and also introduces an evidence-based competency model for information security and cybersecurity professionals. The work's findings shed light on several previously missed characteristics and provide new insights into the current state of security competency models. According to the results, target groups can use the models in many different ways, from policymaking to performance management. Thematically, the models emphasize the CyBOK knowledge areas "security operations and incident management" and "risk management and governance." Less attention is paid to more technically oriented knowledge areas, such as "hardware security." In this work, in total, we extracted 240 competencies from existing models, with most of the competencies falling into the class "professional competencies." As many models only reduce the qualities of a security expert to professional competencies, they paint an inaccurate picture of the security domain. Additionally, the studied models are not exhaustive in terms of content coverage. Addressing these limitations, the proposed competency model provides a holistic view of the security domain by including content covering the full range of competency classes and CyBOK knowledge areas. In sum, the model and its competencies are up to date and have already undergone a process of validation.

Our future work will include investigating and exploring the effectiveness of the proposed model in empirical studies to consider implications concerning the usefulness of the model in practical settings. Furthermore, we would like to assess individuals' general awareness of competency models in organizational and educational contexts. Additionally, we plan to analyze job advertisements based on a category system derived from the competency model. Lastly, the maintenance of the competency model using, for example, focus groups, online surveys, or subject matter expert groups is necessary to ensure the currency and long-term usefulness of the competency model. To enhance maintenance efforts and stimulate scientific investigation, we have compiled a designated maintenance and replication package [9].

ACKNOWLEDGMENTS

This publication was partially supported by the Erasmus+ project MIDSISE - Meeting Industrial Demand for Skills in Information Security Education (reference number 2019-1-LI01-KA203-000130) funded by the European

Commission as well as the project PROMIS - Customized courses for professionals in security (reference number 20210026) funded by the Knowledge Foundation of Sweden.

REFERENCES

[1] Heimo H. Adelsberger, Ulf D. Ehlers, and Dirk Schneckenberg. 2008. Stepping up the Ladder - Competence Development Through E-Learning?!. In *Proceedings of ED-MEDIA 2008 - World Conference on Educational Multimedia, Hypermedia & Telecommunications* (Vienna, Austria, June 30-July 4, 2008), J. Luca and E. Weippl (Eds.). AACE, Chesapeake, VA, USA, 4068–4082.

[2] Jason Andress. 2019. *Foundations of Information Security: A Straightforward Introduction.* No Starch Press, San Francisco, CA, USA.

[3] Michael Armstrong and Stephen Taylor. 2014. *Armstrong's handbook of human resource management practice* (13. ed.). Kogan Page, London, UK.

[4] Miriam E. Armstrong, Keith S. Jones, Akbar S. Namin, and David C. Newton. 2020. Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Transactions on Computing Education* 20, 4 (2020), 1–25. https://doi.org/10.1145/3421254

[5] Liesbeth K.J. Baartman and Elly de Bruijn. 2011. Integrating knowledge, skills and attitudes: Conceptualising learning processes towards vocational competence. *Educational Research Review* 6, 2 (2011), 125–134. https://doi.org/10.1016/j.edurev.2011.03.001

[6] Mike Barkmin and Torsten Brinda. 2020. Analysis of Programming Assessments — Building an Open Repository for Measuring Competencies. In *Koli Calling '20: Proceedings of the 20th Koli Calling International Conference on Computing Education Research* (Koli, Finland, November 19-22, 2020) *(Koli Calling '20)*. ACM, New York, NY, USA, Article 31, 10 pages. https://doi.org/10.1145/3428029.3428039

[7] Victor R. Basili, Gianluigi Caldiera, and Dieter H. Rombach. 1994. The Goal Question Metric approach. In *Encyclopedia of Software Engineering*, John J. Marciniak (Ed.). John Wiley & Sons, New York, NY, USA, 528–532.

[8] Daniel Bendler and Michael Felderer. 2022. *Competency Pool and the Competency Model for Information Security and Cybersecurity Professionals*. Zenodo. https://doi.org/10.5281/ZENODO.4765645

[9] Daniel Bendler and Michael Felderer. 2022. Maintenance/Replication Package. https://doi.org/10.5281/ZENODO.5913477

[10] Borka J. Blažič. 2021. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society* 67 (2021), 101769. https://doi.org/10.1016/j.techsoc.2021.101769

[11] British Computer Society. 2020. *SFIAplus - IT skills framework.* BCS. Retrieved June 6, 2020 from https://www.bcs.org/membership/sfiaplus-it-skills-framework/

[12] Kathrin Bröker and Johannes Magenheim. 2014. Are there competences every computer scientist should have?. In *2014 IEEE Global Engineering Education Conference (EDUCON)* (Istanbul, Turkey, April 3-5, 2014). IEEE, 999–1002. https://doi.org/10.1109/EDUCON.2014.6826224

[13] Nita G. Brooks, Timothy H. Greer, and Stevens A. Morris. 2018. Information systems security job advertisement analysis: Skills review and implications for information systems curriculum. *Journal of Education for Business* 93, 5 (2018), 213–221. https://doi.org/10.1080/08832323.2018.1446893

[14] Jason Brown. 2020. An examination of the Skills Framework for the Information Age (SFIA) version 7. *International Journal of Information Management* 51 (2020), 102058. https://doi.org/10.1016/j.ijinfomgt.2019.102058

[15] Jason Brown and Alan Parr. 2018. ICT Skill Frameworks: Do They Achieve Their Goals and Users' Expectations? *Advanced Journal of Professional Practice* 1, 2 (2018), 38–47. https://doi.org/10.22024/UNIKENT/03/AJPP.506

[16] Diana L. Burley, Jon Eisenberg, and Seymour E. Goodman. 2014. Would cybersecurity professionalization help address the cybersecurity crisis? *Commun. ACM* 57, 2 (2014), 24–27. https://doi.org/10.1145/2556936

[17] Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, and Ana Respício. 2018. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security* 75 (2018), 24–35. https://doi.org/10.1016/j.cose.2018.01.015

[18] Tracey Caldwell. 2013. Plugging the cyber-security skills gap. *Computer Fraud & Security* 2013, 7 (2013), 5–10. https://doi.org/10.1016/S1361-3723(13)70062-9

[19] Anthony F. Camilleri. 2011. A report on e-Competence Frameworks: For the Malta Information Technology Agency MITA. Retrieved March 23, 2020 from https://knowledgeinnovation.eu/wp-content/uploads/2015/05/MITA-eCompetences-Master-2.pdf

[20] Michael A. Campion, Alexis A. Fink, Brian J. Ruggeberg, Linda Carr, Geneva M. Phillips, and Ronald B. Odman. 2011. Doing competencies well: Best practices in competency modeling. *Personnel Psychology* 64, 1 (2011), 225–262. https://doi.org/10.1111/j.1744-6570.2010.01207.x

[21] careeronestop.org. 2015. Competency Models In Action: College Uses Cybersecurity Competency Model to Align and Create Curricula. Retrieved March 3, 2021 from https://www.careeronestop.org/CompetencyModel/Info_Documents/Excelsior-CaseSummary.pdf

[22] CC2020 Task Force. 2020. *Computing Curricula 2020: Paradigms for Global Computing Education (CC2020).* ACM, New York, NY, USA. https://doi.org/10.1145/3467967

[23] Committee on National Security Systems. 2010. National Information Assurance Glossary. Retrieved January 22, 2021 from https://www.hsdl.org/?view&did=7447

[24] Wm. Arthur Conklin, Raymond E. Cline, and Tiffany Roosa. 2014. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *2014 47th Hawaii International Conference on System Sciences* (Waikoloa, HI, USA, January 6-9, 2014). IEEE, Los Alamitos, CA, USA, 2006–2014. https://doi.org/10.1109/HICSS.2014.254

[25] Carlos Costa and Maribel Y. Santos. 2017. The data scientist profile and its representativeness in the European e-Competence framework and the skills framework for the information age. *International Journal of Information Management* 37, 6 (2017), 726–734. https://doi.org/10.1016/j.ijinfomgt.2017.07.010

[26] William Crumpler and James A. Lewis. 2019. *The Cybersecurity Workforce Gap.* Center for strategic and international studies. Retrieved March 22, 2021 from https://www.csis.org/analysis/cybersecurity-workforce-gap

[27] Jessica Dawson and Robert Thomson. 2018. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in psychology* 9 (2018), 1–12. https://doi.org/10.3389/fpsyg.2018.00744

[28] Tommaso De Zan and Fabio Di Franco. 2019. *Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database.* ENISA, Heraklion, Greek. Retrieved March 23, 2021 from https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[29] Department of Business Innovation and Skills. 2014. *Cyber Security Skills: Business Perspectives and Government's Next Steps.* HMSO, London, UK. Retrieved March 9, 2021 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

[30] Efrim Boritz and Carla Carnaghan. 2017. Competence-based Education and Assessment in the Accounting Profession in Canada and the USA. In *Competence-based vocational and professional education*, Martin Mulder (Ed.). Springer International, Cham, Switzerland, 273–296.

[31] Enhancement of cyber educational system of Montenegro. 2013. Usable cyber security competency framework. Retrieved May 7, 2020 from http://ecesm.net/sites/default/files/Dev%203.2%20-%20Usable%20cyber%20security%20competency%20framework%20%5Bdraft%202016.03.31%5D.pdf

[32] Michelle R. Ennis. 2008. Competency models: A Review of the Literature and The Role of the Employment and Training Administration (ETA). Retrieved April 29, 2021 from https://wdr.doleta.gov/research/FullText_Documents/Competency%20Models%20-%20A%20Review%20of%20Literature%20and%20the%20Role%20of%20the%20Employment%20and%20Training%20Administration.pdf

[33] John Erpenbeck, Lutz von Rosenstiel, Sven Grote, and Werner Sauter (Eds.). 2017. *Handbuch Kompetenzmessung: Erkennen, verstehen und bewerten von Kompetenzen in der betrieblichen, pädagogischen und psychologischen Praxis* (3. ed.). Schäffer-Poeschel, Stuttgart, Germany.

[34] Ismael E. Espinosa-Curiel, Josefina Rodríguez-Jacobo, and Alberto J. Fernández-Zepeda. 2011. A competency framework for the stakeholders of a software process improvement initiative. In *Proceedings of the 2011 International Conference on Software and Systems Process (ICSSP'11)*, David Raffo, Dietmar Pfahl, and Li Zhang (Eds.). ACM, New York, NY, USA, 139–148. https://doi.org/10.1145/1987875.1987898

[35] European Committee for Standardization. 2020. e-Competence Framework (e-CF): A common European Framework for ICT Professionals in all sectors: Version 4.0. Retrieved June 27, 2020 from https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:67073,1218399&cs=1A148766F9EC80CBD3340728E3B8BB892

[36] European Union Agency for Cybersecurity. 2020. Emerging trends: ENISA Threat Landscape: From January 2019 to April 2020. Retrieved March 22, 2021 from https://www.enisa.europa.eu/publications/emerging-trends

[37] European Union Agency for Cybersecurity. 2020. Main incidents in the EU and worldwide: ENISA Threat Landscape: From January 2019 to April 2020. Retrieved April 20, 2021 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

[38] EY. 2018. Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. Retrieved October 8, 2020 from https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

[39] Michael Felderer, Matthias Büchler, Martin Johns, Achim D. Brucker, Ruth Breu, and Alexander Pretschner. 2016. Chapter one - Security Testing: a survey. *Advances in Computer* 101 (2016), 1–51. https://doi.org/10.1016/bs.adcom.2015.11.003

[40] Luis Fernandez-Sanz, Josefa Gómez-Pérez, and Ana Castillo-Martinez. 2018. Analysis of the European ICT Competence Frameworks. In *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals*, Manish Gupta, Ahuja Vandana, and Shubhangini Rathore (Eds.). Vol. 160. IGI Global, Hershey, PA, USA, 225–245. https://doi.org/10.4018/978-1-5225-5297-0.ch012

[41] Stephen Frezza, Charles Wallace, Mats Daniels, Arnold Pears, Åsa Cajander, Amanpreet Kapoor, Roger McDermott, Anne-Kathrin Peters, and Mihaela Sabin. 2018. Modelling competencies for computing education beyond 2020: A research Based approach to Defining Competencies in the Computing Disciplines. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE 2018 Companion*, Guido Rößling and Bruce Scharlau (Eds.). ACM, New York, NY, USA, 148–174. https://doi.org/10.1145/3293881.3295782

[42] Steven Furnell. 2021. The cybersecurity workforce and skills. *Computers & Security* 100 (2021), 102080. https://doi.org/10.1016/j.cose.2020.102080

[43] Vahid Garousi, Michael Felderer, and Mika V. Mäntylä. 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology* 106 (2019), 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

[44] Vahid Garousi and Mika V. Mäntylä. 2016. When and what to automate in software testing? A multi-vocal literature review. *Information and Software Technology* 76 (2016), 92–117. https://doi.org/10.1016/j.infsof.2016.04.015

[45] German Qualifcations Framework Working Group. 2011. The German Qualifications Framework for Lifelong Learning. Retrieved November 16, 2021 from https://www.dqr.de/media/content/Der_Deutsche_Qualifikationsrahmen_fue_lebenslanges_Lernen.pdf

[46] Adam Gordon. 2015. *Official (ISC)2 guide to the CISSP CBK.* CRC Press, Boca Raton, FL, USA.

[47] Francois Goupil, Pavel Laskov, Irdin Pekaric, Michael Felderer, Alexander Dürr, and Frederic Thiesse. 2022. Towards Understanding the Skill Gap in Cybersecurity. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 1 (ITiCSE 2022)* (Dublin, Ireland, July 08-13, 2022), Brett A. Becker, Keith Quille, Mikko-Jussi Laakso, Erik Barendsen, and Simon (Eds.). ACM, New York, NY, USA, 477–483. https://doi.org/10.1145/3502718.3524807

[48] Joseph Hallett, Robert Larson, and Awais Rashid. 2018. Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD, USA, 1–9.

[49] Johannes Hartig and Eckhard Klieme. 2006. Kompetenz und Kompetenzdiagnostik. In *Leistung und Leistungsdiagnostik*, Karl Schweizer (Ed.). Springer, Berlin, Germany, 127–143.

[50] Johannes Hartig and Eckhard Klieme. 2007. *Möglichkeiten und Voraussetzungen technologiebasierter Kompetenzdiagnostik: Eine Expertise im Auftrag des Bundesministeriums für Bildung und Forschung.* BMBF, Berlin, Germany.

[51] Nicole Herbert, Kristy de Salas, Ian Lewis, Julian Dermoudy, and Leonie Ellis. 2014. ICT Curriculum and Course Structure: the Great Balancing Act. In *Proceedings of the Sixteenth Australasian Computing Education Conference* (Auckland, New Zealand, January 20-23, 2014), Jacqueline Whalley (Ed.). Australian Computer Society, Darlinghurst, NSW, Australia, 21–30.

[52] Volker Heyse and John Erpenbeck. 2010. *Kompetenztraining: Informations- und Trainingsprogramme* (2. ed.). Schäffer-Poeschel, Stuttgart, Germany.

[53] HM Government. 2016. *National Cyber Security Strategy 2016-2021.* HM Government, London, UK. Retrieved September 22, 2020 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[54] (ISC)^2. 2018. Building A Resilient Cybersecurity Culture: A dedicated staff with a clear mission helps retain and engage a cybersecurity workforce. https://www.isc2.org/-/media/Files/Reports/Building-A-Resilient-Cybersecurity-Culture.ashx?la=en&hash=5BBBD1218138977BF7150E1593319F70B5670B6F

[55] (ISC)^2. 2018. Hiring and Retaining Top Cybersecurity Talent: What employers need to know about cybersecurity jobseekers in 2018. Retrieved March 25, 2021 from https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

[56] (ISC)^2. 2020. Cybersecurity Professionals Stand Up to a Pandemic: (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2020. Retrieved March 22, 2021 from https://www.isc2.org/Research/Workforce-Study

[57] ISO/IEC. 2005. *Information technology, security techniques, code of practice for information security management.* International standard, Vol. ISO/IEC 27002 (2005). ISO/IEC, Genf, Schweiz.

[58] IT Security Competency Model. [n.d.]. DOCPLAYER. Retrieved May 8, 2020 from https://docplayer.net/15738823-Information-technology-it-specialist-gs-2210-it-security-competency-model.html

[59] Johannes Hartig, Andreas Frey, and Nina Jude. 2012. Validität. In *Testtheorie und Fragebogenkonstruktion*, Helfried Moosbrugger and Augustin Kelava (Eds.). Springer, Berlin, Germany, 143–171.

[60] Joint Task Force on Cybersecurity Education. 2017. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Retrieved March 24, 2020 from https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf Version 1.0.

[61] Keith S. Jones, Akbar S. Namin, and Miriam E. Armstrong. 2018. The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Transactions on Computing Education* 18, 3 (2018), 12 pages. https://doi.org/10.1145/3152893

[62] Eckhard Klieme, Hermann Avenarius, Werner Blum, Peter Döbrich, Hans Gruber, Manfred Prenzel, Kristina Reiss, Kurt Riquarts, Jürgen Rost, Heinz-Elmar Tenorth, and Helmut J. Vollmer. 2003. *Zur Entwicklung nationaler Bildungsstandards: Eine Expertise.* BMBF, Berlin, Germany.

[63] Eckhard Klieme and Johannes Hartig. 2008. Kompetenzkonzepte in den Sozialwissenschaften und im erziehungswissenschaftlichen Diskurs. In *Kompetenzdiagnostik*, Manfred Prenzel, Ingrid Gogolin, and Heinz-Hermann Krüger (Eds.). VS Verlag für Sozialwissenschaften, Wiesbaden, Germany, 11–29. https://doi.org/10.1007/978-3-531-90865-6_2

[64] E. Klieme and D. Leutner. 2006. Kompetenzmodelle zur Erfassung individueller Lernergebnisse und zur Bilanzierung von Bildungsprozessen. Beschreibung eines neu eingerichteten Schwerpunktprogramms der DFG. *Zeitschrift für Pädagogik* 52, 6 (2006), 876–903.

[65] Kenneth J. Knapp, Christopher Maurer, and Miloslava Plachkinova. 2017. Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education* 28, 2 (2017), 101–114.

[66] Brian R. von Konsky, Ashley Jones, and Charlynn Miller. 2014. Visualising career progression for ICT professionals and the implications for ICT curriculum design in higher education. In *Proceedings of the Sixteenth Australasian Computing Education Conference* (Auckland, New Zealand, January 20-23, 2014), Jacqueline Whalley and Daryl D'Souza (Eds.). Australian Computer Society, Darlinghurst, NSW, Australia, 13–20.

[67] Matthias Kramer, Peter Hubwieser, and Torsten Brinda. 2016. A Competency Structure Model of Object-Oriented Programming. In *2016 International Conference on Learning and Teaching in Computing and Engineering (LaTICE)* (Mumbai, India, March 31-April 3, 2014). IEEE, Los Alamitos, CA, USA, 1–8. https://doi.org/10.1109/LaTiCE.2016.24

[68] Matthias Kramer, David Tobinski, and Torsten Brinda. 2016. Modelling Competency in the Field of OOP: From Investigating Computer Science Curricula to Developing Test Items. In *1st International Conference on Stakeholders and Information Technology in Education (SAITE)* (Guimarães, Portugal, July 5-8, 2016). Springer, Cham, Germany, 37–46. https://doi.org/10.1007/978-3-319-54687-2_4

[69] Stefan Krumm, Inga Mertin, and Christina Dries. 2012. *Kompetenzmodelle.* Hogrefe, Göttingen, Germany.

[70] Udo Kuckartz. 2018. *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (4. ed.). Beltz Juventa, Weinheim, Germany.

[71] Françoise D. Le Deist and Jonathan Winterton. 2005. What Is Competence? *Human Resource Development International* 8, 1 (2005), 27–46. https://doi.org/10.1080/1367886042000338227

[72] Carol Lefebvre, Eric Manheimer, and Julie Glanville. 2008. Searching for studies. In *Cochrane Handbook for Systematic Reviews of Interventions Version 5.1.0*, Julian Higgins and Sally Green (Eds.). Cochrane, Chap. 6. Retrieved February 11, 2021 from https://crtha.iums.ac.ir/files/crtha/files/cochrane.pdf

[73] Yair J. Levy and Timothy J. Ellis. 2006. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science Journal* 9 (2006), 181–212. https://doi.org/10.28945/479

[74] Qiang Liu, Wentao Zhao, Ruijin Wang, and Jiangyong Shi. 2021. A Competence-Based Three-Layer Cybersecurity Education Framework and Its Application. In *ACM Turing Award Celebration Conference - China (ACM TURC 2021)* (Hefei, China, July 30-August 1, 2021). ACM, New York, NY, USA, 54–60. https://doi.org/10.1145/3472634.3472649

[75] Richard S. Mansfield. 1996. Building competency models: Approaches for HR professionals. *Human Resource Management* 35, 1 (1996), 7–18. https://doi.org/10.1002/(SICI)1099-050X(199621)35:1<7::AID-HRM1>3.0.CO;2-2

[76] Daniel P. Manson, Steven S. Curl, and Javier Torner. 2009. A Framework for Improving Information Assurance Education. *Communications of the IIMA* 9, 1 (2009), 79–90.

[77] Solga Marc, Ryschka Jurij, and Mattenklott Axel. 2011. Personalentwicklung: Gegenstand, Prozessmodell, Erfolgsfaktoren. In *Praxishandbuch Personalentwicklung*, J. Ryschka, M. Solga, and A. Mattenklot (Eds.). Springer Gabler, Wiesbaden, Germany, 19–34.

[78] Leanne H. Markus, Helena D. Cooper-Thomas, and Keith N. Allpress. 2005. Confounded by Competencies? An Evaluation of the Evolution and Use of Competency Models. *New Zealand Journal of Psychology* 34, 2 (2005), 117–127.

[79] Anne F. Marrelli, Janis Tondora, and Michael A. Hoge. 2005. Strategies for developing competency models. *Administration and policy in mental health* 32, 5-6 (2005), 533–561. https://doi.org/10.1007/s10488-005-3264-0

[80] Philipp Mayring. 2015. *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12. ed.). Beltz Verlag, Weinheim, Germany.

[81] David C. McClealland. 1973. Testing for competence rather than for "intelligence". *American Psychologist* 28, 1 (1973), 1–14.

[82] Natalia Miloslavskaya and Alexander Tolstoy. 2016. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. In *4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (Vienna, Austria, August 22-24, 2016), Muhammad Younas, Irfan Awan, and Joyce El Haddad (Eds.). IEEE, Piscataway, NJ, USA, 83–90. https://doi.org/10.1109/W-FiCloud.2016.31

[83] Kevin D. Mitnick and William L. Simon. 2002. *The art of deception: Controlling the human element of security.* Wiley Publishing, Indianapolis, IN, USA.

[84] Raduan A. Nur, Nab Seung-Il, Kim Young-Heung, and Oh Chun-Sik. 2020. An Analysis of the Horizontal and Vertical Consistency of ICT Skill Standards in Selected Countries and Regions. *International Journal of Innovation, Creativity and Change.* 11, 11 (2020), 132–146.

[85] Alessandra Orsoni and Brian Colaco. 2013. A Competency Framework for Software Development Organizations. In *2013 UKSim 15th International Conference on Computer Modelling and Simulation* (Cambridge, UK, April 10-12, 2013), David Al-Dabass (Ed.). IEEE, Piscataway, NJ, USA, 507–511. https://doi.org/10.1109/UKSim.2013.101

[86] Geet Parekh, David DeLatte, Geoffrey L. Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T. Sharman. 2018. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education* 61, 1 (2018), 11–20. https://doi.org/10.1109/TE.2017.2715174

[87] Amaanullah Parker and Irwin Brown. 2019. Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In *Information Security: 17th International Conference* (Pretoria, South Africa, August 15-16, 2019), Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, and Jan Eloff (Eds.). Springer International Publishing, Cham, Germany, 176–192.

[88] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad R. Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE 2018 Companion* (Larnaca, Zypern,

July 2-4, 2018), Guido Rößling and Bruce Scharlau (Eds.). ACM, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[89] David N. Perkins, Eileen Jay, and Shari Tishman. 1993. Beyond Abilities: A Dispositional Theory of Thinking. *Merrill-Palmer Quarterly* 39, 1 (1993), 1–21.

[90] Eetu Pikkarainen. 2014. Competence as a Key Concept of Educational Theory: A Semiotic Point of View. *Journal of Philosophy of Education* 48, 4 (2014), 621–636. https://doi.org/10.1111/1467-9752.12080

[91] Henk Plessius and Pascal Ravesteyn. 2016. Mapping the European e-Competence Framework on the domain of Information Technology: a comparative study. In *BLED 2016 Proceedings* (Bled, Slovenia, June 19-22, 2016). 1–13.

[92] Leigh E. Potter and Gregory Vickers. 2015. What Skills do you Need to Work in Cyber Security?. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15* (Newport Beach, CA, USA, June 4-6, 2015), Diana Burley, Indira R. Guzman, Daniel P. Manson, and Leigh E. Potter (Eds.). ACM Press, New York, NY, USA, 67–72. https://doi.org/10.1145/2751957.2751967

[93] Ibrahim Rahhal, Ibtissam Makdoun, Ghita Mezzour, Imane Khaouja, Kathleen Carley, and Ismail Kassou. 2019. Analyzing Cybersecurity Job Market Needs in Morocco by Mining Job Ads. In *EDUCON: 2019 IEEE Global Engineering Education Conference* (Dubai, United Arab Emirates, April 9-11, 2019), Alaa K. Ashmawy and Sebastian Schreiter (Eds.). IEEE, Piscataway, NJ, USA, 535–543. https://doi.org/10.1109/EDUCON.2019.8725033

[94] Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, and Andrew Martin (Eds.). 2019. *CyBOK: The Cyber Security Body of Knowledge: Version 1.0.* Retrieved March 23, 2020 from https://www.cybok.org/media/downloads/CyBOK_version_1.0_YMKBy7a.pdf

[95] Samuel T. Redwine (Ed.). 2006. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software: Version 1.1.* U.S. Department of Homeland Security.

[96] Gerhard Röhner, Torsten Brinda, Volker Denke, Lutz Hellmig, Theo Heußer, Arno Pasternak, Andreas Schwill, and Monika Seiffert. 2016. Bildungsstandards Informatik für die Sekundarstufe II: Beilage zu LOG IN, 36. Jg. (2016), Heft Nr. 183/184. Retrieved April 1, 2020 from https://informatikstandards.de/standards/bildungsstandards-informatik-fuer-die-sekundarstufe-ii

[97] Werner Sauter and Franz-Peter Staudt. 2016. *Strategisches Kompetenzmanagement 2.0: Potenziale nutzen - Performance steigern.* Springer Gabler, Wiesbaden, Germany.

[98] David Scheffer, Harald Schmitz, and Werner Sarges. 2007. Das Kompetenzmodell auf Basis des Wertequadrats: Motor von Veränderungen in Unternehmen. In *Entwicklungsquadrat – Theoretische Fundierung und praktische Anwendungen*, Fritz Westermann (Ed.). Hogrefe, Göttingen, Germany, 223–244.

[99] Jeffery S. Schippmann, Ronald A. Ash, Mariangela Battista, Linda Carr, Lorraine D. Eyde, Beryl Hesketh, Jerry Kehoe, Kenneth Pearlman, Erich P. Prien, and Juan I. Sanchez. 2000. The practice of competency modeling. *Personnel Psychology* 53, 3 (2000), 703–740.

[100] Joachim Schöpfel. 2010. Towards a Prague Definition of Grey Literature. In *Twelfth International Conference on Grey Literature: Transparency in Grey Literature* (Prague, Czech Republic, December 6-7, 2010). 11–26.

[101] Margrit Schreier. 2012. *Qualitative Content Analysis in Practice.* SAGE, London, UK.

[102] Yvonne Sedelmaier and Dieter Landes. 2014. Software engineering body of skills (SWEBOS). In *2014 IEEE Global Engineering Education Conference (EDUCON)* (Istanbul, Turkey, April 3-5, 2014). IEEE, 395–401. https://doi.org/10.1109/EDUCON.2014.6826125

[103] Rose Shumba. 2015. Towards a Digital Forensics Competency-Based Program: Making Assessment Count. In *Annual ADFSL Conference on Digital Forensics, Security and Law.* (Daytona Beach, FL, USA, May 19-21, 2015) *(5)*, Rose Shumba (Ed.). 193–204.

[104] Klas E. Soderquist, Alexandros Papalexandris, George Ioannou, and Gregory Prastacos. 2010. From task–based to competency–based: A typology and process supporting a critical HRM transition. *Personnel Review* 39, 3 (2010), 325–346. https://doi.org/10.1108/00483481011030520

[105] Jonathan Sterne, Matthias Egger, and David Moher. 2008. Addressing reporting biases. In *Cochrane Handbook for Systematic Reviews of Interventions Version 5.1.0*, Julian Higgins and Sally Green (Eds.). Cochrane, Chap. 10.

[106] Gregory W. Stevens. 2013. A Critical Review of the Science and Practice of Competency Modeling. *Human Resource Development Review* 12, 1 (2013), 86–107. https://doi.org/10.1177/1534484312456690

[107] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. 2020. What Are Cybersecurity Education Papers About?. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA, March 11-14, 2020), Jian Zhang, Mark Sherriff, Sarah Heckman, Pamela Cutter, and Alvaro Monge (Eds.). ACM, New York, NY, USA, 2–8. https://doi.org/10.1145/3328778.3366816

[108] U. S. Department of Labor. 2017. Renewable Energy Competency Model. Retrieved September 02, 2022 from https://www.careeronestop.org/CompetencyModel/competency-models/renewable-energy.aspx

[109] Marcel van der Klink and Jo Boon. 2003. Competencies: the triumph of a fuzzy concept. *International Journal of Human Resources Development and Management* 3, 2 (2003), 125–137. https://doi.org/10.1504/IJHRDM.2003.002415

[110] Marcel van der Klink, Jo Boon, and Kathleen Schlusmans. 2007. Competences and vocational higher education: Now and in future. *European Journal of Vocational Training* 40, 1 (2007), 67–82.

[111] Femi Vance. 2010. A Comparative Analysis of Competency Frameworks for Youth Workers in the Out-of-School Time Field. *Child Youth Care Forum* 39, 6 (2010), 421–441. https://doi.org/10.1007/s10566-010-9116-4

[112] Rossouw von Solms and Johan van Niekerk. 2013. From information security to cyber security. *Computers & Security* 38 (2013), 97–102. https://doi.org/10.1016/j.cose.2013.04.004

[113] Joke Voogt and Natalie P. Roblin. 2012. A comparative analysis of international frameworks for 21^{st} century competences: Implications for national curriculum policies. *Journal of Curriculum Studies* 44, 3 (2012), 299–321. https://doi.org/10.1080/00220272.2012.668938

[114] Franz E. Weinert. 1999. *Defintion and Selection of Competencies: Concepts of Competence.* OECD, Paris, Frankreich.

[115] Franz E. Weinert. 2001. Concept of Competence: A Conceptual Clarification. In *Defining and selecting key competencies*, Dominique S. Rychen and Laura H. Salganik (Eds.). Hogrefe & Huber, Seattle, WA, USA, 45–65.

[116] Franz E. Weinert. 2001. Vergleichende Leistungsmessung in Schulen - eine umstrittene Selbstverständlichkeit. In *Leistungsmessung in Schulen*, Franz E. Weinert (Ed.). Beltz, Weinheim, Germany, 17–32.

[117] Corina White, Clifford A. Whitcomb, Rabia Khan, Dana Grambow, Jessica Delgado, and José G. Vélez. 2016. Development of a Systems Engineering Career Competency Model for the U.S. Department of Defense. *INCOSE International Symposium* 26, 1 (2016), 1864–1874. https://doi.org/10.1002/j.2334-5837.2016.00266.x

[118] Michael E. Whitman. 2018. Industry Priorities for Cybersecurity Competencies. *Journal of The Colloquium for Information System Security Education* 6, 1 (2018), 1–21.

[119] Michael E. Whitman and Herbert J. Mattord. 2009. *Principles of information security* (3. ed.). Course Technology, Boston, MA, USA.

[120] Jonathan Winterton, Françoise Delamare-Le Deist, and Emma Stringfellow. 2006. *Typology of knowledge, skills and competences: Clarification of the concept and prototype.* Office for Official Publications of the European Communities, Luxembourg.

[121] World Economic Forum. 2018. *The future of jobs report 2018.* World Economic Forum, Geneva, Switzerland. Retrieved March 5, 2021 from https://www.weforum.org/reports/the-future-of-jobs-report-2018

[122] Yu Xiao and Maria Watson. 2019. Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research* 39, 1 (2019), 93–112. https://doi.org/10.1177/0739456X17723971

[123] Muhammad M. Yamin and Basel Katt. 2019. Cyber Security Skill Set Analysis for Common Curricula Development. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)* (Canterbury, UK, August 26-29, 2019). ACM, New York, NY, USA, 1–8. https://doi.org/10.1145/3339252.3340527

[124] Samuel C. Yang. 2021. A meta-model of cybersecurity curriculums: Assessing cybersecurity curricular frameworks for business schools. *Journal of Education for Business* 96, 2 (2021), 99–110. https://doi.org/10.1080/08832323.2020.1757594

SELECTED SOURCES

[125] Mark Ardis, Dick Fairley, Thomas Hilburn, Ken Nidiffer, Massood Towhidnejad, Mary J. Willshire, and Kate Guillemette. 2014. *Software Engineering Competency Model: SWECOM: A Project of the IEEE Computer Society.* IEEE. Retrieved April 28, 2021 from http://www.dahlan.id/files/ebooks/SWECOM.pdf

[126] AXELOS. 2016. Skills Framework. Retrieved May 5, 2020 from https://www.axelos.com/Corporate/media/Files/CPD/axelos-skills-framework-light.pdf

[127] Chief Human Capital Officers Council. 2011. Competency Model for Cybersecurity. Retrieved April 22, 2020 from https://www.chcoc.gov/content/competency-model-cybersecurity

[128] CIO Council. 2012. 2012 Clinger-Cohen Core Competencies & Learning Objectives. Retrieved April 19, 2020 from https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/2012-Learning-Objectives-Final.pdf

[129] Club Informatique des Grandes Entreprises Francaises. 2011. Information Systems roles in large companies: HR nomenclature - 2011. Retrieved March 24, 2020 from https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_IS_roles_in_large_companies_HR_nomenclature_CIGREF_EN.pdf

[130] Department of Labor and Industry. 2014. Competency Model for Information Technology Occupation: Security Analyst. Retrieved April 2, 2020 from https://www.dli.mn.gov/sites/default/files/pdf/IT_security_analyst_sum.pdf

[131] European Committee for Standardization. 2014. Case Studies for the application of the e-CF 3.0: A common European framework for ICT Professionals in all industry sectors. Retrieved March 25, 2020 from http://www.ecompetences.eu/wp-content/uploads/2014/02/Case_studies_e-CF_3.0_CEN_CWA_16234-4_2014.pdf

[132] European Committee for Standardization. 2014. European e-Competence Framework 3.0: A common European framework for ICT Professionals in all industry sectors. Retrieved March 25, 2020 from http://relaunch.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf

[133] European Committee for Standardization. 2014. User guide for the application of the European e-Competence Framework 3.0: A common European framework for ICT Professionals in all industry sectors. Retrieved March 25, 2020 from http://ecompetences.eu/wp-content/uploads/2014/02/User-guide-for-the-application-of-the-e-CF-3.0_CEN_CWA_16234-2_2014.pdf

[134] Elizabeth K. Hawthorne, Robert D. Campbell, Cara Tang, Cindy S. Tucker, and Jim Nichols. 2014. *Information Technology Competency Model of Core Learning Outcomes and Assessment for Associate-Degree Curriculum: Technical Report.* ACM, New York, NY, USA. Retrieved May 14, 2020 from http://ccecc.acm.org/files/publications/ACMITCompetencyModel14October201420150114T180322.pdf

[135] Thomas Hilburn, Mark Ardis, Glenn Johnson, Andrew J. Kornecki, and Nancy R. Mead. 2013. Software Assurance Competency Model. Retrieved May 5, 2020 from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_47965.pdf

[136] Hong Kong Monetary Authority. 2019. Update on Enhanced Competency Framework on Cybersecurity. Retrieved May 10, 2020 from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190110e1.pdf

[137] Information-Technology Promotion Agency. 2016. IT Human Resources Development: i Competency Dictionary (iCD). Retrieved May 2, 2020 from https://www.ipa.go.jp/english/humandev/icd.html

[138] Institute of Information Security Professionals. 2018. IISP Skills Framework. Retrieved March 31, 2020 from https://www.ciisec.org/

[139] Evangelos Moustroufas, Ioannis Stamelos, and Lefteris Angelis. 2015. Competency profiling for software engineers: Literature Review and a new Model. In *Proceedings of the 19th Panhellenic Conference on Informatics* (Athen, Greek, October 1-3, 2015), Nikitas N. Karanikolas, Demosthenes Akoumianakis, Mara Nikolaidou, Dimitris Vergados, and Michalis Xenos (Eds.). ACM, New York, NY, USA, 235–240. https://doi.org/10.1145/2801948.2801960

[140] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved April 6, 2020 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[141] Personal Data Protection Commission. 2020. DPO Competency Framework and Training Roadmap. Retrieved April 30, 2020 from https://www.pdpc.gov.sg/dp-competency#competencies

[142] Loina Prifti, Marlene Knigge, Harald Kienegger, and Helmut Krcmar. 2017. A Competency Model for "Industrie 4.0" Employees. In *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, Jan M. Leimeister and Walter Brenner (Eds.). St. Gallen, Schweiz, 46–60.

[143] Mihaela Sabin, Hala Alrumaih, John Impagliazzo, Barry Lunt, Ming Zhang, Brenda Byers, William Newhouse, Bill Paterson, Svetlana Peltsverger, Cara Tang, Gerrit van der Veer, and Barbara Viola. 2017. *Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology.* ACM, New York, NY, USA. https://doi.org/10.1145/3173161

[144] Kim Se-Yun, Seong T. Park, and Mi H. Ko. 2015. Analysis of the Competencies of Information Security Consultants: Comparison between Required Level and Retention Level. *Indian Journal of Science and Technology* 8, 21 (2015), 1–8. https://doi.org/10.17485/ijst/2015/v8i21/79119

[145] SFIA Foundation. 2018. Skills Framework for the Information Age: SFIA 7: The complete reference. Retrieved April 3, 2020 from https://www.sfia-online.org/en/framework/sfia-7/documentation/sfia-7-the-complete-reference

[146] SkillsFuture. 2019. *Skills Framework for Infocomm Technology.* Retrieved May 13, 2020 from https://www.skillsfuture.sg/skills-framework/ict#

[147] Heikki Topi, Helena Karsten, Sue Brown, João A. Carvalho, Brian Donnellan, Jun Shen, Bernard C. Y. Tan, and Mark F. Thouin. 2017. MSIS 2016: Global Competency Model for Graduate Degree Programs in Information Systems. *Communications of the Association for Information Systems* 40 (2017), MSIS–i – MSIS–107.

[148] Janet Tweedie and Julie West. 2010. Cyber Security Capability Framework & Mapping of ISM Roles: Final Report. Retrieved April 23, 2020 from https://www.yumpu.com/en/document/read/43006585/cyber-security-capability-framework-mapping-of-ism-roles-agimo

[149] U. S. Department of Energy. 2013. Essential Body of Knowledge (EBK): A Competency and Functional Framework for Cyber Security Workforce Development. Retrieved May 2, 2020 from https://www.energy.gov/sites/prod/files/2014/04/f15/DOEEBK_1-2013Revision_NICEv01_SCRM_clean_v04.pdf

[150] U. S. Department of Homeland Security. 2008. Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. Retrieved April 10, 2020 from https://www.hsdl.org/?view&did=234220

[151] U. S. Department of Homeland Security. 2012. Software Assurance Professional Competency Model. Retrieved April 1, 2020 from https://docplayer.net/22397688-Software-assurance-professional-competency-model.html

[152] U.S. Department of Labor. 2012. Information Technology Competency Model. Retrieved March 24, 2020 from https://www.careeronestop.org/competencymodel/competency-models/pyramid-download.aspx?industry=information-technology

[153] U.S. Department of Labor. 2019. Cybersecurity Competency Model. Retrieved April 24, 2020 from https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity

CURRICULA

[154] FH Campus Wien. 2020. *Masterstudium: IT-Security.* FH Campus Wien. Retrieved September 18, 2020 from https://www.fh-campuswien.ac.at/studium-weiterbildung/studien-und-lehrgangsangebot/detail/it-security-master.html

[155] FH Joanneum. 2020. *IT & Mobile Security: Master.* FH Joanneum. Retrieved September 18, 2020 from https://www.fh-joanneum.at/it-und-mobile-security/master/

[156] FH Oberösterreich. 2020. *Information Security Management: Masterstudiengang.* FH Oberösterreich. Retrieved September 18, 2020 from https://www.fh-ooe.at/campus-hagenberg/studiengaenge/master/information-security-management/

[157] FH Oberösterreich. 2020. *Sichere Informationssysteme: Bachelorstudium.* FH Oberösterreich. Retrieved October 18, 2020 from https://www.fh-ooe.at/campus-hagenberg/studiengaenge/bachelor/sichere-informationssysteme/

[158] FH Oberösterreich. 2020. *Sichere Informationssysteme: Masterstudium*. FH Oberösterreich. Retrieved September 18, 2020 from https://www.fh-ooe.at/campus-hagenberg/studiengaenge/master/sichere-informationssysteme/

[159] FH St. Pölten. 2020. *Cyber Security and Resilience: Master Studiengang*. FH St. Pölten. Retrieved September 18, 2020 from https://www.fhstp.ac.at/de/studium-weiterbildung/informatik-security/cyber-security-and-resilience

[160] FH St. Pölten. 2020. *Information Security: Master Studiengang*. FH St. Pölten. Retrieved September 18, 2020 from https://www.fhstp.ac.at/de/studium-weiterbildung/informatik-security/information-security

[161] FH St. Pölten. 2020. *IT-Security: Bachelor Studiengang*. FH St. Pölten. Retrieved September 18, 2020 from https://www.fhstp.ac.at/de/studium-weiterbildung/informatik-security/it-security?gclid=EAIaIQobChMIoIzc5be-7AIVh7LVCh3d2woPEAAYAyAAEgJyIvD_BwE

[162] FH Technikum Wien. 2020. *Masterstudiengang: IT-Security*. FH Technikum Wien. Retrieved October 18, 2020 from https://www.technikum-wien.at/studium/master/it-security/

[163] Universität Klagenfurt. 2020. *Master: Artificial Intelligence and Cyber Security*. Universität Klagenfurt. Retrieved September 18, 2020 from https://www.aau.at/studien/master-artificial-intelligence-and-cybersecurity/