Information security education based on job profiles and the e-CF

Marcel Spruit, https://orcid.org/0000-0003-3171-4906
The Hague University of Applied Sciences, The Hague, The Netherlands

Abstract

Purpose: The information security field requires standardised education. This could be based on generic job profiles and a standard competence framework. The question is whether this is possible and feasible. To find out, the author did a case study: developing an information security master curriculum based on a generic PVIB job profile and the underlying competence framework e-CF.
Design/methodology/approach: The research is a case study, using Design Science. Starting point is the specification of the learning goals for a cybersecurity master curriculum, using a generic PvIB job profile and the underlying competence framework e-CF. The curriculum has subsequently been developed, using backward design. Thereafter, the curriculum has been submitted for accreditation to test the successfulness of the approach.
Findings: A generic job profile and a competence framework such as the e-CF support the development of standardised education. The generic PVIB job profile used works well. The e-CF can be useful, but requires modifications and the introduction of sub-competences. However, the main complaint concerning the e-CF is the use of examples instead of mandatory content.
Originality/value: Competence frameworks are available to formulate job descriptions, and are also suited for developing standardised education. Little research has been done on this. This case study shows that a competence framework is a useful tool for developing standardised education, although the e-CF may not be the most appropriate.

This article has been published in the journal *Higher Education, Skills and Work-based Learning*. Accepted for publication on 26 July 2021. Reference: Spruit, M. (2021), "Information security education based on job profiles and the e-CF", *Higher Education, Skills and Work-based Learning*. doi: 10.1108/HESWBL-09-2020-0208.

Introduction

In today's information society, many organisations are highly dependent on their digital information systems and the information they contain. Organisations need to protect their growing volumes of digital information against an increasingly complex set of threats (Anderson, 2001; Smith, 2017). This requires well-educated and experienced information security, or cybersecurity, professionals.

However, organisations are finding it increasingly difficult to find well-educated and experienced information security professionals who are able to define, realise and maintain information security measures and to increase information security awareness (De Zan, 2019; Morgan, 2019; Vogel, 2016). Moreover, the shortage of suitable information security professionals has negative impact on the innovation and professionalisation of the information security field, and the realisation of information security education. This situation does not only apply to the Netherlands, but to many Western countries (Morgan, 2019). The main cause is the rapidly growing number of information security positions in a world that becomes more and more digitalised. Although there are several options for information security education, there are relatively few opportunities to get a higher vocational or applied university degree. In the Netherlands in 2019, there were only 12 bachelor studies on information/cybersecurity and 8 master studies (Van Noord and Barthel, 2019).

In addition, there is little consensus about the competences with respect to information security that should be taught to connect well to the professional practice (Bishop *et al*., 2017; Butler *et al*., 2018; De Zan, 2019; Parker and Brown, 2019; Vogel, 2016). This has resulted in a large number of hard to compare and immature qualifications (Spruit and Van Noord, 2011). In this chaotic situation, employers have been overtaken by commercial education providers who have an interest in fragmentation of information security education. As a result, information security professionals cannot clearly demonstrate their knowledge and skills based on their certificates. And employers cannot check whether a candidate for a security position is well-educated and experienced in information security.

Standardisation of information security education could be part of the solution. Such standardisation requires that employers and the information security field jointly specify the required competences of information security professionals by means of one or more broadly supported generic job profiles. Basing the profiles on a standard competence framework could make standardisation of education easier.

In a prior Dutch study, the Dutch Association of Information Security Professionals (PvIB) has defined such generic job profiles based on a competence framework, namely the European e-Competence Framework (e-CF) (Spruit and Van Noord, 2017).

The question is whether it is possible and feasible to develop standardised information security education based on the generic job profiles defined by the PvIB and the underlying standard competence framework e-CF.

Methodology

The research is a case study. The reason for this choice is that we have found little scientific literature on the usefulness of generic job profiles in combination with a standard competence framework, such as the e-CF, for the development of standardised education. The educational field could benefit from case studies to build knowledge about this topic.
The case study in this paper is from the information security domain. The Hague University turned out to need a new information or cybersecurity master of science curriculum. The university has been receiving signals for some time that such a curriculum would be very welcome. Thus, the case chosen is the development of a standardised master of science curriculum for information security, to show that building standardised education based on a generic job profile and the underlying competence framework is possible and feasible.

The research follows a Design Science approach (Hevner *et al.*, 2004; Johannesson and Perjons, 2014). Following the Design Science approach the next steps have been taken:

1. Defining the learning goals of the curriculum to be developed. For this, a generic PvIB job profile was used that was broadly supported by both information security professionals (supply side) and employers (demand side). By making use of the standard competence framework e-CF, the competences specified in the profile can be further elaborated into fairly detailed knowledge and skills elements.
2. Developing the curriculum. The intended teachers of the study develop the curriculum on the basis of the specified learning goals and additional mandatory preconditions such as the Bologna Framework (Bologna Working Group, 2005). The teachers use their experience with developing education as well as their knowledge of mandatory preconditions and the characteristics of the hosting university. The standardisation of the study should come from the standardised knowledge and skills elements and not from the way in which the teachers develop the knowledge and skills elements into their lessons.
3. Testing the curriculum. For this, we preferred the independent judgment by an experienced audit panel of an accreditation organisation over other methods such as a survey. Therefore, the new curriculum has been submitted for accreditation by the official accreditation organisation for Dutch higher education (NVAO). The NVAO uses a standard approach for assessing a new curriculum in higher education. Smooth and successful accreditation is a measure of how well the program has been developed.
4. Evaluating the broader applicability. After the curriculum has been successfully accredited, an evaluation can be done with respect to the extent the generic PvIB job profile and the standard competence framework e-CF are suitable for developing standardised education. Furthermore, an indication can be given to what extent the

approach may be suitable for other information security education and to what extent the approach may be suitable for other countries.

Literature review

Competences

In order to build (standardised) education, one has to specify the competences that should be taught. In literature there is confusion about the precise definition of a competence (Delamare and Winterton, 2005; Ennis, 2008; Mulder *et al*., 2006; Salman *et al*., 2020; Sultana, 2009; Winterton *et al*., 2006). In this paper we use the following definition: a competence is a demonstrated ability to apply knowledge and skills to successfully perform given tasks and functions in a given role or position (CEN, 2014; Dedović and Mušić, 2017; Delamare and Winterton, 2005). A competence can then be described by a set of knowledge and skills elements. Other elements that can be trained, e.g. insight and attitude, are considered to be part of these.

Competence-based education

Vocational and applied university education is often built according to the concept of competency-based (or outcome-based) education (Curry and Docherty, 2017; Morcke *et al*., 2013). Although this concept has not been defined unambiguously, it usually refers to education with two specific elements: (1) it is based on specification of the outcome of the curriculum in terms of competences (Morcke *et al*., 2013), also referred to as backward design (Davidovitch, 2013; Richards, 2013); (2) the curriculum offers a flexible and individualised approach, in which each student can acquire the predefined competences in the order, method and pace that suit the student best (Curry and Docherty, 2017; Dedović and Mušić, 2017; Morcke *et al*., 2013). Using this interpretation, traditional education follows a more or less fixed timetable that is not tailored to the individual student and can, but does not have to, be based on backward design.

There is a considerable amount of literature about competency-based education and its benefits (Burke, 1989; Frank *et al*., 2010; Leggett, 2015; Morcke *et al*., 2013; Sabin *et al*., 2018). The main advantage of competency-based education is that it is flexible and tailored to the individual student, making it efficient and attractive for students. The entry knowledge level and learning pace of students may vary. Although not reserved for competency-based education, learning to learn and learning to manage one's own career can be part of the education (Draaisma *et al*., 2018; Hughes *et al*., 2017; Kuijpers and Scheerens, 2006). There are also critical publications about competency-based education (Biemans *et al*., 2004; Koenen *et al*., 2015; Morcke *et al*., 2013; Norman *et al*., 2014; Soare, 2015). These do not

deny the benefits, but indicate that there are also drawbacks, such as the difficulty to specify and test the required competences, resource implications and curriculum planning. Some drawbacks of competency-based education can be seen as benefits of traditional education. This is in line with our own experience with traditional vocational and applied university curricula: (1) it is relatively easy to organise; (2) it requires relatively little teacher time; (3) it offers more opportunities for knowledge transfer between students; (4) students have less study delay because individual students want to keep pace with the group. The latter two arguments especially apply to part-time education with small groups of students with similar entry knowledge level, similar learning potential and some (job) experience.

Standardised education

The Dutch Association of Information Security Professionals (PvIB) has carried out an extensive consultation about support for standardised education in the information security field. The consultation used workshops and interviews with a large group of information security professionals, employers and representatives from several educational institutes. The consultation showed substantial support for standardised information security education on different educational levels (secondary vocational, higher vocational and university level) (Spruit and Van Noord, 2014). The individuals and organisations consulted agreed that standardised education should be based on new generic job profiles, provided by the PvIB, which in turn are based on a standard competence framework. Since the study has been performed in the Netherlands and aims to be applicable to other European countries, there was a strong preference for the European e-Competence Framework (e-CF) version 3.0 (CEN, 2014). In addition, the e-CF is seen as a promising competence framework by various Dutch government institutions. The knowledge and skills elements in the e-CF can be used on different educational levels.
Some authors are reluctant to introduce standardisation (Martinez and Zorita, 2007), but standardisation of vocational and applied university education can improve the alignment of graduates' knowledge and skills with professional practice, the recognisability of the education outcome and the flow of graduates to further education (Elken, 2017; Spruit and Van Noord, 2011; Tarman, 2016).

Generic PVIB job profiles

A generic job profile is a formal description of the minimum requirements for a typical job. A typical job is well-recognised and standardised job. Examples of typical jobs in the information security field are Information Security Officer and ICT Security Manager. A generic job profile describes the mission, tasks and responsibilities of a practitioner of the typical job and specifies the minimum competences (knowledge and skills) the practitioner must have (CEN, 2014). This includes both job-specific competences and general

competences (Heusdens *et al.*, 2018). Achieving the minimum competences in the relevant profile can be regarded as a qualification for the related typical job (Spruit and Van Noord, 2017). After achieving the qualification for a typical job a practitioner can further specialise by gaining experience in the job and by additional education. Given the multitude of possible specialisations on top of a typical job, it is not useful to formulate generic job profiles for specialisations. Moreover, many specialisations change relatively fast and probably do not need standardisation at all (Martinez and Zorita, 2007).

Generic job profiles for the information security field are based on typical medium-sized information processing organisations in which information security plays a prominent role, such as ministries, agencies, medium-sized banks and industrial organisations (Spruit and Van Noord, 2017). Organisations that are either less or more demanding in terms of information security impose less, respectively more, strict demands on their information security positions.

A generic job profile is related to a typical job and is not meant to be used directly as a job description for a specific organisation. It can however be included in a job description. But it is also possible to compile a particular job description from more job profiles, or from just a part of a job profile. Subsequently, the organisation will usually want to give its own twist to the way in which the job description has been specified in order to match its specific needs. The importance of generic job profiles is not that job descriptions can be formulated more easily, but that they can be used to standardise education and to align education to the needs of the working field.

Given the broad support in the information security field for standardised education based on one or more generic job profiles, the PvIB demarcated the information security field and defined six typical jobs, each getting its own generic job profile (Spruit and Van Noord, 2017). The generic job profiles were based on the job profile template of the European standardisation institute CEN (CEN, 2018). The PvIB linked the profiles to the European e-Competence Framework (e-CF) in order to formulate and elaborate competences in a standardised way.

To gain broad support for the profiles, the PvIB followed a stepwise approach: (1) a working group defined provisional typical jobs, their tasks and the required competences; (2) workshops were held with a large number of information security professionals, employers, lecturers and standardisation experts to determine the selection of typical jobs, their tasks and the required competences; (3) the PvIB drew up generic job profiles accordingly; (4) an extensive review process for fine-tuning.

The most important elements of the profiles with respect to the development of education are a list of required competences and required experience. The list of required competences consists of a set of rather coarse-grained competences. The elaboration of the competences into knowledge and skills elements uses the competence framework e-CF. The other element,

the required expertise, is rather straightforward and is filled in with prior education (type of education and field of education) and work experience (job function and years). The relevance of including experience in the profiles is to fill the gaps between the coarse-grained competences. These gaps arise because not all small, though required, competences are included in the competence list.
Education that matches a generic PVIB job profile, and the underlying knowledge and skills elements, is standardised. It also matches the needs of the professional practice.

The e-CF

The e-CF describes and elaborates competences. The competences mentioned in the generic job profile are selected from the e-CF (ICT specific competences) or defined by the PvIB Working Group on Skills (general competences). Those competences are formulated fairly coarse-grained and need to be further elaborated. The ICT specific competences (e-competences) have been elaborated in the e-CF, version 3.0 (CEN, 2014). The general competences have been elaborated similarly by the PvIB working group.

Results

Evaluation of the e-CF

Together with the PvIB Working Group on Skills we evaluated completeness and consistency of the knowledge and skills elements of the e-CF. We found that the e-CF content is far from complete and consistent. In fact, the content needs significant modification. This seems strange to an official standard (as of 2016), but it seems to be a deliberate choice of the European standardisation institute CEN which is responsible for the development of the e-CF. In their opinion the framework presents merely examples of knowledge and skills elements (CEN, 2014, p. 10). The consequence is that the e-CF is actually not a standard, but a guideline.
However, for the development of standardised education we need a formal reference that can be used as a solid basis. Therefore we modified the content of the e-CF competences to improve the completeness and consistency. We used the modified competences to elaborate the competences in the job profiles.
Non-standard frameworks such as ISACA (2018) and ad hoc job profiles such as ISF (2013) are built on non-standard competences and have their own education specified, or do not refer to education at all.
To get an impression of the extent to which competences have been elaborated, Table I shows the details of a (modified) e-CF competence, namely Information security management (CEN, 2014) and Table II shows the details of a general competence, namely Research. The

competence description shows a brief characterisation of the competence, the level of the competence and its knowledge and skills elements.

[Table I]

[Table II]

It would be nice if competences, which are defined quite coarse-grained in the e-CF, would have been divided into sub-competences. Table III shows an example for the competence Information security management.

[Table III]

The sub-competences could be further elaborated into knowledge and skills elements. In principle, this results in the same set of knowledge and skills elements as in the (modified) e-CF competence (Tables I and II). However, determining knowledge and skills elements is more transparent and more balanced if they are derived from sub-competences. If done well, the resulting knowledge and skills elements can be used directly as learning goals for standardised education. Obviously, the level of detail is a compromise between the precision required for standardisation and the autonomy of the users of the specification, for example teachers. The derivation from competence to sub-competences to elements/goals for the competence G4, Research, is shown in Table IV.

[Table IV]

Competences, and its knowledge and skills elements, have competence levels. The e-CF uses a range from 1 through 5 (CEN, 2014). As we use the (modified) e-CF for describing competences, the most obvious choice would be to use the e-CF competence levels. However, the e-CF levels are proficiency levels instead of competence levels. An e-CF proficiency level describes appreciation and responsibilities. It can be used to specify the characteristics of a specific job, but it does not specify the competence level of a person. Therefore, we have chosen another five-level scheme, based on the European Qualifications Framework for Lifelong Learning (EQF, 2008).
We conclude that the e-CF can certainly be used, although not unmodified, to elaborate competences from generic job profiles. In order to use the e-CF effectively, we had to improve the content and use a different competence level scheme.

Building standardised education

A generic PvIB job profile can be used to develop matching standardised education, using backward design. This is possible with both the traditional and the competency-based approach, and also with any option in between. Given the different benefits and drawbacks, the choice between competency-based education and traditional education, or somewhere in between, depends on the context.
Following the backward design approach, an information security curriculum can be designed on the basis of the competences specified in a generic information security job profile. The ICT-related competences (e-competences) have been elaborated in the (modified) e-CF. The general competences have been elaborated similarly by the PvIB Working Group on Skills. The knowledge and skills elements of the specified competences can be used directly as learning goals for the curriculum. The level of detail of the knowledge and skills elements is a thought out compromise between the precision required for standardisation and the autonomy of teachers. Teachers can build their own course material based on the specified learning goals, namely the specified knowledge and skills elements.
To demonstrate that this approach works, we designed a new technically oriented Master of Science on information security at the Hague University of Applied Sciences. It is a two-year part-time program (60 ECTS), named Master Cyber Security Engineering. To be admitted, students must have a bachelor's degree in computer science, information security or cybersecurity, as well as a job in this area.

[Table V]

Firstly, we selected the most relevant generic PVIB job profile, namely ICT Security Specialist 3 (Table V). We took the competences from the profile:

- A7: Technology trend monitoring, level 4.
- B4: Solution deployment, level 4.
- E3: Risk management, level 3.
- E8: Information security management, level 3.
- G3: Communication and persuasion, level 2.
- G4: Research, level 4.
- G7: Analytical skills, level 4.
- G8: Integrity, level 2.

Each of the competences is further elaborated into knowledge and skills elements, making use of the modified e-CF and the descriptions of the PvIB working group. The knowledge and skills elements are the learning goals. Additional learning goals came from mandatory preconditions such as the Bologna Framework (Bologna Working Group, 2005).

[Figure 1]

Secondly, we designed the basic structure of the curriculum. The structure was based on three semesters divided into three modules each, and completed with a master thesis in the fourth semester (Figure 1). A practice-oriented individual or group project is planned in each module. Those projects improve insight and skills and take about half the study load. In terms of content, the semesters are about the following:

1. Conceptualisation of cyber security. This semester is a concise tour through all sorts of relevant aspects, such as ICT security, human factor, management, legislation and ethics.
2. Cybersecurity building blocks. In this semester the students dive deep into ICT security. Technical experts in ICT security from outside the university are invited to give guest lectures.
3. Cybersecurity in sectors and trends. In this semester the knowledge from the previous semesters is applied to organisations in specific sectors. Technical and organisational experts from those sectors are involved. Furthermore, the latest trends are discussed.
4. Research. Each student has to do an individual scientific research project and write a master thesis.

Thirdly, we linked the learning goals to the modules. For this we defined the sub-competences which we would have expected in the e-CF and the PvIB list (Tables III and IV). Each sub-competence becomes a learning line in the curriculum. To limit the number of learning lines, related sub-competences can be combined into a single learning line. Each learning line contains courses and project tasks. For example, the first sub-competence of competence G.4 (Table IV) becomes a learning line “Scientific research”. This learning line contains various courses and project tasks, distributed over different modules. For example, Module 1 contains three courses within this learning line (with learning goals, see Table IV): “Introduction to research” (K1, K2), “Literature study” (K3) and “Interviewing” (K3). The module project emphasises the formulation of a research question, literature study and interviewing (S1, S2, S4). Together, the courses and project tasks per learning line cover the learning goals of the sub-competence.

Finally, the teachers built their own course material for the courses and module projects they are responsible for. For the second and third semester they work together with external experts.

Because the curriculum is part-time, all students have a job in the ICT or ICT security field. Consequently, there is considerable interaction between the students and there are opportunities for real-life training: (1) students take problems from their job to the study program, where they are used as cases; (2) students can apply new knowledge and train their

insight and skills directly in practice; (3) students do their individual and group projects in their own organisations.

Considering the way in which we have set up the curriculum, it has basically become a traditional curriculum with a fixed timetable. Traditional education benefits from small groups of part-time students which have similar entry knowledge level and learning potential as well as some job experience. These characteristics apply to our master. We achieve a similar entry knowledge level, learning potential and job experience with a selective intake. Furthermore, the first three modules of the programme are used to level the starting level of the students where necessary. This gives us some advantages of traditional education: (1) relatively easy to organise; (2) requires relatively little teacher time; (3) more possibilities for knowledge transfer between students; (4) less study delay because individual students want to keep pace with the group.

In addition, we introduced elements of competency-based education: (1) the outcome has been defined in terms of competences; (2) individualised homework and projects make up the major part of the study load; (3) the first three modules are even more individualised with the aim of bringing the knowledge level of the students to a similar level. Furthermore, learning to learn and learning to manage one's own career are addressed in the curriculum.

In general, a curriculum can vary from completely traditional to completely competency-based (Koenen *et al*., 2015). We chose somewhere in between, where we see an optimum between the benefits of both extremes.

Each new bachelor or master program in the Netherlands requires formal accreditation by the Accreditation Organisation of the Netherlands and Flanders (NVAO) according to the accreditation criteria established by the Dutch government (NVAO, 2018). This also applies to the new Master Cyber Security Engineering. The NVAO accreditation committee judged positively in the first and final round. One of the positive findings was the use of a generic job profile, combined with the e-CF, that can count on substantial support from professionals, employers and educators. Furthermore, the committee liked the structured and balanced approach to design and develop the master program. The program started in 2019.

Other educational institutions in the Netherlands, but also in other European countries, can use the generic information security job profiles to design new curricula or to adapt existing curricula. Different curricula based on the same generic job profile are equivalent and can be accredited more effectively. Moreover, the curricula match the needs of the professional practice, have recognisable education outcome, and moving on to follow-up education becomes easier.

We demonstrated that developing a new information security curriculum based on a broadly supported generic job profile is possible and feasible. Because the curriculum has been based on a generic job profile, the curriculum is standardised.

Educational institutions outside Europe may use the same approach to develop standardised education, leading to the same benefits, but they should check whether the job profiles defined in Europe and the underlying European competence framework are suitable.

Conclusion

The information security field requires well-educated and experienced information security professionals with known and broadly supported levels of information security competences. This becomes feasible by standardisation of education. Standardisation of education improves the alignment of graduates' knowledge and skills with professional practice, the recognisability of the education outcome and the flow of graduates to further education. The question is whether it is possible and feasible to develop standardised information security education based on broadly supported generic job profiles and a standardised competence framework.

The case study showed that it is possible and feasible to develop an information security curriculum based on a generic job profile. The development of the Master Cyber Security Engineering, based on the generic PVIB job profile "ICT Security Specialist 3" and the underlying competence framework e-CF, has been used as a case. This resulted in a standardised information security curriculum which was successfully accredited.

The generic PVIB job profile appeared to work as expected. The aggregation level of the competences was acceptable, but could be improved by using sub-competences to nuance coarse-grained competences.

The e-CF turned out to be less successful. We observed that it needs significant modification. This seems strange as the e-CF is an official European standard as of 2016. The explanation is that CEN, the responsible party for the e-CF, has deliberately chosen that the e-CF only provides examples. Consequently the e-CF is actually not a standard, but a guideline. Such a guideline is not suitable for the development of standardised information security education as standardisation requires well-defined reference levels. To solve the problem we needed to modify the e-CF to get an updated and well-defined content.

We suggest that CEN changes the current approach and thoroughly reviews the e-CF and consequently transforms it into a well-defined standard that can be used as a reference. This would make the framework very useful for the development of standardised education and it also creates a solid foundation for qualification.

The approach used in this study would likely work also for developing standardised education outside the information security field, and in other countries, even outside Europe. A necessary condition is that broadly supported generic job profiles are available. Outside Europe, a more mature standard competence framework than e-CF may be preferred.

References

Anderson, R. (2001), "Why Information Security is Hard – An Economic Perspective", in *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, pp. 358-367.

Biemans, H., Nieuwenhuis, L., Poell, R., Mulder, M. and Wesselink, R. (2004), "Competence-based VET in The Netherlands: background and pittfalls", *Journal of Vocational Education and Training*, Vol. 56 No. 4, pp. 523-538.

Bishop, M., Burley, D., Buck, S., Ekstrom, J.J., Futcher, L., Gibson, D., Hawthorne, E.K., Kaza, S., Levy, Y., Mattord, H. and Parrish, A. (2017), "Cybersecurity Curricular Guidelines", in Bishop, M., Futcher, L., Miloslavskaya, N. & Theocharidou, M. (Eds), *Information Security Education for a Global Digital Society*, Springer, pp. 3-13.

Bologna Working Group (2005), *A Framework for Qualifications of the European Higher Education Area*, Ministry of Science, Technology and Innovation, Copenhagen.

Burke, J.W. (1989), *Competency based education and training*, The Falmer Press, London.

Butler, K., Cunningham, R.K., Van Oorschot, P.C., Safavi-Naini, R., Matrawy, A. and Clark, J. (2018), "A Discussion on Security Education in Academia", *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto Canada, October, 2018*, ACM, New York, pp. 2187-2188.

CEN (2014), *CEN Workshop Agreement CWA 16234:2014 Part 1, European e-Competence Framework 3.0 - Part 1: A common European Framework for ICT Professionals in all industry sectors*, CEN, Brussels.

CEN (2018), *CEN Workshop Agreement CWA 16458-1:2018 E European ICT professional role profiles - Part 1: 30 ICT profiles*, CEN, Brussels.

Curry, L. and Docherty, M. (2017), "Implementing Competency-Based Education", *Collected Essays on Learning and Teaching*, Vol. 10, pp. 61-73.

Davidovitch, N. (2013), "Learning-Centered Teaching And Backward Course Design – From Transferring Knowledge To Teaching Skills", *Journal of International Education Research*, Vol. 9 No. 4, pp. 329-338.

De Zan, T. (2019), *Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions*, GCSEC, Rome.

Dedović, L. and Mušić, D. (2017), "Competency-based learning model in practice", in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, September 14-16, 2017*, IEEE, Subotica, pp. 39-45.

Delamare Le Deist, F. and Winterton, J. (2005), "What is competence?", *Human Resource Development International*, Vol. 8 No. 1, pp. 27-46.

Draaisma, A., Meijers, F. and Kuijpers, M. (2018), "The development of strong career learning environments: the project 'Career Orientation and Guidance' in Dutch vocational education", *Journal of Vocational Education and Training*, Vol. 70 No. 1, pp. 27-46.

Elken, M. (2017), "Standardization of (higher) education in Europe – policy coordination 2.0?", *Policy and Society*, Vol. 36 No. 1, pp. 127-142.

Ennis, M.R. (2008), *Competency Models: A Review of the Literature and the Role of the Employment and Training Administration (ETA)*, Employment and Training Administration, U.S. Department of Labor, Washington DC.

EQF (2008), *The European Qualifications Framework for Lifelong Learning (EQF)*, Office for Official Publications of the European Communities, Luxembourg.

Frank, J.R., Mungroo, R., Ahmad, Y., Wang, M., De Rossi, S. and Horsley, T. (2010), "Toward a definition of competency-based education in medicine: a systematic review of published definitions", *Medical Teacher*, Vol. 32, pp. 631-637.

Heusdens, W.T., Baartman, L.K.J. and De Bruijn, E. (2018), "Knowing everything from soup to dessert: an exploratory study to describe what characterises students' vocational knowledge", *Journal of Vocational Education and Training*, Vol. 70 No. 3, pp. 435-454.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design Science in Information Systemes Research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75-105.

Hughes, D., Law, B. and Meijers, F. (2017), "New school for the old: Career guidance and counselling in education", *British Journal of Guidance & Counselling*, Vol. 45, pp. 133-137.

ISACA (2018), *ISACA Exam Candidate Information Guide*, ISACA, Schaumburg.

ISF (2013), *The modern CISO: Managing risk and delivering value. ISF Briefing No. 23*, ISF, London.

Johannesson, P. and Perjons, E. (2014), *An Introduction to Design Science*, Springer, Cham.

Koenen, A.K., Dochy, F. and Beghmans, I. (2015), "A phenomenographic analysis of the implementation of competence-based education in higher education", *Teaching and Teacher Education*, Vol. 50, pp. 1-12.

Kuijpers, M. and Scheerens, J. (2006), "Career competencies for the modern career", *Journal of Career Development*, Vol. 32, pp. 303-319.

Leggett, T. (2015), "Competency-Based Education: A Brief Overview", *Radiologic Technology*, Vol. 86 No. 4, pp. 445-448.

Martinez-Brawleyu, E.E. and Zorita, P.M.B. (2007), "Tacit and Codified Knowledge in Social Work: A Critique of Standardization in Education and Practice", *Families in Society: The Journal of Contemporary Social Services*, Vol. 88 No. 4, pp. 534-542.

Morcke, A.M., Dornan, T. and Eika, B. (2013), "Outcome (competency) based education: an exploration of its origins, theoretical basis, and empirical evidence", *Advances in health Sciences Education*, Vol. 18 No. 4, pp. 851-863.

Morgan, S. (2019), *The 2019/2020 Official Annual Cybersecurity Jobs Reports*, Herjavec, Toronto.

Mulder, M., Weigel, T. and Collins, K. (2006), "The concept of competence concept in the development of vocational education and training in selected EU member states. A critical analysis", *Journal of Vocational Education and Training*, Vol. 59 No. 1, pp. 65-85.

Norman, G., Norcini, J. and Bordage, G. (2014), "Competency-Based Education: Milestones or Millstones?", *Journal of Graduate Medical Education*, Vol. 6 No. 1, pp. 1-6.

NVAO (2018), *Assessment Framework for the Higher Education Accreditation System of the Netherlands*, Accreditation Organisation of the Netherlands and Flanders, The Hague.

Parker, A. and Brown, I. (2019), "Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa", in Venter, H., Loock, M, Coetzee, M., Eloff, M. & Eloff, J. (Eds), *17th International Conference, ISSA 2018, Pretoria, South Africa, August 15-16, 2018*, Springer, pp. 176-192.

Richards, J.C. (2013), "Curriculum Approaches in Language Teaching: Forward, Central, and Backward Design", *RELC Journal*, Vol. 44 No. 1, pp. 5-33.

Sabin, M., Alrumaih, H. and Impagliazzo, J. (2018), "A Competency-based Approach toward Curricular Guidelines for Information Technology Education", in *EDUCON2018, IEEE Global Engineering Education Conference, Santa Cruz, Spain, April 18-20, 2018*, IEEE, pp. 1214-1221.

Salman, M., Ganie, S.A. and Saleem, I. (2020). "The concept of competence: a thematic review and discussion", *European Journal of Training and Development*, Vol. 44 No. 6/7, pp. 717-742.

Smith, S.S. (2017), *2017 Internet Crime Report*, FBI, Washington DC.

Soare, E. (2015), "Perspectives on designing the competence based curriculum", *Procedia – Social and Behavioral Sciences*, Vol. 180, pp. 972-977.

Spruit, M. and Van Noord, F. (2011), *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers*, CPNI, The Hague.

Spruit, M. and Van Noord, F. (2014), "Qualification for Information Security Professionals", *Proceedings of the Symposium Cyber Security Science and Engineering IST-122, Tallinn, Estland, Oktober 13-14, 2014*. doi: 10.14339/STO-MP-IST-122-14-doc.

Spruit, M. and Van Noord, F. (2017), *Job profiles for information security 2.0*, PVIB, Nijkerk.

Sultana, R.G. (2009), "Competence and competence frameworks in career guidance: complex and contested concepts", *International Journal for Educational Vocational Guidance*, Vol. 9, pp. 15-30.

Tarman, B. (2016), "Innovation and education", *Research in Social Sciences and Technology*, Vol. 1 No. 1, pp. 77-97.

Van Noord, F. and Barthel, J.P. (2019). Inventarisatie van erkende cyber-securityopleidingen in Nederland. *IB Magazine*, Vol. 19 No. 3, pp. 8-11.

Vogel, R. (2016), "Closing the cybersecurity skills gap", *Salus Journal*, Vol. 4 No. 2, pp. 32-46.

Winterton, J., Delamare Le Deist, F. and Stringfellow, E. (2006), *Typology of knowledge, skills and competences: clarification of the concept and prototype*, Office for Official Publications of the European Communities, Luxembourg.

Table I: Competence Information security management (E.8) on competence level 3 (CEN, 2014) with modifications (added text in italic, removed text in strike through).

Competence	Level	Knowledge Knows/is aware of/ is familiar with	Skills Is able to
E.8, Information security management: [Original text removed] *Is able to set up an information security strategy of an organisation, evaluate the information security risks and implement, monitor, test, evaluate and modify the required controls for the organisation's information and ICT.*	3 *(bachelor level):* [Original text removed]	*K0 the principles and models for information security and its management* K1 the *principles of information*~~organisation's~~ security ~~management~~ policy and ~~its~~ *the potential* implications for *business processes and* engagement with customers, suppliers and subcontractors K2 the best practices and standards in information security management K3 the ~~critical risks for information security management~~ *relevant threats, vulnerabilities and controls for the information systems of the organisation* K4 the ICT internal audit approach ~~K5 security detection techniques, including mobile and digital~~ K6 cyber attack techniques and counter measures ~~for avoidance~~ K7 computer forensics *K8 the principles, standards en techniques for SIEM (security information and event analysis)*	*S0 organise information security management* S1 document the information security management policy, linking it to business strategy S2 analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack S3 establish a*n* ~~risk management~~ *information security* plan to ~~feed and produce preventative action plans~~ *elaborate information security controls and facilitate and stimulate its implementation* S4 perform security audits S5 apply monitoring and testing techniques S6 establish the recovery plan ~~S7 implement the recovery plan in case of crisis~~

Table II: Competence Research (G.4) on competence level 4.

Competence	Level	Knowledge Knows/is aware of/ is familiar with	Skills Is able to
G.4, Research: Is able to design and execute a scientific research project and publish the results.	4 (master level)	K1 principles of (technical) research K2 methods for (technical) research K3 techniques for (technical) research K4 guidelines for scientific (technical) writing K5 principles and techniques for references to literature	S1 describe the reason for a research project S2 formulate (technical) research questions S3 select and apply appropriate research methods S4 select and apply research techniques effectively S5 manage research data (incl. pseudonymisation and anonymisation) S6 assess the quality of research data S7 analyse research data (incl. statistics) S8 formulate conclusions and recommendations S9 write a research report or a research paper S10 use reference management software

Table III: Competence Information security management (E.8) divided into sub-competences.

Competence	Sub-competence
E.8, Information security management: Is able to set up an information security strategy of an organisation, evaluate the information security risks and implement, monitor, test, evaluate and modify the required controls for the organisation's information and ICT.	• Is able to apply the main principles (incl. security-by-design), models, methods, techniques and standards for information security and its management to a specific organisation. • Is able to explain which impact people have on information security and point out which interventions can change their behaviour. • Is able to draw up an information security strategy and an information security plan for a specific organisation and explain its impact on the business processes and the relation with customers, suppliers and subcontractors. • Is able to monitor, test, review, audit and evaluate the security of information and indicating improvements based on the findings. • Knows the main threats and threat scenarios related to information, including mobile equipment and industrial control systems, and is able to explain the impact on a specific organisation. • Knows the main preventive, detective and repressive controls with respect to information, including mobile equipment and industrial control systems, and is able to select and apply the controls in a specific organisation. • Knows the characteristics and applications of digital forensics and is able to explain the impact on a specific organisation. • Is able to implement monitoring and logging of security data and security incidents in an organisation and evaluate the output.

Table IV: Deriving learning goals from sub-competences.

Competence	Sub-competence	Learning goals
G.4, Research (level 4): Is able to design and execute a scientific research project and publish the results.	• Is able to set up and carry out a scientific research using appropriate scientific research methods and techniques.	Knows: K1 principles of (technical) research K2 methods for (technical) research K3 techniques for (technical) research Is able to: S1 describe the reason for a research project S2 formulate (technical) research questions S3 select and apply appropriate research methods S4 select and apply research techniques effectively S5 manage research data (incl. pseudonymisation and anonymisation) S6 assess the quality of research data S7 analyse research data (incl. statistics) S8 formulate conclusions and recommendations
	• Is able to describe and justify a research in a report or paper.	Knows: K4 guidelines for scientific (technical) writing K5 principles and techniques for references to literature Is able to: S9 write a research report or a research paper S10 use reference management software

Table V: Job profile for ICT Security Specialist 3 (for clarity, parts of text have been removed) (Spruit and Van Noord, 2017).

Profile title	ICT Security Specialist 3		
Summary	Designs and implements the organisation's ICT security policies.		
Mission	Proposes and implements technical security measures for ICT. Advises and supports to ensure secure ICT operation. Takes direct action to secure all or part of a network or system. Is recognised as the ICT security expert by peers.		
Deliverables	Accountable	Responsible	Contributor
	• Knowledge base on ICT security	• ICT security improvement proposals • New technology integration proposals • Technical ICT security solutions, measures and updates • Selection and implementation of security tools • ……	• Risk Management strategy • ICT security policies and its implementation • Risk analyses for ICT • ……
Main tasks	• Watch in-depth technology trends with respect to ICT security • Observe current threats and threat trends and determine their possible impact on the org. • Provide knowledge base on information security • Draw up improvement proposals for ICT security • Draw up proposals for integration of new information technology • ……		
e-Competences (from e-CF)	A.7. Technology trend monitoring		Level 4
	B.4. Solution deployment		Level 4
	E.3. Risk management		Level 3
	E.8. Information security management		Level 3
General competences	G.3. Communication and persuasion		Level 2
	G.4. Research		Level 4
	G.7. Analytical skills		Level 4
	G.8. Integrity		Level 2
Experience	A completed master study in the ICT domain or equivalent level of knowledge and skills.		
KPI	Necessary ICT security measures in place and effective.		

Figure 1: Structure of the Master Cyber Security Engineering.