Qualification for Information Security Professionals

Marcel Spruit
The Hague University of Applied Sciences
THE NETHERLANDS

m.e.m.spruit@hhs.nl

Fred van Noord
Dutch Society for Information Security PvIB
THE NETHERLANDS

fredvannoord@pvib.nl

ABSTRACT

Worldwide there is a lack of well-educated and experienced information security specialists. The first step to address this issue is arranging enough people with a well-known and acceptable basic level of information security competences. However, there might be a lot of information security education and training, but there is anything but a well-defined outflow level with a known and acceptable basic level of information security competences. There exists a chaotic situation in respect of the qualification of information security professionals, with the emergence of a large number of difficult to compare certificates and job titles. Apparently the information security field requires uniform qualifications that are internationally recognized. Such qualifications could be an excellent way of unambiguously clarifying the knowledge and skills of information security professionals. Furthermore it gives educational institutions a framework which facilitates the development of appropriate information security education and training.

1.0 INTRODUCTION

In today's information society, it is important for every organization to handle (digitalized) information with care. Organizations need to protect their growing volumes of information against an increasingly complex set of threats. This calls for well-educated information security specialists.

However, worldwide there is a lack of well-educated information security specialists. The first step to address this issue is arranging enough people with a well-known and acceptable basic level of information security competences. Intended information security specialists can use this basic level as a foundation on which they build their specialization.

Do we already have enough education and training which deliver people with a known and acceptable basic level of information security competences? We are still far from that. There is a lot of information security education and training, but there is anything but a well-defined outflow level with a known and acceptable basic level of information security competences.

Over the past few years, a chaotic situation has arisen in respect of the qualification of information security professionals, with the emergence of a large number of difficult to compare certificates and job titles. As a consequence, information security professionals are unable to clearly identify their knowledge and skills on the basis of their job title and the supporting certificates. Employers are unable to see if a candidate for a security job is a well-trained and experienced information security professional. And educational institutions are reluctant to develop new information security education and training.

Apparently the information security field requires uniform qualifications which are internationally recognized. Such qualifications could be an excellent way of unambiguously clarifying the knowledge and skills of information security professionals and give educational institutions a framework which facilitates the development of appropriate information security education and training. The latter leads to more and better educated professionals with a recognized basic level of cyber security competences.

2.0 PROGRAMME QUALIFICATION OF INFORMATION SECURITY

Initiated by the Dutch Association of Information Security PvIB a number of well known Dutch and multinational organizations[1] have joined forces to start the programme Qualification of Information Security (QIS). The programme strives for a clear and transparent situation for qualification. The aim is the realization of a uniform qualification framework for information security professionals that is widely supported and that is connected to the European e-Competence Framework (e-CF) as well as existing qualification frameworks for information security.

The intended qualification framework is targeted to:

- The information security professionals. They can use the qualification system for showing their competences and for managing their education and training.
- The employers. They can use the qualification system for selecting and hiring information security professionals.
- The educators. They can use the qualification system for setting up information security education and training.

3.0 APPROACH

The programme articulated the steps to realize uniform qualification for information security professionals:

- Check whether there is sufficient public support for a (new) qualification system.
- If so, formulate the design principles that must be met.
- Describe the information security field and it's typical jobs.
- Define a job profile for each typical job.
- Define an education profile for each typical job.
- Set up a managed qualification system.

4.0 PUBLIC SUPPORT AND DESIGN PRINCIPLES

An essential precondition for a qualification system is broad acceptance by on the one hand the group of professionals concerned, and on the other hand the employers that can use the profiles for the recruitment and the selection of professionals and the educational institutions that can use the profiles for establishing education and training.

The first step of the programme was to set up a preliminary investigation to check whether there is significant public support for uniform qualification for information security professionals. The preliminary investigation started in 2011 and delivered its report in April 2011 [1].

[1] Rabobank, ING, ABN AMRO, EY, AkzoNobel, Dutch national government, Dutch Cyber Security Council (Cyber Security Raad), ECP (Programme Digital Skills & Safety) and PvIB

As part of the preliminary investigation a desk study has been performed, as well as 23 individual and group interviews with information security professionals, employers, educators and certification bodies. The first results were discussed during a seminar with information security professionals.

The picture that emerged from the investigation was that a uniform qualification system for information security professionals was very welcome, with particularly strong support among information security professionals and educators. Furthermore it was found that the intended qualification system has to meet a number of design principles:

- It covers the full scope of information security (information risk management and ICT security), but not the small-scale and specialized jobs.
- It contains qualifications on different levels, for example secondary vocational, higher vocational and university level.
- It contains a body of knowledge and skills, as well as keeping up knowledge and skills.
- It is compliant with an international standard for qualification, later on particularized to the European e-Competence Framework (e-CF) [2].
- It shows how it incorporates existing qualifications for information security, such as CISSP, CISM, ISSMP, SSCP et cetera.
- It provides for a transitional provision for professionals already working in information security.
- Its qualifications are recognized internationally.
- It is a suitable basis for a certification registry.
- It is managed and supported by an independent organization.

As there was particularly strong support among information security professionals and educators, the support among employers became a critical success factor. To make sure that the intended qualification system as well as the design principles could count on significant support among employers a covenant has been drawn up [3]. The aim of the covenant was that employers could endorse the intended qualification system and state that they have the intention to use the qualification system once it becomes available. The covenant was presented to the major Dutch employers' federations and a significant number of employers. During a information security seminar in May 2013 the first signatures were put under the covenant by representatives of eight large well-known Dutch organizations. So it seems that there is sufficient support for the intended qualification system by employers.

To ensure that broad acceptance remains during the progress of the programme, information security professionals, employers and educators are participating in each step of the programme. Furthermore, the intermediate results will be reviewed by representative groups from the PvIB (representing the information security professionals), the QIS steering committee and projects committee (representing the employers), as well as providers of information security education and training (representing the educators).

5.0 INFORMATION SECURITY AND TYPICAL JOBS

5.1 Information security

Information security is preservation of confidentiality, integrity and availability of information [4]. This definition clearly indicates that information security has a broad scope. Our preliminary investigation [1] revealed that information security professionals distinguish various domains within information security.

Although several breakdowns into domains were suggested the following one had the widest support:

- *Information risk management*. The set of coordinated activities to direct and control an organisation with regard to risks related to the organisation's information [5]. This involves spoken, written, printed, digital and other data. The scope therefore goes beyond ICT.
- *ICT security*. This involves the design, implementation, maintenance and evaluation of security measures relating to ICT (hardware and software). In this domain thorough knowledge of ICT plays an essential role.
- A number of domains within information security that already have recognized qualification of their own: *IT audit* [6], *forensic investigation* [7] and *business continuity management* [8].
- A number of small-scale domains, such as cryptography, that are exercised by a relatively small number of professionals.

We will use this breakdown.

The domains that already have recognized qualification in place are beyond our scope, because there is no need to set up any qualification if there already exists recognized qualification.

For the small-scale domains with only few practitioners it is not meaningful to invest in uniform qualification. Therefore these domains are also beyond our scope.

Our scope is therefore limited to the two domains mentioned first: *information risk management* and *ICT security*.

When uniform and recognized qualification levels are defined for information risk management and ICT security, as was done previously for the domains that already have recognized qualification in place, those qualification levels can be considered well-known and acceptable basic levels of information risk management and ICT security competences. Intended information security specialists can use these well-known and acceptable basic levels as a foundation on which they build further specialization (see Figure 1).

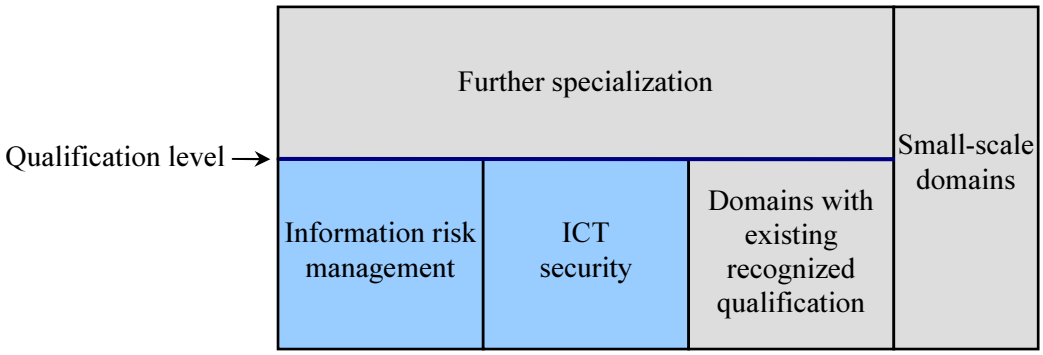

Figure 1: Information security domains.

Given the multitude of possible specializations it is not useful to formulate uniform qualification levels for specializations.

5.2 Typical information security jobs

Anyone, in any job, has to deal with information security more or less. For most people information security

is only one of the many aspects of their daily work. It requires some attention, but it is only a minor aspect. For some people, however, information security is their main focus, or at least one of their major concerns. These people, the professionals in information security, work on specifying, implementing, supporting, advising on and/or monitoring information security. The jobs we look for relate to these professionals in information security.

In practice we come across many different job names in the domains information risk management and ICT security. We see that different job names require different levels of knowledge and skills. Some examples of job names are shown in Table 1, arranged by domain and level.

Table 1: Examples of job names, arranged by domain and level.

Domain / Level	Information risk management	ICT security
Strategic and/or tactical (higher vocational or university grade)	• Chief Information Security Officer • Chief Information Risk Officer • Information Security Manager • Information Risk Manager • Senior Information Security Consultant • Information Risk Consultant	• ICT Security Manager • Chief Information Technology Security Officer • Senior ICT Security Consultant • Senior ICT Security Specialist • Senior Cyber Security Consultant • Senior Cyber Security Specialist
Tactical and/or operational (secondary or higher vocational grade)	• Information Security Officer • Information Risk Officer • Information Security Consultant	• ICT Security Officer • ICT Security Consultant • ICT Security Specialist • Cyber Security Specialist • Cyber Security Consultant

Any organization may choose its own job names and therefore these names are not very meaningful outside the organization. However, the division into two domains and two levels leads to very different jobs with different levels of knowledge and skills. We need to be able to distinguish between those different kinds of jobs. Therefore we identified one typical job for each cell in Table 1 (see Table 2).

Table 2: Typical jobs in information security.

	Information Risk Management	ICT security
Strategic and/or tactical	**Chief Information Security Officer** (CISO; also referred to as 'Corporate Information Security Officer', or 'Chief/Corporate Information Risk Officer')	**ICT Security Manager** (also referred to as 'Cyber Security Manager')
Tactical and/or operational	**Information Security Officer** (ISO; also referred to as 'Information Risk Officer')	**ICT Security Specialist** (also referred to as 'Cyber Security Specialist')

The name of each typical job is of course arbitrary, but we selected it such that it is very common in its domain and level. Also, the two names of typical jobs in ICT security already exist in the documentation of CEN [9].

6.0 JOB PROFILES

The four typical jobs we specified in the previous section are the basis for qualification of information security professionals. To be able to qualify for those typical jobs we first have to elaborate the jobs. For each one we need a formal description, called a job profile.

The job profiles are based on medium-sized information processing organisations in which information security plays a prominent role, such as ministries, agencies, medium-sized banks and industrial organisations. Organisations that are either less or more complex in terms of information security impose less, respectively more, strict demands on their information security positions.

In section 4.0 we mentioned that one of the design principles for the intended qualification system is that it must be compliant with an international standard for qualification, later on particularized to the European e-Competence Framework (e-CF) [2]. The e-CF defines and elaborates professional competences for the ICT field. When working out our four job profiles we will use competences defined in the e-CF.

The e-CF is accompanied by CWA 16458 [9] which specifies standard job profiles for ICT jobs. It is a matter of course that we use the template defined in CWA 16458 for our four job profiles. However, we added two items, namely *general competences* and *experience*.

6.1 Competences

A competence is a demonstrated ability to apply knowledge, skills and attitude for achieving observable results [2]. A competence is usually described by a concise statement of what knowledge, skills and attitude are required in a specific context. The knowledge and skills components of a competence can have certain levels, ranging from 1 through 5 (see Table 3).

Table 3: Competence levels.

Level	Knowledge	Skills
5	Exceptionally comprehensive and detailed knowledge and understanding of the subject	Guiding others who carry out the activity in a very complex context
4	Very extensive and detailed knowledge and understanding of the subject	Carrying out the activity in a very complex context
3	Knowledge and understanding of the subject in detail	Carrying out the activity in a difficult context
2	Knowledge and understanding of all major aspects of the subject	Carrying out the activity in a simple context
1	Basic knowledge and understanding of the subject	Carrying out the activity in a simple context under guidance

A dilemma is the number of competences to specify in a job profile. Too few competences makes the profile too light and not very distinctive. Too many competences make the profile too heavy and very difficult to comply to.

We learned from an informal discussion with an examination body that they figured out in an explorative pilot that a group of experienced testers scored across the board on only one e-CF competence above par, namely testing. Further investigation was not publicly reported, but we have to consider the possibility that

the profession of tester requires only one or two e-CF competences as a solid foundation, and of course some general competences too. Therefore, it is likely that any other ICT related job also requires only a small number of e-CF competences, as well as some general competences.

CEN specifies in CWA 16458 [9] two to five e-CF competences per job profile, and no general competences.

CIGREF [10] includes up to twenty-two e-CF competences in a job profile.[2] The profile Chief Information Security Officer (CISO) for example contains eight e-CF competences, and no general competences.

We believe that CEN is closest to the optimum number of e-CF competences, albeit somewhat on the high side given the experience of the examination body we spoke. In our believe the optimum number of competences in a job profile is two to four e-CF competences, as well as three to six general competences.

Note that working with standard job profiles with standard competences reduces the fit between a job profile and a job description for a specific situation. In the traditional approach a job description can be drawn up by defining, out of the blue, all competences required for the specific situation. If done well, the job description matches the needs of the organization precisely. However, when working with standard job profiles with standard competences the job profile has to be selected that comes closest to the job description needed. As that does not match the specific needs precisely, the organization has to tune the job description to match its needs. The advantage of standard job profiles with standard competences is not to define job descriptions more easily, but to get more possibilities for education, training, testing, qualification and exchange, due to the standardization and the consequent economies of scale.

Existing frameworks of for example (ISC)[2] and ISACA and ad hoc job profiles of for example ISF [11] are built on non-standard competences and have their own qualification specified, or do not refer to any qualification.

6.2 Elaborate job profiles

A job profile is a formal job description that describes the mission, tasks and responsibilities of a practitioner of a specific profession and specifies the competences (knowledge, skills and attitude) that the practitioner must have. The job profiles are drawn up using the template from CWA 16458 [9]. Two items were added, namely *general competences* and *experience*.

As discussed in section 5.0 we have four typical jobs for which we need job profiles:

- Chief Information Security Officer (CISO).
- Information Security Officer (ISO).
- ICT Security Manager.
- ICT Security Specialist.

Two job profiles, ICT Security Manager and ICT Security Specialist, were adopted from CWA 16458 (profiles 11 and 12). However, extensive review of the profiles revealed that the content of these profiles did not match the expectations of the consulted professionals. For example, the specified e-CF competences were not entirely in line with the expectations of the professionals and general competences were not specified at all. In other areas, too, the profiles required modifications.

[2] The IT Project Manager profile has twenty-two e-CF competences.

The job profiles for CISO and ISO were not specified in CWA 16458. This is not entirely unexpected, since CISO and ISO are not ICT jobs and as such are beyond the scope of the document (although other non-ICT functions are described in CWA 16458, such as Chief Information Officer and Quality Assurance Manager).

Table 4 shows one of the job profiles for information security, namely ICT Security Specialist. All four profiles are described in the job profiles document [12].

Table 4: Job profile for ICT Security Specialist.

Profile title	**ICT SECURITY SPECIALIST**		
Summary statement	Implements the organisation's ICT security policies.		
Mission	Proposes and implements necessary security controls. Advises, supports and informs to ensure secure ICT operation. Takes direct action to secure all or part of a network or system. Is recognised as the ICT technical security expert by peers.		
Deliverables	Accountable	Responsible	Contributor
	• Knowledge base on ICT security	• New technology integration proposals • ICT security controls and updates • Selection and implementation of security tools • ICT security assessments, tests, reviews and audits • Monitoring security of ICT	• Risk Management policy • ICT security policies and its implementation • Risk analyses for ICT • ICT continuity plan
Main tasks	• Watch technology trends with respect to ICT security • Provide knowledge base on information security • Provide proposals for the integration of new technology • Implement necessary security controls and updates • Select and implement security tools • Monitor and perform ICT security assessments, tests, reviews and audits • Monitor security of ICT resources and evaluate ICT security risks • Test the ICT continuity plan • Make recommendations to line management concerning ICT security and risks		
e-Competences (from e-CF)	A.7. Technology Trend Monitoring		Level 3
	B.4. Solution Deployment		Level 2
	E.8. Information Security Management		Level 3
General competences	G.3. Communication and persuasion		Level 2
	G.4. Technical research		Level 3
	G.7. Analytical skills		Level 3
	G.8. Integrity		Level 3
Experience	A completed secondary vocational study in the ICT domain or equivalent study		
KPI	ICT security measures in place and effective		

The competences in the profile are described in more detail elsewhere. The e-CF competences are elaborated in the e-CF framework [2] and the general competences are elaborated in the job profiles document [12].

To get an impression of the extent to which competences have been elaborated, Table 5 shows the details of one competence, Information Security Management [2]. The competence description shows a brief characterization of the competence, the level of the competence and its knowledge and skills components.

Table 5: Competence E.8: Information Security Management [2].

e-Competence	Level	Knowledge Knows/is aware of/ is familiar with	Skills Is able to
E.8, Information Security Management Implements information security policy. Monitors and takes action against intrusion, fraud and security breaches or leaks. Ensures that security risks are analysed and managed with respect to enterprise data and information. Reviews security incidents, makes recommendations for security policy and strategy to ensure continuous improvement of security provision.	Level 3: Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches.	K1 the organisation's security management policy and its implications for engagement with customers, suppliers and subcontractors K2 the best practices and standards in information security management K3 the critical risks for information security management 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	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 risk management plan to feed and produce preventative action plans S4 perform security audits S5 apply monitoring and testing techniques S6 establish the recovery plan S7 implement the recovery plan in case of crisis

A job profile of a typical job is not meant to be used directly as a job description. 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 organization will wish to give its own twist to the way in which the job description has been specified in order to match its needs. Therefore the contents of a job description will usually differ from generic job profiles. As long as the differences do not become too large (80/20 rule), the job profiles provide a sound indication of the information security jobs, and the requirements imposed on them.

An organization can label a job description with any name it wants. Even if an organization opts for copying a profile of a typical job, for example Chief Information Security Officer, it may choose to label it differently, for example Information Security Manager (different label, same content).

7.0 EDUCATION PROFILES

The job profiles described in the previous section contain competences. Every practitioner should master the competences specified for his or her job. This implies that the practitioner must be able to acquire those competences. There are two possibilities for acquiring competences, namely learning in course (education and training) or learning in practice (on the job). A combination is also possible.

Learning in course and learning in practice both have advantages and disadvantages. Learning in course ensures mastery of the intended competences more quickly, but the learning effect is generally limited to just those competences. Learning in practice generally requires more time before the intended competences are acquired, but on the other hand, other competences are acquired too. The latter may not be immediately necessary but it does provide a broader basis and as a consequence greater flexibility in understanding and practical performance. Because of the different advantages and disadvantages, both options are useful.

To make learning in course possible, appropriate education and training must be available. Education and training can be established on the basis of the competences listed in the job profiles. The competences are described in detail in e-CF (see Table 5). However, for someone assigned to design a course for a specific job profile, the level of detail is, by and large, too low. Therefore we need to elaborate the competences into more detailed sets of learning goals. Table 6 shows this for one of the e-CF competences. Obviously, the resulting level of detail is a compromise between the precision required for standardization and the autonomy of the educator.

Table 6: Competence Information Security Management elaborated into learning goals.

e-Competence	Level	Knowledge and skills	Learning goals | level 1..5
E.8, Information Security Management	Level 3	Knows/is aware of/ is familiar with: K1 the organisation's security management policy and its implications for engagement with customers, suppliers and subcontractors K2 the best practices and standards in information security management K3 the critical risks for information security management 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	Has knowledge and understanding of: • The main models, methods and techniques with respect to information security, their characteristics and application | 3 • The main models, methods and techniques with respect to the management of information security, their characteristics and application | 3 • The main principles and models with respect to governance and alignment, their characteristics and application | 2 • The relations between information security and other appearances of security (integral security) | 3 • The main models, methods and techniques with respect to risk analysis, their characteristics and application | 3 • The main threats for information systems and ICT, including mobile devices and process control systems | 3 • The main preventive and repressive controls for information systems and ICT, including mobile devices and process control systems | 3 • The main models, methods and techniques with respect to continuity management, their characteristics and application | 2 • The relevant standards with respect to information security | 3 • The relevant legislation with respect to information security | 3 • The methods and techniques with respect to audit and peer review, their characteristics and application | 3 • The characteristics and application of digital forensic research | 1

		Is able to: 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 risk management plan to feed and produce preventative action plans S4 perform security audits S5 apply monitoring and testing techniques S6 establish the recovery plan S7 implement the recovery plan in case of crisis	Is able to: • Formulate and disseminate an information security strategy | 2 • Set up and manage an information security organization | 2 • Formulate and implement an information security plan, including a disaster recovery section | 3 • Perform risk analyses | 3 • Perform information security audits and peer reviews | 2 • Read, interpret and judge risk analyses, audit and assessment reports | 3 • Present and explain the results of a risk analysis to specialists and non-specialists | 3 • Formulate recovery measures after a severe ICT incident | 3 • Formulate the commission to a digital forensic investigation | 1

An education profile is the description of the competences of a job profile, in which the competences have been elaborated into learning goals. We developed education profiles for the four job profiles described in section 6.

Educational institutions can use the education profiles to establish appropriate education and training or to adapt existing education and training. If different studies for a specific job profile are based on the same education profile, the studies are equivalent and can be accredited more effectively. As a consequence specialization training can count on larger groups of participants with a similar well-known and recognized entry level.

Little action need be taken to provide for learning in practice. The huge variety of jobs in all kinds of businesses and bodies offer sufficient opportunities for acquiring competences in practice. Examination of the competences can be based on the competence descriptions in e-CF (see Table 5).

Learning in course and learning in practice occur in all kinds of combinations. Sometimes, the two are interchangeable, for example, when an individual with several years of specific experience is for that reason exempted from parts of a study. Sometimes, the two complement each other. For example, when the acquisition of the knowledge part of a competence is learned in a study and the skills part is learned on the job.

Both learning in course and learning in practice require a mechanism to examine the acquired competences, so that people can qualify for the competences and in the end for a job profile. This calls for one or more examination bodies that establish an examination process with uniform examination criteria. The examination bodies have to make sure that the examination criteria are kept up to date.

8.0 MANAGED QUALIFICATION SYSTEM

The sets of job and education profiles need to be brought together into a qualification system. In order to operate effectively and continuously the intended qualification system requires an independent organization that manages the system. Agreements with that organization should cover service levels and costs. To boost the international character of the qualification system it might be useful to have the qualification system managed by an international organization.

The organization that manages the qualification system should develop processes and procedures in order to put flesh on the bones of the qualification system. This includes an exemption provision to incorporate existing qualifications for information security (e.g. CISSP or CISM), a transitional provision for professionals already working in information security, procedures for maintaining and extending competences, and possibly a certification registry.

There is a need for recognized education and training with which qualifications can be achieved. These education and training could be new, or existing and tailored to the profiles of the qualification system. Unmodified existing education and training might also qualify for a new profile if its scope already matches the scope of the profile. To assess whether existing education and training match the new profiles it is necessary to map the contents onto the new education profiles.

The intended qualification system should issue qualifications that are recognized internationally. Steps have been taken to bring the qualification system to the attention of the international standardization bodies CEN and ISO. However, standardization is a time consuming process, so we do not expect that the qualification system becomes an international standard on short term. Another approach is to look for mutual recognition with existing qualification systems. This needs to be explored.

9.0 CONCLUSIONS

The information security field requires uniform qualifications which are internationally recognized. Because of that we need a uniform qualification system for information security professionals. There is large public support for such a system, provided that the system meets a number of design principles (see section 4).

We started to realize a uniform qualification system for information security professionals. For that we summarized the information security field, and pointed out typical jobs within this field (see section 5). For each typical job we specified a job profile (see section 6). To facilitate educational institutions establishing appropriate education and training we specified education profiles which elaborate competences into learning goals (see section 7).

Next steps include the working out of qualification system management, including an exemption provision to incorporate existing qualifications for information security (e.g. CISSP and CISM), a transitional provision for professionals already working in information security, procedures for maintaining and extending competences, and possibly a certification registry. Also recognized education and training need to be established. And last but not least the issued qualifications need international recognition.

REFERENCES

[1] Spruit, M. and Noord, F. van (2011) *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers* (in Dutch). Research report. The Hague, The Netherlands: CPNI.NL. http://www.cpni.nl/files/4113/0252/0259/Certificeringsschema_infobev_v1.0_11_april_2011.pdf

[2] 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*. http://ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf

[3] PvIB (2013) *Convenant voor steun aan uniform kwalificatiestelsel voor professionals informatiebeveiliging* (in Dutch). Convenant. Nijkerk, The Netherlands: PvIB.

[4] ISO (2009) *ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary*, ISO.

[5] ISO (2009) *ISO Guide 73:2009, Risk management – Vocabulary*, ISO.

[6] NOREA (2013) *Exam Candidate Information Guide*, ISACA.

[7] ECABO (2010) *Digitaal Forensisch Onderzoeker – Beroepscompetentieprofiel* (in Dutch), ECABO.

[8] Business Continuity Academy, www.businesscontinuityacademy.nl.

[9] CEN (2012) *CEN Workshop Agreement CWA 16458:2012 E, European ICT Professional Profiles*. ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf.

[10] CIGREF (2011) *Information Systems roles in large companies*. http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_IS_roles_in_large_companies_HR_nomenclature_CIGREF_EN.pdf

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

[12] Spruit, M. and Noord, F. van (2014) Job profiles for information security. Nijkerk, The Netherlands: PvIB. www.pvib.nl/download/?id=17696561