# Job profiles for information security 2.0

## A basis for uniform qualification of information security professionals

Picture by suphakit73 / FreeDigitalPhotos.net

| | |
|---|---|
| Stakeholders: | Dutch Association of Information Security Professionals (PvIB) and the programme Qualification of Information Security (QIS) |
| Authors: | Marcel Spruit and Fred van Noord |
| Version: | 2.0 English |
| Publication date: | 1 January 2017 |
| Publisher: | © PvIB, 2017 (www.pivb.nl)<br>ISBN: 978-90-78786-00-9 |

This work has the license *Creative Commons Attribution-NoDerivatives 4.0 International* (CC BY-ND 4.0). See https://creativecommons.org/licenses/by-nd/4.0/.

# Table of contents

# Introduction

## Background

In today's information society, it is becoming increasingly important for every organisation to handle information with care. Organisations are required to protect ever growing volumes of information against an increasingly complex threat scenario. This calls for well-trained and experienced information security professionals. Qualifications are an excellent way of clarifying the knowledge and experience of information security professionals.

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.[1] As a consequence, information security professionals are unable to clearly identify their knowledge and experience on the basis of their job title and the supporting certificates. Employers are unable to see when the candidate before them is a well-trained and experienced information security professional. At the same time, teaching institutions are becoming increasingly cautious in investing in new training programmes in information security.

The Dutch Association of Information Security Professionals (PvIB), an organisation of professionals, has set itself the goal of increasing the level of professionalism within the field of information security, while at the same time establishing a clear and transparent situation in respect of qualification.[2]
A uniform system of qualifications for professionals in information security will provide that clarity.

To be able to ensure uniform qualification of information security professionals, it is first important to identify precisely which professions are represented within the field of information security, what those professions entail and which competences (knowledge and skills) are required. These elements are described in so-called job profiles.

## Purpose

This document provides job profiles for the profession information security .

## Scope

Information security is a subject with greater or lesser relevance to everyone in every organisation. For the majority of people in an organisation, information security is just one of the aspects of their day-to-day work that although requiring sufficient attention, does not occupy a leading role. For example, we expect a System Architect to have focused sufficient attention on security, in the system architecture.

---

[1] *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers (Investigation into the qualification and certification of information security professionals)*, Report VKA/HEC/CPNI, version 1.0, 2011 (in Dutch).

[2] A qualification is a formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards (Reference: European Qualifications Framework, Key Terms). The assessment and validation process is generally based on an exam or the assessment of a portfolio.

And we expect a Software Engineer to produce secure code. Most people have ‘something’ to do with information security. But that does not make them ‘information security professionals’.

For a number of people, however, information security is core business. These people, the ‘true’ information security professionals, have a prominent role in the organisation, specification, execution, support, consultancy and/or monitoring in the field of information security. For them, information security is their central area of attention, or at least one of the most important areas of attention.

Information security professionals work together with other people in other positions in which information security occupies a less prominent position. Many of them are crucial for the performance of the Information security professionals, for example because they offer management or guidance, or deliver essential input or support. These include for example the Chief Executive Officer, the Chief Information Officer, the Enterprise Architect and a variety of others. However, although they are essential for good information security in an organisation, they are not considered information security professionals.

The job profiles described in this document relate only to professionals in information security, in other words, those individuals for whom information security is core business.

## Operating principles

The following operating principles were employed in describing the job profiles for professions within the field of information security:

- The job profiles are drawn up for ‘true’ information security jobs in which so many information security professionals are involved that it is worthwhile drawing up standardised profiles for them.
- The job profiles specify the essential knowledge, skills and experience.
- The job profiles are based on the European e-Competence Framework 3.0 (e-CF).[3]
- The job profiles are broadly supported within the field of information security.
- The job profiles are suitable as a basis for a uniform system of qualifications for information security professionals.

## Accounting

This document was drawn up at the request of the board of the Dutch Association of Information Security Professionals (PvIB) by the PvIB Working Group on the Qualification of Information Security Professionals. The job profiles in this document are intended to be used for a uniform qualification system for information security professionals.

One essential precondition for a job profile is broad acceptance of the profiles on the one hand by the group of professionals in question and on the other hand by the employers and teaching institutions that can make use of the profiles for the recruitment and selection of professionals and the organisation of study programmes, respectively. To ensure broad acceptance, this document has

[3] 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

been reviewed by a representative group from the PvIB, the steering committee and projects committee of the programme Qualification of Information Security, professionals in positions to which the described profiles relate and providers of information security training.

# The profession

The profession of information security is broad in its scope. Initial investigation revealed that within the field of information security, it is important to distinguish between the domains *information risk management* and *ICT security*:[4]

- *Information risk management* is defined as the coordination of activities to direct and control an organisation with regard to risks related to the organisation's information.[5,6] It is aimed at securing the information function as a whole.
- *ICT security* involves the design, implementation, maintenance and evaluation of security measures relating to ICT (hardware and software). In this domain, specialist knowledge of ICT plays an essential role.

Alongside these two domains, within the professional field of information security, there are a number of other domains each with their own uniform qualification, namely IT audit,[7] forensic investigation [8]and business continuity management.[9] Job profiles have already been drawn up for these domains. They are therefore beyond the scope of this document.

There are also a number of small-scale specialist domains such as cryptology, that are exercised by a relatively small number of professionals, and for which it is not meaningful to invest in uniform qualifications and job profiles. These domains are also beyond the scope of this document.

For the domains *information risk management* and *ICT security*, job profiles are drawn up in this document, for the purposes of uniform qualification. These profiles are meant to be applied in the Netherlands and beyond.

---

[4] *Onderzoek naar kwalificatie and certificatie van informatiebeveiligers*, *(Investigation into the qualification and certification of information security professionals),* Report VKA/HEC/CPNI, version 1.0, 2011 (in Dutch).

[5] Based on: *ISO Guide 73:2009, Risk management – Vocabulary*, ISO, 2009.

[6] Information provision involves preparing, storing, processing, viewing, transporting and destroying spoken, written, printed, digital and other data. The scope of information provision therefore goes beyond the scope of ICT.

[7] NOREA, www.norea.nl; *Exam Candidate Information Guide*, ISACA, 2013.

[8] *Digitaal Forensisch Onderzoeker – Beroepscompetentieprofiel (Digital Forensics Investigator – Job competence profile)*, ECABO, 2010 (in Dutch).

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

# Job profiles

To be able to qualify professionals in information security, it is first essential to distinguish which jobs exist in the field of information security, and what those jobs involve. The jobs are described in the form of job profiles.

A job profile provides a formal description of a job. It describes the mission, tasks and responsibilities of the practitioner of the particular profession and specifies the competences (knowledge and skills) that the practitioner must possess.

Within the field of information security, a distinction is made between the domains *information risk management* and *ICT security*. The first is aimed at securing the information function as a whole, the second at securing the ICT systems used.

Within the domain *information risk management* we distinguish between a practitioner at strategic and/or tactical level, a *Chief Information Security Officer*, and a practitioner at tactical and/or operational level, an *Information Security Officer*.

Within the domain *ICT security*, we distinguish between a practitioner at tactical level, an *ICT Security Manager*, and a practitioner at operational level, an *ICT Security Specialist*.[10]

Within the field of information security, we have therefore identified four jobs for which job profiles must be described:

- Chief Information Security Officer (CISO);[11]
- Information Security Officer (ISO);[12]
- ICT Security Manager;
- ICT Security Specialist.

| | **Security of the information** (Information risk management) | **Security of the ICT** (ICT security) |
|---|---|---|
| **Strategic and/or tactical** | CISO | ICT Security Manager |
| **Tactical and/or operational** | ISO | ICT Security Specialist * |

* The job ICT Security Specialist has three qualification levels numbered 1 (secondary vocational education level) through 3 (university level).

[10] The term 'specialist' can be misleading. In daily use, the term specialist often refers to a very expert professional. That is not the intended meaning here. Here the term specialist refers to the fact that the person in question is not a generalist. The specialist intended in this context has developed and trained with a clear focus on ICT security technology. A person may become a very expert professional (in other words a specialist in the daily sense) by acquiring additional knowledge and skills over a period of years, after obtaining a qualification as ICT Security Specialist (for example on the basis of a specific ICT security training programme). In the description provided here there is no separate qualification for such a very expert specialist.

[11] Also referred to as *Corporate Information Security Officer* (CISO), or *Chief/Corporate Information Risk Officer* (CIRO).

[12] Also referred to as *Information Risk Officer* (IRO).

For each of these jobs, a job profile is provided below. These profiles are intended for use within the Netherlands and beyond. For that reason, this document has been drawn up in English.

In an earlier publication by PvIB, the jobs *Information Security Architect* (ISA) and the *Business Information Security Architect* (BISA) were referred to.[13] These jobs are no longer considered separate information security jobs because architecture, also in respect of information security, is seen as the responsibility of the *Enterprise Architect* and *Systems Architect*. In exceptional information security situations, in addition to these two professionals, a *(Business) Information Security Architect* may be required, but nonetheless a separate profile is not justified.

For the description of the job profiles, use was made of the document CWA 16458.[14] Within this document, job profiles are formulated for jobs in the ICT sector. The jobs *ICT Security Manager* and *ICT Security Specialist* are included in those descriptions (profiles 11 and 12).

Initially, the job profiles for *ICT Security Manager* and *ICT Security Specialist* were adopted from the document CWA 16458. However, the *PvIB Working Group on the Qualification of Information Security Professionals* observed that the content of these profiles did not match well with the expectations of the working group. For example, the specified e-competences were not entirely in line with the expectations of the professional group and the necessary general competences, prior education and experience were not specified. In other areas, too, the profiles required further significant alteration. In response, the working group had both profiles carefully reviewed and where necessary revised. Following publication and general distribution of version 1 of this document, additional comments were received that have led to a further revision of the profiles. It also emerged that employers and trainers distinguish between three different levels of ICT Security Specialist. As a consequence, the working group added a further two levels to the ICT Security Specialist,[15] once again had the profiles carefully reviewed, and where necessary revised. New versions of the profiles are contained in this document.

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 positions and as such are beyond the scope of CWA 16458.[16] In this document, the new job profiles for CISO and ISO are included. These profiles were drawn up analogously to the other profiles and have undergone the same reviews and updating processes.

Further advancement and specialisation are possible from within each of the jobs described. An ISO can acquire additional knowledge and skills to become specialised in for example water authority processes, or an ICT Security Specialist 2 can for example specialise further in ethical hacking. The job profiles relate to the ‘standard’ jobs. Further advancement and specialisation is so diverse that no further specific job profiles have been elaborated.

On the other hand, it is also possible to advance into another (standard) job. Obvious pathways for professional improvement are those from ISO to CISO, and from ICT Security Specialist 1 to ICT Security Specialist 2 and from ICT Security Specialist 2 to ICS Security Specialist 3.

---

[13] B. Bokhorst et al., *Functions in information security*, PvIB, 2006.

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

[15] The ICT Security Specialist described in CWA 16458 approximately equates to the second (middle) of the three new profiles for ICT Security Specialist, in other words ICT Security Specialist 2.

[16] Although other non-ICT functions are described in CWA 16458, such as Chief Information Officer, Enterprise Architect, Quality Assurance Manager and Project Manager.

The job profiles list the competences (e-competences and general competences), alongside a competence level for each competence.

As concerns the competences, the choice can be made to include every competence which may be in part or in its entirety be somewhat useful in a specific job profile, in the competence list for that profile. Because each competence consists of a series of competence elements (knowledge or skills) a never-ending list of competence elements is thus created. On the other hand, it can be decided to only include the important competences, the ‘core’ competences. That choice also results in a considerable list of competence elements, but one which does remain manageable. In order to maintain a manageable number of competence elements for each job profile, the second approach has been chosen, in other words including only the ‘core’ competences in the job profiles. For each job profile this means around 8 competences, or more than 100 competence elements. In qualifying for a job profile, all the (core) competences described in the profile are completely tested. It is implicitly assumed that the competence elements that are useful but that do not form part of a core competence, will nonetheless be dealt with in education or in on-the-job training, together with the described core competences. It is after all extremely unlikely that the core competences will be acquired in isolation, either in education or on the job.
The e-competences and general competences are elaborated in a separate document ‘Competences for information security professionals’.

A competence level indicates to what extend a specific competence and in turn the underlying competence elements (knowledge or skill) are mastered. To measure a competence level, a distinction is made between measuring a knowledge level and measuring a skill level. This is elaborated in annex B.
The decision has been taken to operate a single competence level for each competence. This means that the various competence elements (knowledge or skill) that make up a single competence must be mastered at the same level. This results in limited discrepancies with practice, and massively simplifies and clarifies the testing of a specific competence.

# Chief Information Security Officer [17]

| Profile title | CHIEF INFORMATION SECURITY OFFICER (CISO) | | |
|---|---|---|---|
| **Summary statement** | Defines the information security strategy and organises and manages the organisation's information security in line with the organisation's needs and risk appetite. | | |
| **Mission** | Defines the organisation's information security strategy, based on a risk management approach and anticipating the information security threat landscape, trends and business needs. Sets up the information security organisation and determines and assigns necessary resources. Initiates and coordinates information security deployment and integration throughout the organisation. Ensures an appropriate level of information security and information security behaviour based on the organisation's needs and risk appetite. Is recognised as the information security strategy expert by internal and external stakeholders. | | |
| **Deliverables** | **Accountable** | **Responsible** | **Contributor** |
| | • Information security strategy<br>• Information security organisation and expertise<br>• Business continuity organisation<br>• Adapt information security to other security domains<br>• Compliance with information security requirements and architecture<br>• Information security awareness across the organisation<br>• Organisation's risk readiness for emerging information security and ICT risks<br>• Information risk analyses, security designs and solutions<br>• Information security assessments, tests, reviews and audits | • Information security project portfolio<br>• Corporate information security activities and projects<br>• Monitoring the relevant risks for the organisation<br>• Monitoring compliance with policy, legislation and regulation<br>• Coordinated response after major information security or ICT incidents<br>• Corporate information security policies, standards, methods and techniques | • Risk management strategy<br>• Information systems governance<br>• Service Level Agreements<br>• Information security architecture |

[17] This job profile is not included in CWA 16458.

| | | |
|---|---|---|
| **Main tasks** | • Define the organisation's strategy for information security<br>• Organise information security and the necessary expertise<br>• Ensure adaptation of information security to other security domains, including privacy protection, physical security and continuity management<br>• Establish a business continuity organisation<br>• Coordinate the response to serious information security or ICT incidents<br>• Provide an information security project portfolio<br>• Initiate and coordinate corporate information security activities and projects<br>• Provide corporate information security policies, standards, methods and techniques<br>• Monitor and ensure the quality of information risk analyses, security designs and solutions<br>• Monitor and ensure compliance with information security requirements and architecture and consistent application of Security-by-Design and Privacy-by-Design<br>• Monitor and ensure information security awareness throughout the organisation<br>• Monitor the relevant risks for the organisation<br>• Ensure the organisation's risk readiness for emerging information security and ICT risks<br>• Monitor and ensure the quality of information security assessments, tests, reviews and audits<br>• Monitor the extent to which the organisation complies with information security policy, legislation and regulations on the basis of assessments, tests, reviews and audits<br>• Inform senior general management on the status of information security and incidents, and present improvement proposals | |
| **e-Competences (from e-CF)** | D.1. Information Security Strategy Development | Level 4 |
| | E.3. Risk Management | Level 3 |
| | E.4. Relationship Management | Level 3 |
| | E.8. Information Security Management | Level 4 |
| **General competences** | G.1. Leadership | Level 3 |
| | G.3. Communication and persuasion | Level 3 |
| | G.5. Organisational sensitivity | Level 3 |
| | G.6. Management | Level 3 |
| | G.7. Analytical skills | Level 4 |
| | G.8. Integrity | Level 3 |
| **Education and experience** | • A completed relevant Master study[18] or equivalent level of knowledge and skills<br>• Five years' work experience in an information security position<br>• Five years' work experience in a management position | |
| **KPI** | An appropriate level of information security and information security awareness based on the organisation's needs and risk appetite. | |

[18] A Master study in economic, exact, technical or human sciences domain.

# Information Security Officer [19]

| Profile title | INFORMATION SECURITY OFFICER (ISO) | | |
|---|---|---|---|
| **Summary statement** | Implements information security in compliance with the organisation's information security strategy. | | |
| **Mission** | Implements the organisation's information security. Provides information security plan, risk analyses, risk monitoring, incident registration, tools, training and evaluation with respect to information security. Initiates and manages information security and awareness projects. Is recognised as the information security expert by internal and external stakeholders. | | |
| **Deliverables** | **Accountable** | **Responsible** | **Contributor** |
| | • Knowledge base on information security<br>• Registration, analysis and reporting of information security incidents | • Information security implementation<br>• Adapt information security to other security domains<br>• Information security projects<br>• Security awareness training and education<br>• Information system risk analyses<br>• Translating information security needs into security measures<br>• Information security designs and solutions<br>• Monitoring and reporting on information security risks<br>• Information security assessments, tests, reviews and audits | • Information security strategy<br>• Information security project portfolio<br>• Information security architecture<br>• Risk management policy<br>• Corporate information security activities and projects<br>• Corporate information security policies, standards, methods and techniques<br>• Knowledge exchange on information security |

[19] This job profile is not included in CWA 16458.

| | | |
|---|---|---|
| **Main tasks** | • Implement the organisation's information security<br>• Provide knowledge base on information security<br>• Ensure adequate registration, analysis and reporting of information security incidents<br>• Initiate and manage information security projects<br>• Adapt information security activities and projects to other information security domains, including privacy protection and physical security<br>• Provide information security awareness training and education<br>• Perform risk analyses for information systems<br>• Monitor and report on information security risks<br>• Articulate information security needs of the organisation into security measures<br>• Provide information security designs and solutions and the implementation of security-by-design and privacy-by-design in information systems<br>• Present information security solutions to colleagues and superiors<br>• Monitor and perform information security assessments, tests, reviews and audits<br>• Present improvement proposals concerning information security and risks to management | |
| **e-Competences (from e-CF)** | E.3. Risk Management | Level 2 |
| | E.8. Information Security Management | Level 3 |
| **General competences** | G.2. Project management | Level 2 |
| | G.3. Communication and persuasion | Level 2 |
| | G.4. Research | Level 2 |
| | G.5. Organisational sensitivity | Level 2 |
| | G.7. Analytical skills | Level 3 |
| | G.8. Integrity | Level 2 |
| **Education and experience** | • A completed relevant Bachelor study[20] or equivalent level of knowledge and skills<br>• Two years' work experience in a relevant position. | |
| **KPI** | Information security risks are identified and measures are in place. | |

[20] A Bachelor study in economic, exact, technical or human sciences domain.

# ICT Security Manager

| Profile title | ICT SECURITY MANAGER | | |
|---|---|---|---|
| **Summary statement** | Defines the organisation's ICT security policies in line with the organisation's information security strategy and architecture and organises and manages the organisation's ICT security. | | |
| **Mission** | Defines the ICT security policies anticipating the ICT security threat landscape, trends, the organisation's ICT and future needs. Sets up the ICT security organisation and determines and assigns necessary resources. Manages ICT security deployment across all ICT systems. Ensures an appropriate level of ICT security based on the organisation's needs and risk appetite. | | |
| **Deliverables** | **Accountable** | **Responsible** | **Contributor** |
| | • ICT security policies and its implementation<br>• ICT security organisation and expertise<br>• ICT security projects<br>• ICT security assessments, tests, reviews and audits | • ICT security project portfolio<br>• ICT security procedures<br>• Risk analyses for ICT<br>• Monitoring and reporting on ICT risks<br>• ICT continuity plan and testing<br>• ICT security training policy | • Risk management policy<br>• Information security strategy<br>• Information security architecture<br>• Service Level Agreements<br>• Information security implementation<br>• New technology<br>• integration proposals |
| **Main tasks** | • Define the organisation's ICT security policies in line with the organisation's information security strategy and architecture<br>• Organise ICT security and the necessary expertise<br>• Manage the implementation of the organisation's ICT security policies<br>• Provide an ICT security project portfolio<br>• Define ICT security training policy<br>• Define and implement procedures linked to ICT security<br>• Perform risk analyses for ICT<br>• Monitor and report on ICT risks<br>• Establish the ICT continuity plan and ensure regular testing<br>• Initiate and supervise ICT security projects<br>• Ensure the quality of ICT security assessments, tests, reviews and audits<br>• Watch technology trends with respect to ICT security<br>• Inform (C)ISO and senior general management about ICT security status and incidents and present improvement proposals | | |
| **e-Competences (from e-CF)** | A.7. Technology Trend Monitoring | | Level 2 |
| | E.3. Risk Management | | Level 2 |
| | E.8. Information Security Management | | Level 3 |

| | | |
|---|---|---|
| **General competences** | G.2. Project management | Level 3 |
| | G.3. Communication and persuasion | Level 3 |
| | G.6. Management | Level 3 |
| | G.7. Analytical skills | Level 2 |
| | G.8. Integrity | Level 3 |
| **Education and experience** | • A completed relevant Bachelor study[21] or equivalent level of knowledge and skills<br>• Three years' work experience in an ICT security position<br>• Three years' work experience in a management position | |
| **KPI** | An appropriate level of ICT security based on organisation's needs and risk appetite. | |

[21] A Bachelor study in exact or technical domain.

# ICT Security Specialist 3

| Profile title | ICT SECURITY SPECIALIST 3 | | |
|---|---|---|---|
| **Summary statement** | 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<br>• New technology integration proposals<br>• Technical ICT security solutions, measures and updates<br>• Selection and implementation of security tools<br>• ICT security assessments, tests, reviews and audits<br>• Monitoring and securing the technical security measures for ICT<br>• Testing the ICT incident/response and/or continuity plan | • Risk Management strategy<br>• ICT security policies and its implementation<br>• Risk analyses for ICT<br>• Forensic investigation<br>• ICT incident/response and/or continuity plan<br>• Knowledge exchange on ICT security |
| **Main tasks** | • Watch in-depth technology trends with respect to ICT security<br>• Observe current threats and threat trends and determine their possible impact on the organisation<br>• Provide knowledge base on information security<br>• Draw up improvement proposals for ICT security<br>• Draw up proposals for integration of new information technology<br>• Design technical ICT security solutions<br>• Present ICT security solutions to colleagues and management<br>• Realize technical security measures and security updates in systems and networks<br>• Select and implement security tools<br>• Ensure and monitor ICT security assessments, tests, reviews and audits<br>• Contribute to forensic investigation<br>• Monitor and secure technological security measures for ICT and evaluate ICT security risks<br>• Test the ICT incident/response and/or continuity plan<br>• Supervise less experienced colleagues in ICT security<br>• Present improvement proposals concerning ICT security and risks to line management | | |

| | | |
|---|---|---|
| **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 |
| **Education and 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. | |

# ICT Security Specialist 2

| Profile title | ICT SECURITY SPECIALIST 2 | | |
|---|---|---|---|
| **Summary statement** | 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 networks and systems or parts of those. | | |
| **Deliverables** | **Accountable** | **Responsible** | **Contributor** |
| | • Knowledge base on ICT security | • ICT security improvement proposals<br>• Technical ICT security solutions, measures and updates<br>• Selection and implementation of security tools<br>• ICT security assessments, tests and reviews<br>• Monitoring and securing the technical security measures for ICT | • ICT security policies and its implementation<br>• Risk analyses for ICT<br>• Forensic investigation<br>• ICT incident/response and/or continuity plan<br>• Knowledge exchange on ICT security |
| **Main tasks** | • Watch technology trends with respect to ICT security<br>• Monitor current threats and threat trends and determine their possible impact on the organisation<br>• Provide knowledge base on ICT security<br>• Draw up improvement proposals for ICT security<br>• Design technical ICT security solutions<br>• Present ICT security solutions to colleagues and managers<br>• Realize technical security measures and security updates in systems and networks<br>• Select and implement security tools<br>• Ensure and monitor ICT security assessments, tests and reviews<br>• Contribute to forensic investigation<br>• Monitor and secure the technical security measures for ICT and evaluate ICT security risks<br>• Test elements of the ICT incident/response and/or continuity plan<br>• Present improvement proposals concerning ICT security and risks to line management | | |

| | | |
|---|---|---|
| **e-Competences (from e-CF)** | A.7. Technology trend monitoring | Level 3 |
| | B.4. Solution deployment | Level 3 |
| | E.8. Information security management | Level 2 |
| **General competences** | G.3. Communication and persuasion | Level 2 |
| | G.4. Research | Level 3 |
| | G.7. Analytical skills | Level 3 |
| | G.8. Integrity | Level 2 |
| **Education and experience** | A completed higher professional study in the ICT domain or equivalent level of knowledge and skills. | |
| **KPI** | Necessary ICT security measures in place and effective. | |

# ICT Security Specialist 1

| **Profile title** | **ICT SECURITY SPECIALIST 1** | | |
|---|---|---|---|
| **Summary statement** | Implements technical security measures for ICT and monitors the organisation's ICT security. | | |
| **Mission** | Implements the necessary security measures in ICT. Supports and informs to ensure secure ICT operation. Takes direct action to secure networks and systems or parts of those. | | |
| **Deliverables** | **Accountable** | **Responsible** | **Contributor** |
| | | • Technical ICT security measures and updates<br>• Selection and implementation of security tools<br>• Monitoring of technical security measures for ICT | • ICT security policies and its implementation<br>• Risk analyses for ICT |
| **Main tasks** | • Watch major technology trends with respect to ICT security<br>• Implement technical ICT security measures and security updates in systems and networks<br>• Select and implement security tools<br>• Monitor technical security measures for ICT and evaluate ICT security risks<br>• Report on operation of ICT security measures | | |
| **e-Competences (from e-CF)** | A.7. Technology trend monitoring | | Level 2 |
| | B.4. Solution deployment | | Level 2 |
| | E.8. Information security management | | Level 2 |
| **General competences** | G.3. Communication and persuasion | | Level 1 |
| | G.4. Research | | Level 2 |
| | G.8. Integrity | | Level 2 |
| **Education and experience** | A completed secondary vocational study in the ICT domain or equivalent level of knowledge and skills. | | |
| **KPI** | Common ICT security measures in place. | | |

# How to use the job profiles

## Job profiles and job descriptions

Within the domain of information security, a whole variety of job designations are currently in use. A person who at strategic level is responsible for information risk management can for example have the job title Chief Information Security Officer, but equally Information Risk Manager or Information Security Manager. In each of these positions, the person in question undertakes similar tasks and requires similar competences, namely the tasks and competences laid out in the generic job profile *Chief Information Security Officer*. This job profile should be seen as a typical job description, formulated in terms recognisable within the professional field.

The generic job profile is *not meant* to be used directly as a job description but it *could* be included in a job description. On the other hand, it is also possible to assemble a particular function from a series of job profiles, or from just one part of a single job profile. However, even if an organisation does opt to fully take up a single profile, for example *Chief Information Security Officer*, into a single position, it may decide to use another name for that function, for example Information Security Manager (different flag, same content). An organisation can also opt to appoint a Chief Information Security Officer on the basis of the job profile Information Security Officer.

In practice, every organisation will compile a specific information security function on the basis of one or more (parts of) job profiles, and decide on their own job designation. Subsequently, the organisation will also wish to give its own twist to the way in which the position in question is occupied. This is not random practice but above all useful. The organisation may for example wish to lay down in the job description specific knowledge of the organisation and the sector. In addition, each organisation has specific characteristics that require the adaptation of the tasks that make up the job. There are also a series of ‘lesser’ issues that may or may not be specific to the organisation (for example tasks or competences) that have to be specified in the job description but are ‘too unimportant’ to be included in the job profile. By this practice a job description will normally differ from the generic job profiles. As long as the differences do not become too great (80/20 rule), the job profiles continue to provide a sound indication of the information security functions, and the requirements imposed on them.

## Simple and complex organisations

In the first instance, the described job profiles were drawn up for medium-sized information processing organisations, in which information security plays a prominent role. Think of ministries, agencies, medium-sized banks and medium-sized industrial organisations for whom information provision is of key importance.

Organisations that are less complex in terms of information security generally speaking impose less strict demands on their information security functions. Examples include small municipalities or companies with a relatively restricted information flow. In their job descriptions for the information security positions, for a number of competences they may specify lower levels than outlined in the underlying job profiles, or may even opt to scrap certain competences.

On the other hand, organisations that are more complex in terms of information security will generally speaking impose stricter requirements on their information security functions. This for example applies to large international banks and large multinationals that are heavily dependent on their information flows. In their job description for the information security functions, they may specify higher levels for certain competences than outlined in the underlying job profile and/or demand extra competences.

## Education and examination

In the described job profiles, competences are listed that a practitioner of the profession in question should master. A practitioner must be able to acquire those competences. In principle there are two possibilities for acquiring competences, namely education or learning in practice. A combination of the two is also possible.

Education and learning in practice both have advantages and disadvantages. Education in the form of a study programme ensures mastery of the intended competences more quickly, but the learning effect is often limited to just those competences. Learning in practice often requires more time before the intended competences are acquired, but on the other hand, other competences are also acquired that may not be immediately necessary but that do provide the person in question with a broader basis and as a consequence greater flexibility in understanding and practical performance. Because of the varying advantages and disadvantages, it is preferable to keep both options open.

Suitable education can be provided for training upcoming information security professionals by education institutions. They can elaborate new study programmes and courses on the basis of the competences described in the job profiles. The competences are then used as attainment targets for the new study programmes and courses. The competences can also be used, in respect of already existing study programmes and courses, to determine whether those programmes actually develop the required competences. Examinations can also be based on the specified competences.

Generally speaking, initial study programmes (university/ higher professional education/ secondary vocational education) do not fit on all job profiles. For example, ' highly demanding' job profiles (*Chief Information Security Officer* and *ICT Security Manager*) impose higher demands than initial study programmes can deliver. On the other hand, such study programmes can be suitable for establishing a solid foundation, on top of which graduates can acquire the necessary additional competences for one of the 'highly demanding' job profiles, by acquiring work experience and following additional courses.

Little action need be taken to provide for learning in practice. In principle, the huge variety of businesses and bodies offer sufficient opportunities for acquiring the necessary competences in practice. On the other hand, a mechanism must be put in place according to which the acquired competences can be examined, so that people can qualify for specific job profiles. Examination can be based on the competences specified in the job profiles. With that in mind, an examination process will have to be established with uniform examination criteria, and taken up by one or more examining bodies.

In principle, a variety of combinations of education and learning in practice are possible. In certain cases, the two options are interchangeable. For example, an individual with several years of work experience may be exempted from part of a study programme. In other cases, the two possibilities will complement one another. Take for example the acquisition of additional competences referred to above, for one of the 'more demanding' job profiles by acquiring work experience and following additional courses, having completed an initial study programme.

# Continued learning and professional improvement

A professional who has qualified for one of the job profiles outlined in this document will (have to) acquire additional knowledge and skills over the course of time. Every professional is after all required to maintain his professional expertise at a suitable level (lifelong learning) by acquiring knowledge and skills necessary for anticipating the relevant social and technical developments. As a result, the professional is permanently able to successfully exercise his profession, in a changing world.

As well as maintaining a level of professional expertise, a professional may opt to acquire additional knowledge and skills in a particular subdomain, with a view to specialising in that subdomain. Based on this additional expertise, the professional will acquire a specialisation over and above the standard professional qualification. In this way, an ICT Security Specialist 2 can for example acquire further specialist expertise in ethical hacking. In that case, the professional is able to undertake tasks that cannot be carried out by an average practitioner of the same job. Such specialisations are not part of the generic job profiles, but may nonetheless be a requirement in particular job descriptions.

An exception is an individual who initially qualifies for one of the standard job profiles, and subsequently acquires all the necessary knowledge and skills for another standard job profile. In that case, it is possible for that individual to become qualified for the latter standard job profile. Obvious professional improvement pathways are those from ISO to CISO, and from ICT Security Specialist 1 to ICT Security Specialist 2, and from ICT Security Specialist 2 to ICT Security Specialist 3.

# Annex A: Legend for job profile table

| Term | Description [22] |
|---|---|
| Profile title | Gives a commonly used name to a profile. |
| Summary statement | Indicates the main purpose of the profile. The purpose is to present to stakeholders and users a brief, concise understanding of the specified profile. It should be understandable by professionals, managers and Human Resource Personnel. |
| Mission | Describes the rationale of the profile. The purpose is to specify the designated job defined in the profile. |
| Deliverables | Specifies the profile by key deliverables. Also adds the dimension of responsibility following the RACI model. Mention the level of responsibility – A: accountable, R: responsible, C: contributor – to be carried out by the profile. |
| Main tasks | Provides a list of typical tasks to be performed by the profile. A task is an action taken to achieve a result. |
| e-Competences | Provides a list of necessary e-competences (from the e-CF) to carry out the mission. Assignment level is important. |
| General competences | Provides a list of necessary general competences to carry out the mission. Assignment level is important. |
| Education and experience | Specifies the minimum required prior education and experience. |
| KPI | Indicates the main performance indicator (KPI – Key Performance Indicator). |

[22] Based on *CEN Workshop Agreement CWA 16458:2012 E, European ICT Professional Profiles*; ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf.

# Annex B: Competence levels

The job profiles for information security specify competences, or knowledge and skills, for the information security professionals. Each competence is given an indication of the level at which that competence must be mastered. In line with e-CF, a competence level can have a value between 1 (low) and 5 (high).[23] The competence levels are explained below.

**Competence levels in respect of knowledge**

A competence level in respect of the knowledge of a specific knowledge domain is measured according to two aspects, namely the *completeness* of the knowledge of the domain and the *level of mastery* of that knowledge. The level of mastery is based on the taxonomy of Bloom (see the explanation at the end of the annex).

| Competence level knowledge * | | Completeness of the knowledge domain | | |
|---|---|---|---|---|
| | | Only some key elements | All key elements | Very extensive |
| Level of mastery of the knowledge | Analyse, evaluate and innovate | | **4** | **5** |
| | Select and apply | | **3** | |
| | Reproduce and explain | **1** | **2** | |

* A score in an empty cell is rounded off to the next value below or to the left.

As a rule, we state that knowledge of a specific domain is in particular meaningful if the professional is familiar with all key elements from that domain.
So, in determining a knowledge level, we will in the first instance assume knowledge of *all key elements* of the given knowledge domain. The level then indicates how well the professional is able to handle that knowledge. The scale ranges from level 2 – the ability to reproduce and explain all key elements – to level 4 – the ability to analyse, evaluate and innovate all key elements.
If a professional does not yet master the 'reproduce and explain' level for all key elements, that professional is at level 1, the minimum level.
If a professional has more knowledge than required to 'analyse, evaluate and innovate all key elements', the professional is at level 5, the maximum level.

For example: A professional who is not only able to reproduce, explain, select and apply but also analyse, evaluate and innovate all the key elements of a given knowledge domain (for example "best practices in and standards for information security management"), masters this knowledge at level 4.

[23] The competence levels in e-CF are in fact accountability levels and not competence levels. For that reason, the description of the levels has been adjusted so that they are effectively competence levels.

**Competence levels in respect of skills**

A competence level in respect of the skill with which a professional is able to execute a specific activity is measured according to two aspects, namely the *complexity* of the activity and the degree of *independence* with which the professional is able to carry out this activity.

| Competence level skills * | | Complexity of the activity | | |
|---|---|---|---|---|
| | | Structured and predictable | **Un**structured **or un**predictable | **Un**structured **and un**predictable |
| Independence of execution | Provides supervision | | | **5** |
| | Independent | **2** | **3** | **4** |
| | Under supervision | **1** | | |

* A score in an empty cell is rounded off to the next value below or to the left.

As a rule we state that the skill to carry out a specific activity is in particular meaningful if that activity can be independently undertaken by the professional.
So, in determining a skill levels, we will assume the ability to *independently* carry out the given activity. The scale ranges from level 2 – the ability to independently carry out the activity in a structured and predictable environment – to level 4 – the ability to carry out the activity in an **un**structured **and un**predictable environment.
If a professional cannot yet independently execute the activity in a structured and predictable environment, that professional is at level 1, the minimum level.
If a professional is able to even supervise others in an **un**structured and **un**predictable environment, in carrying out the activity, that professional has reached level 5, the maximum level.

For example: A professional who is able to independently carry out the activity 'performing security audits' in an unstructured and unpredictable environment (for example a medium-sized to large organisation) masters this skill at level 4.

**Level of mastery of knowledge, and the taxonomy of Bloom**

The *level of mastery* of knowledge is based on the taxonomy of Bloom.[24] This taxonomy has been reduced to three levels, as outlined in the table below.

[24] B.S. Bloom, J.T. Hastings, G.F. Madaus. *Handbook on formative and summative evaluation of student learning*. McGraw Hill, New York, 1971.

| Taxonomy of Bloom | Level of mastery of knowledge |
|---|---|
| Creating | Analyse, evaluate and innovate |
| Evaluating | |
| Analyzing | |
| Applying | Select and apply |
| Understanding | Reproduce and explain |
| Remembering | |

# Annex C: Glossary

| Term | Definition / description |
|---|---|
| Accountable | To be Accountable is to be the only “owner” of the work. The owner must sign off or approve when the task, objective or decision is complete. He/she must make sure that responsibilities are assigned for all related activities. There is only one owner accountable for each deliverable. [CWA 16458] |
| Competence (level) | Competence is a demonstrated ability to apply knowledge, skills and attitude for achieving observable results. A competence can have a level from 1 to 5. [CWA16234-1] |
| Contributor | Contributors provide input before work can be completed and signed-off on. They are “in the loop” and active participants. Several people can be contributors to one deliverable. [CWA 16458] |
| e-competence (level) | A competence in the ICT domain. An e-competence can have a level from 1 to 5. |
| Deliverables | A predefined result of a task in a working context. [CWA 16458] |
| Education profile | A formal description of a curriculum. The curriculum brings together the knowledge, skills and attitude needed for the related job profile. |
| Experience | Practical contact with and observation of facts or events. [Oxford Dictionaries] |
| General competence | A competence not specific for the ICT domain. A general competence can have a level from 1 to 5. |
| Information risk management | Coordinated activities to direct and control an organisation with regard to risks related to the organisation’s information. [ISO Guide 73] |
| ICT security | Preservation of confidentiality, integrity and availability of ICT. [based on definition of information security] |
| Information security | Preservation of confidentiality, integrity and availability of information. [ISO 27000] |
| Job profile | A formal description of a job. It describes the mission, tasks and responsibilities of a practitioner in the job and specifies the competences the practitioner must have. |
| Knowledge | The "set of know-what" (e.g. programming languages, design tools...). [CWA 16458] |
| Qualification | A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards. [European Qualifications Framework, Key Terms] |
| Responsible | The “Doers” of the work are responsible for the work. They must fulfil the task or objective or make the decision. Several people can be jointly responsible for one deliverable. [CWA 16458] |
| Skill | The ability to carry out managerial or technical tasks. [CWA 16458] |
| Task | An action taken to achieve a result. A task may be associated with deadlines, resources, goals, specifications and/or the expected results. [CWA 16458] |

# About PvIB

With more than 1400 members, PvIB, the Dutch Association of Information Security Professionals, is the platform in the Netherlands where information, knowledge and experience about information security are collated, improved, enriched and redistributed. PvIB brings together all stakeholders and interested parties in the field of information security. PvIB delivers a contribution to issues with a clear social relevance. PvIB promotes the networking of individual professionals in the field of information security.

The target group for PvIB consists of anyone involved in information security through their study or profession, and people who demonstrate a particular interest in the subject. The members of PvIB are employed by businesses, government bodies and educational institutions, large and small. The products and services of PvIB are intended for the professionals and are not commercial.

PvIB is striving to establish a clear profile for the field of information security and to support the development of the profession of information security, for example by promoting the development of an approved qualification structure. PvIB emphasize recognition at European level.