Beroepsprofielen Informatiebeveiliging 2.0

Een basis voor uniforme kwalificatie van informatiebeveiligers

Afbeelding van suphakit73 / FreeDigitalPhotos.net

Opdrachtgever:	Platform voor Informatiebeveiliging (PvIB) en programma Qualification of Information Security (QIS)
Auteurs:	Marcel Spruit en Fred van Noord
Versie:	2.0a Nederlands
Publicatiedatum:	1 januari 2017
Uitgever:	PvIB, © 2017 (www.pivb.nl) ISBN: 978-90-78786-03-0

Inhoudsopgave

Inleiding

Aanleiding

In de huidige informatiemaatschappij wordt het steeds belangrijker dat iedere organisatie zorgvuldig omgaat met informatie. Organisaties moeten steeds meer informatie beschermen tegen een steeds complexer dreigingenbeeld. Hiervoor zijn goed opgeleide en ervaren informatiebeveiligers nodig. Kwalificaties zijn een middel om de kennis en ervaring van informatiebeveiligers inzichtelijk te maken.

In de afgelopen jaren is op het gebied van kwalificatie van informatiebeveiligers een chaotische situatie ontstaan met een groot aantal onderling moeilijk vergelijkbare certificaten en titels.[1] Daardoor kunnen informatiebeveiligers met hun titels en de bijbehorende certificaten niet duidelijk maken welke kennis en ervaring zij hebben. Werkgevers kunnen niet zien wanneer zij een goed opgeleide en ervaren informatiebeveiliger voor zich hebben. En opleidingsinstellingen denken nog een keer extra na alvorens te investeren in nieuwe opleidingen op het gebied van informatiebeveiliging.

De beroepsvereniging Platform voor Informatiebeveiliging (PvIB), streeft naar het professionaliseren van de beroepsgroep van informatiebeveiligers en daarbij hoort een overzichtelijke en transparante situatie op het gebied van kwalificatie.[2] Een uniform kwalificatiestelsel voor informatiebeveiligers voorziet daarin.

Om informatiebeveiligers uniform te kunnen kwalificeren, moet eerst duidelijk zijn welke beroepen binnen het vakgebied informatiebeveiliging voorkomen, wat deze beroepen inhouden en welke competenties (kennis en vaardigheden) daarvoor nodig zijn. Dit wordt beschreven in zogenaamde beroepsprofielen.

Doelstelling

Dit document beschrijft beroepsprofielen voor het vakgebied informatiebeveiliging.

Afbakening

Informatiebeveiliging is een onderwerp waar iedereen in elke organisatie in meer of mindere mate mee te maken heeft. Voor de meeste mensen in een organisatie is informatiebeveiliging één van de aspecten van het dagelijkse werk, waaraan voldoende aandacht besteed moet worden, maar het speelt geen hoofdrol. Zo verwachten we van bijvoorbeeld een Systeemarchitect dat in de systeemarchitectuur voldoende aandacht is besteed aan beveiliging. En van een Systeemontwikkelaar (Software Engineer) verwachten we veilige code. De meeste mensen doen 'iets' met informatiebeveiliging. Maar daarmee zijn zij nog geen 'informatiebeveiligers'.

---

[1] *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers*, Rapport VKA/HEC/CPNI, versie 1.0, 2011.

[2] Een kwalificatie is een formeel resultaat van een beoordelings- en validatieproces, dat wordt verworven wanneer een bevoegde instantie bepaalt dat de leerresultaten die een individu heeft bereikt, aan gegeven normen voldoen (Bron: European Qualifications Framework, Key Terms). Het beoordelings- en validatieproces is in het algemeen gebaseerd op toetsing door middel van een examen of het beoordelen van een portfolio.

Voor een aantal mensen is informatiebeveiliging echter ‘core business’. Deze mensen, de 'echte' informatiebeveiligers, hebben een organiserende, specificerende, uitvoerende, ondersteunende, adviserende en/of controlerende rol op het gebied van informatiebeveiliging. Bij hen is informatiebeveiliging het belangrijkste aandachtspunt, of ten minste één van de belangrijkste aandachtspunten.

De informatiebeveiligers werken samen met andere mensen in andere functies waarin informatiebeveiliging een minder prominente plaats inneemt. Verscheidene van hen zijn cruciaal voor het functioneren van de informatiebeveiligers, bijvoorbeeld omdat ze leiding of sturing geven, of onontbeerlijke input of ondersteuning geven. Hieronder vallen bijvoorbeeld de Chief Executive Officer, de Chief Information Officer en de Enterprise Architect. Maar hoewel zij onmisbaar zijn voor goede informatiebeveiliging in een organisatie, zijn ze geen informatiebeveiligers.

De in dit document beschreven beroepsprofielen hebben betrekking op de informatiebeveiligers, dus degenen waarvoor informatiebeveiliging ‘core business’ is.

Uitgangspunten

Voor het beschrijven van beroepsprofielen voor beroepen binnen het vakgebied informatiebeveiliging worden de volgende uitgangspunten gehanteerd:

- De beroepsprofielen worden opgesteld voor 'echte' informatiebeveiligingsberoepen waarin zoveel informatiebeveiligers omgaan dat het zinvol is om gestandaardiseerde profielen te hebben.
- De beroepsprofielen specificeren de benodigde kennis, vaardigheden en ervaring.
- De beroepsprofielen zijn gebaseerd op het Europees e-Competence Framework 3.0 (e-CF).[3]
- De beroepsprofielen worden breed gedragen binnen het vakgebied informatiebeveiliging.
- De beroepsprofielen zijn geschikt als basis voor een uniform kwalificatiestelsel voor informatiebeveiligers.

Verantwoording

Dit document is op verzoek van het bestuur van PvIB opgesteld door de Werkgroep Kwalificatie van informatiebeveiligers van PvIB. De beroepsprofielen in dit document zijn bedoeld om gebruikt te worden voor een uniform kwalificatiestelsel voor professionals in de informatiebeveiliging.

Een randvoorwaarde voor beroepsprofielen is brede acceptatie van de profielen door enerzijds de betrokken beroepsgroep en anderzijds de werkgevers en opleidingsinstellingen die de profielen kunnen gebruiken voor respectievelijk de werving en selectie van professionals en het inrichten van opleidingen. Om brede acceptatie te ondersteunen is dit document gereviewd door een representatie van de PvIB, de stuurgroep en klankbordgroep van het programma Qualification of Information Security, functionarissen die werkzaam zijn in functies waar de hier beschreven profielen betrekking op hebben, alsmede opleiders op het gebied van informatiebeveiliging.

---

[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.

Vakgebied

Het vakgebied informatiebeveiliging is breed. Uit vooronderzoek is gebleken dat het wenselijk is om binnen het vakgebied informatiebeveiliging onderscheid te maken tussen de domeinen *informatierisicomanagement* en *ICT-beveiliging*:[4]

- *Informatierisicomanagement* is het sturen en beheersen van een organisatie met betrekking tot risico's op het gebied van de informatievoorziening.[5,6] Het richt zich op het beveiligen van de informatievoorziening als geheel.
- *ICT-beveiliging* omvat het ontwerpen, implementeren, onderhouden en evalueren van beveiligingsmaatregelen met betrekking tot de ICT (hardware en software). In dit domein speelt specialistische kennis van ICT een belangrijke rol.

Naast deze twee domeinen zijn binnen het vakgebied informatiebeveiliging een aantal andere domeinen die met eigen uniforme kwalificatie werken, namelijk IT-audit,[7] forensisch onderzoek[8] en business continuity management.[9] Voor deze domeinen zijn al beroepsprofielen opgesteld. Deze vallen buiten de scope van dit document.

Daarnaast zijn er kleinschalige specialistische domeinen, zoals cryptologie, die slechts door een relatief klein aantal professionals worden beoefend en waarvoor het niet zinvol is om te investeren in uniforme kwalificatie en beroepsprofielen. Ook deze domeinen vallen buiten de scope van dit document.

Voor de domeinen *informatierisicomanagement* en *ICT-beveiliging* zijn in dit document beroepsprofielen beschreven, ten behoeve van uniforme kwalificatie. De profielen kunnen zowel in Nederland, alsook daarbuiten worden toegepast.

---

[4] *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers*, Rapport VKA/HEC/CPNI, versie 1.0, 2011.

[5] Gebaseerd op: *ISO Guide 73:2009, Risk management – Vocabulary*, ISO, 2009.

[6] De informatievoorziening omvat het aanmaken, opslaan, verwerken, bekijken, transporteren en vernietigen van gesproken, geschreven, gedrukte, digitale en andere gegevens. De reikwijdte van de informatievoorziening gaat daarmee verder dan die van de ICT.

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

[8] *Digitaal Forensisch Onderzoeker - Beroepscompetentieprofiel*, ECABO, 2010.

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

Beroepsprofielen

Om professionals in informatiebeveiliging te kunnen kwalificeren, dient eerst te worden vastgesteld welke beroepen binnen het vakgebied informatiebeveiliging worden onderscheiden en wat deze beroepen inhouden. De beroepen worden beschreven door middel van beroepsprofielen.

Een beroepsprofiel geeft een formele beschrijving van een beroep. Het beschrijft de missie, taken en verantwoordelijkheden van een beoefenaar van het betreffende beroep en specificeert de competenties (kennis en vaardigheden) die de beoefenaar dient te bezitten.

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen de domeinen *information risk management* en *ICT-beveiliging*. De eerste richt zich op het beveiligen van de informatievoorziening als geheel en de tweede op het beveiligen van de daarbij gebruikte ICT.

Binnen het domein *information risk management* onderscheiden we een beoefenaar op strategisch en/of tactisch niveau, een *Chief Information Security Officer*, en een beoefenaar op tactisch en/of operationeel niveau, een *Information Security Officer*.

Binnen het domein *ICT-beveiliging* onderscheiden we een beoefenaar op tactisch niveau, een *ICT Security Manager*, en een beoefenaar op operationeel niveau, een *ICT-beveiligingsspecialist*[10].

Daarmee onderscheiden we binnen het vakgebied informatiebeveiliging vier beroepen waarvoor beroepsprofielen moeten worden beschreven:

- Chief Information Security Officer (CISO).[11]
- Information Security Officer (ISO).[12]
- ICT-beveiligingsmanager.
- ICT-beveiligingsspecialist.

[10] De term 'specialist' kan misleidend zijn. In het dagelijks taalgebruik wordt met specialist veelal een zeer deskundige professional bedoeld. Deze betekenis wordt hier niet bedoeld. Hier wordt met specialist bedoeld dat degene geen generalist is. De hier bedoelde specialist heeft zich ontwikkeld met een sterke focus op ICT-beveiligingstechniek. Iemand kan een zeer deskundige professional (ofwel een 'specialist' in het degalijks taalgebruik) worden door na een kwalificatie voor ICT-beveiligingsspecialist (bijvoorbeeld op basis van een specifieke ICT-beveiligingsopleiding) jarenlang extra kennis en vaardigheden op te bouwen. In de hier gegeven beschrijving is er geen aparte kwalificatie voor een dergelijke zeer deskundige specialist.

[11] Ook wel aangeduid als *Corporate Information Security Officer* (CISO), of *Chief/Corporate Information Risk Officer* (CIRO).

[12] Ook wel aangeduid als *Information Risk Officer* (IRO).

	Veiligheid van de I-functie (Information risk management)	**Veiligheid van de ICT-functie** (ICT-beveiliging)
Strategisch en/of tactisch	CISO	ICT-beveiligingsmanager
Tactisch en/of operationeel	ISO	ICT-beveiligingsspecialist *

* Het beroep ICT-beveiligingsspecialist kent drie niveaus, genummerd van 1 (mbo-niveau) tot 3 (universitair niveau).

Voor ieder van deze beroepen wordt hierna een beroepsprofiel gegeven. De profielen zijn bedoeld voor gebruik binnen Nederland alsook buiten Nederland. Daarom wordt ook een Engelstalige versie van dit document gepubliceerd.

In een eerdere publicatie van PvIB zijn ook de beroepen *Information Security Architect* (ISA) en de *Business Information Security Architect* (BISA) benoemd.[13] Deze worden niet meer als aparte informatiebeveiligingsberoepen meegenomen, omdat de architectuurfunctie, ook voor de informatiebeveiliging, wordt gezien als verantwoordelijkheid van de *Enterprise Architect* en de *Systems Architect*. In uitzonderlijke informatiebeveiligingssituaties kan in aanvulling hierop een *(Business) Information Security Architect* nodig zijn, maar dat rechtvaardigt geen apart profiel.

Voor het beschrijven van de beroepsprofielen is gebruik gemaakt van het document CWA 16458.[14] Hierin zijn beroepsprofielen geformuleerd voor beroepen in de ICT-sector. De beroepen *ICT Security Manager* (ICT-beveiligingsmanager) en *ICT Security Specialist* (ICT-beveiligingsspecialist) maken hier deel van uit (profielen 11 en 12). In eerste instantie zijn de beroepsprofielen voor *ICT Security Manager* en *ICT Security Specialist* overgenomen uit CWA 16458 en vertaald. De *Werkgroep Kwalificatie van informatiebeveiligers* van *PvIB* constateerde echter dat de inhoud van deze profielen niet goed overeenkwam met wat de werkgroep verwachtte. Zo waren de genoemde e-competenties niet hetzelfde als de beroepsgroep verwachtte en waren de noodzakelijke algemene competenties, vooropleiding en ervaring niet gespecificeerd. Ook op andere plaatsen in de profielen bleken significante aanpassingen nodig te zijn. De werkgroep heeft de beide profielen grondig laten reviewen en waar nodig aangepast. Na publicatie en brede verspreiding van versie 1 van dit document zijn aanvullende opmerkingen binnengekomen die tot verdere aanpassing van de profielen hebben geleid. Bovendien blijken werkgevers en opleiders onderscheid te maken tussen drie verschillende niveaus van ICT-beveiligingsspecialist (ICT Security Specialist). De werkgroep heeft dan ook bij de ICT-beveiligingsspecialist twee niveaus toegevoegd[15] en de profielen nogmaals grondig laten reviewen en waar nodig aangepast. In dit document zijn de nieuwe profielen gegeven.

De beroepsprofielen voor CISO en ISO zijn niet in CWA 16458 gespecificeerd. Dit is niet geheel tegen de verwachting, want CISO en ISO zijn geen ICT-functies en vallen daarmee buiten de scope van CWA 16458.[16] In het voorliggende document zijn ook de nieuwe beroepsprofielen voor CISO en ISO opgenomen. Deze profielen zijn analoog aan de andere profielen opgesteld en zijn door dezelfde review- en updateslagen gegaan.

---

[13] B. Bokhorst et al., *Functies in de informatiebeveiliging*, 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] De in CWA 16458 beschreven ICT Security Specialist komt ongeveer overeen met de middelste van de nieuwe profielen voor ICT-beveiligingsspecialist (ICT Security Specialist), te weten ICT-beveiligingsspecialist 2.

[16] Hoewel in CWA 16458 wel andere niet-ICT-functies zijn beschreven, zoals Chief Information Officer, Enterprise Architect, Quality Assurance Manager en Project Manager.

Vanuit ieder van de beschreven beroepen is verdere doorgroei en specialisatie mogelijk. Zo kan een ISO extra kennis en vaardigheden verwerven om zich te specialiseren in bijvoorbeeld waterschaps-processen, of kan een ICT-beveiligingsspecialist 2 zich verder specialiseren in bijvoorbeeld ethisch hacken. De beroepsprofielen hebben betrekking op de 'standaard' beroepen. De verdere doorgroei en specialisatie is zodanig divers dat daar geen beroepsprofielen voor zijn uitgewerkt.

Daarentegen is het ook mogelijk om verder door te groeien naar een ander 'standaard' beroep. Voor de hand liggende doorgroeipaden zijn die van ISO naar CISO en die van ICT-beveiligingsspecialist 1 naar ICT-beveiligingsspecialist 2 en van ICT-beveiligingsspecialist 2 naar ICT-beveiligingsspecialist 3.

In de beroepsprofielen zijn competenties (e-competenties en algemene competenties) genoemd, alsmede bij iedere competentie een competentieniveau.

Wat betreft de competenties kan ervoor worden gekozen om elke competentie die geheel of gedeeltelijk enigszins nuttig is in een bepaald beroepsprofiel in de competentielijst van het profiel op te nemen. Omdat elke competentie bestaat uit verscheidene competentie-elementen (kennis of vaardigheid), ontstaat zo een onafzienbare lijst competentie-elementen. Aan de andere kant kan er ook voor worden gekozen om alleen de belangrijke competenties op te nemen, de 'kern'competenties. In dat geval ontstaat ook een aanzienlijke lijst met competentie-elementen, maar die blijft nog te overzien. Om het aantal competentie-elementen per beroepsprofiel behapbaar te houden is voor de tweede benadering gekozen, dus het opnemen van alleen de 'kern'competenties in de beroepsprofielen. Dit betekent per beroepsprofiel omstreeks 8 competenties, ofwel ruim 100 competentie-elementen. Bij het kwalificeren voor een beroepsprofiel worden alle in het profiel beschreven (kern)competenties volledig getoetst. Impliciet gaan we er vanuit dat de competentie-elementen die wel nuttig zijn, maar die geen deel uitmaken van een kerncompetentie, in het onderwijs of bij training on-the-job meeliften met de beschreven kerncompetenties. Het is namelijk zeer waarschijnlijk dat de kerncompetenties, noch in het onderwijs, noch on-the-job, geïsoleerd aangeleerd zullen worden.
De e-competenties en algemene competenties zijn uitgewerkt in een separaat document "Competenties voor informatiebeveiligers".

Een competentieniveau geeft aan hoe uitputtend een bepaalde competentie, en daarmee de onderliggende competentie-elementen (kennis of vaardigheid), worden beheerst. Voor het meten van een competentieniveau wordt onderscheid gemaakt tussen het meten van een kennisniveau en het meten van een vaardigheidsniveau. Dit is uitgewerkt in bijlage B.
Er is voor gekozen om per competentie één competentieniveau te hanteren. Dit betekent dat de verschillende competentie-elementen (kennis of vaardigheid) uit één competentie op hetzelfde niveau beheerst dienen te worden. Dit levert weinig discrepantie op met de praktijk en maakt het toetsen van een bepaalde competentie beduidend eenvoudiger en eenduidiger.

Chief Information Security Officer [17]

Profieltitel	CHIEF INFORMATION SECURITY OFFICER (CISO)		
Samenvatting	Definieert de informatiebeveiligingsstrategie en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.		
Missie	Definieert de informatiebeveiligingsstrategie, gebaseerd op een risicomanagementbenadering en rekening houdend met het informatiebeveiligingsdreigingenbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en wijst deze toe. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiligingsstrategie.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• Informatiebeveiligingsstrategie • Organisatie van informatiebeveiliging en expertise daarvoor • Informatiebeveiligingscalamiteitenorganisatie • Afstemming van informatiebeveiliging met andere beveiligingsdomeinen • Naleving van de eisen en architectuur voor informatiebeveiliging • Informatiebeveiligingsbewustzijn over de hele organisatie • Voorbereid zijn op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's • Informatierisicoanalyses, beveiligingsontwerpen en -oplossingen • Informatiebeveiligingsassessments, -tests, -reviews en -audits	• Projectportfolio voor informatiebeveiliging • Organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Monitoring van de relevante risico's voor de organisatie • Monitoring van compliance met beleid en wet- en regelgeving • Gecoördineerde reactie op ernstige informatiebeveiligings- of ICT-incidenten • Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging	• Risicomanagementbeleid • Informatiesysteem-governance • Service Level Agreements • Informatiebeveiligingsarchitectuur

[17] Dit beroepsprofiel is niet opgenomen in CWA 16458.

Kerntaken	• Definieert de informatiebeveiligingsstrategie voor de organisatie • Organiseert informatiebeveiliging en de daarvoor benodigde expertise • Zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, fysieke beveiliging en continuïteitsmanagement • Zet een informatiebeveiligingscalamiteitenorganisatie op • Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten • Zorgt voor een projectportfolio voor informatiebeveiliging • Initieert en coördineert organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Zorgt voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging • Monitort en borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en -oplossingen • Monitort en borgt het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design • Monitort en borgt informatiebeveiligingsbewustzijn binnen de organisatie • Monitort de relevante risico's voor de organisatie • Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's • Monitort en borgt de kwaliteit van informatiebeveiligingsassessments, -tests, -reviews en -audits • Monitort op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en wet- en regelgeving • Informeert senior algemeen management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen	
e-Competenties (uit e-CF)	D.1. Strategieontwikkeling informatiebeveiliging	Niveau 4
	E.3. Risicomanagement	Niveau 3
	E.4. Relatiemanagement	Niveau 3
	E.8. Informatiebeveiligingsmanagement	Niveau 4
Algemene competenties	G.1. Leiderschap	Niveau 3
	G.3. Communicatie en overtuigingskracht	Niveau 3
	G.5. Organisatiesensitiviteit	Niveau 3
	G.6. Management	Niveau 3
	G.7. Analytisch vermogen	Niveau 4
	G.8. Integriteit	Niveau 3
Opleiding en ervaring	• Een afgeronde relevante Master-opleiding [18] of daarmee vergelijkbaar niveau van kennis en vaardigheden • Vijf jaar werkervaring in een informatiebeveiligingsberoep • Vijf jaar werkervaring in een managementfunctie	
KPI	Een geschikt niveau van informatiebeveiliging en informatiebeveiligingsbewustzijn gebaseerd op de behoeften en risicobereidheid van de organisatie	

[18] Een Master-opleiding in het economische, exacte, technische of menswetenschappelijke domein.

Information Security Officer [19]

Profieltitel	INFORMATION SECURITY OFFICER (ISO)		
Samenvatting	Implementeert informatiebeveiliging in overeenstemming met de informatiebeveiligingsstrategie van de organisatie.		
Missie	Implementeert informatiebeveiliging in de organisatie. Zorgt in het kader van informatiebeveiliging voor een beveiligingsplan, risicoanalyses, risicomonitoring, incidentenregistratie, hulpmiddelen, training and evaluatie. Initieert en bestuurt informatiebeveiliging- en bewustwordingsprojecten. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• Gedocumenteerde kennisverzameling voor informatiebeveiliging • Registratie, analyse en rapportage van informatiebeveiligingsincidenten	• Implementatie van informatiebeveiliging • Afstemming van informatiebeveiliging met andere beveiligingsdomeinen • Informatiebeveiligingsprojecten • Training en opleiding voor informatiebeveiligingsbewustzijn • Risicoanalyses voor informatiesystemen • Vertaling van informatiebeveiligingbehoeftenaar beveiligingsmaatregelen • Informatiebeveiligingsontwerpen en -oplossingen • Monitoring van en rapportage over informatiebeveiligingsrisico's • Informatiebeveiligingsassessments, -tests, -reviews and -audits	• Informatiebeveiligingsstrategie • Projectportfolio voor informatiebeveiliging • Informatiebeveiligingsarchitectuur • Risicomanagementbeleid • organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging • Kennisuitwisseling over informatiebeveiliging

[19] Dit beroepsprofiel is niet opgenomen in CWA 16458.

Kerntaken	• Implementeert informatiebeveiliging in de organisatie • Voorziet in een gedocumenteerde kennisverzameling voor informatiebeveiliging • Zorgt voor adequate registratie, analyse en rapportage van informatiebeveiligings-incidenten • Initieert en managet informatiebeveiligingsprojecten • Stemt informatiebeveiligingsactiviteiten en -projecten af met andere beveiligings-domeinen, waaronder privacybescherming en fysieke beveiliging • Zorgt voor training en opleiding voor informatiebeveiligingsbewustzijn • Voert risicoanalyses voor informatiesystemen uit • Monitort informatiebeveiligingsririco's en rapporteert daarover • Vertaalt de informatiebeveiligingsbehoefte van de organisatie naar beveiligings-maatregelen • Zorgt voor informatiebeveiligingsontwerpen en -oplossingen en de implementatie van security-by-design en privacy-by-design in informatiesystemen • Presenteert informatiebeveiligingsoplossingen aan collega's en leidinggevenden • Realiseert en monitort informatiebeveiligingsassessments, -tests, -reviews en -audits • Presenteert verbetervoorstellen aan het management met betrekking tot informatie-beveiliging en -risico's	
e-Competenties (uit e-CF)	E.3. Risicomanagement	Niveau 2
	E.8. Informatiebeveiligingsmanagement	Niveau 3
Algemene competenties	G.2. Projectmanagement	Niveau 2
	G.3. Communicatie en overtuigingskracht	Niveau 2
	G.4. Onderzoek	Niveau 2
	G.5. Organisatiesensitiviteit	Niveau 2
	G.7. Analytisch vermogen	Niveau 3
	G.8. Integriteit	Niveau 2
Opleiding en ervaring	• Een afgeronde relevante Bachelor-opleiding [20] of een vergelijkbaar niveau van kennis en vaardigheden • Twee jaar werkervaring in een relevant beroep.	
KPI	De informatiebeveiligingsrisico's zijn bekend en de daarvoor benodigde maatregelen zijn getroffen	

[20] Een Bachelor-opleiding in het economische, exacte, technische, of menswetenschappelijke domein.

ICT-beveiligingsmanager

Profieltitel	**ICT-BEVEILIGINGSMANAGER**		
Samenvatting	Definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie en organiseert en managet de ICT-beveiliging van de organisatie.		
Missie	Definieert de ICT-beveiligingsrichtlijnen, rekening houdend met het ICT-beveiligingsdreigingenbeeld, trends, de ICT van de organisatie en toekomstige behoeften. Richt de ICT-beveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en wijst deze toe. Managet de implementatie van ICT-beveiliging voor alle ICT-systemen. Zorgt voor een geschikt niveau van ICT-beveiliging, gebaseerd op de behoeften en risicobereidheid van de organisatie.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• ICT-beveiligings-richtlijnen en implementatie daarvan • ICT-beveiligings-organisatie en expertise • ICT-beveiligings-projecten • ICT-beveiligings-assessments, -tests, -reviews en -audits	• Projectportfolio voor ICT-beveiliging • Procedures voor ICT-beveiliging • Risicoanalyses voor ICT • Monitoring van en rapportage over ICT-risico's • ICT-continuïteitsplan en oefeningen hiervan • Opleidingsbeleid voor ICT-beveiliging	• Risicomanagementbeleid • Informatiebeveiligings-strategie • Informatiebeveiligingsarchitectuur • Service Level Agreements • Implementatie van informatiebeveiliging • Integratievoorstellen voor nieuwe technologie
Kerntaken	• Definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie • Organiseert ICT-beveiliging en de daarvoor benodigde expertise • Managet de implementatie van de ICT-beveiligingsrichtlijnen • Zorgt voor een projectportfolio voor ICT-beveiliging • Definieert het opleidingsbeleid voor ICT-beveiliging • Definieert en implementeert procedures ten behoeve van ICT-beveiliging • Voert risicoanalyses voor ICT uit • Monitort ICT-risico's en rapporteert daarover • Zet het ICT-continuïteitsplan op en zorgt dat dit regelmatig wordt geoefend • Initieert and managet ICT-beveiligingsprojecten • Borgt de kwaliteit van de ICT-beveiligingsassessments, -tests, -reviews en -audits • Volgt technologische ontwikkelingen op het gebied van ICT-beveiliging • Informeert (C)ISO en senior algemeen management over de status van ICT-beveiliging en incidenten en presenteert verbetervoorstellen		
e-Competenties (uit e-CF)	A.7. Volgen van technologische ontwikkelingen		Niveau 2
	E.3. Risicomanagement		Niveau 2
	E.8. Informatiebeveiligingsmanagement		Niveau 3

Algemene competenties	G.2. Projectmanagement	Niveau 3
	G.3. Communicatie en overtuigingskracht	Niveau 3
	G.6. Management	Niveau 3
	G.7. Analytisch vermogen	Niveau 2
	G.8. Integriteit	Niveau 3
Opleiding en ervaring	• Een afgeronde relevante Bachelor-opleiding [21] of daarmee vergelijkbaar niveau van kennis en vaardigheden • Drie jaar werkervaring in een ICT-beveiligingsberoep • Drie jaar werkervaring in een managementfunctie	
KPI	Een geschikt niveau van ICT-beveiliging gebaseerd op de behoeften en de risico-bereidheid van de organisatie	

[21] Een Bachelor-opleiding in het exacte of technische domein.

ICT-beveiligingsspecialist 3

<table>
<tr><td>Profieltitel</td><td colspan="3">ICT-BEVEILIGINGSSPECIALIST 3</td></tr>
<tr><td>Samenvatting</td><td colspan="3">Ontwerpt en geeft invulling aan de ICT-beveiligingsrichtlijnen van de organisatie.</td></tr>
<tr><td>Missie</td><td colspan="3">Doet voorstellen voor en implementeert technische beveiligingsmaatregelen voor de ICT. Adviseert en ondersteunt om ICT veilig te laten werken. Neemt directe actie om systemen en netwerken of delen daarvan te beveiligen. Wordt door vakgenoten beschouwd als de deskundige op het gebied van ICT-beveiliging.</td></tr>
<tr><td>Producten</td><td>Eindverantwoordelijk</td><td>Realiseert</td><td>Draagt bij</td></tr>
<tr><td></td><td>• Gedocumenteerde kennisverzameling voor ICT-beveiliging</td><td>• Verbetervoorstellen voor beveiliging van ICT
• Integratievoorstellen voor nieuwe technologie
• Technische ICT-beveiligingsoplossingen, -maatregelen en -updates
• Selectie en implementatie van beveiligingshulpmiddelen
• ICT-beveiligingsassessments, -tests, -reviews en -audits
• Monitoring en borging van de technische beveiligingsmaatregelen voor de ICT
• Testen van het ICT-incident/response- en/of -continuïteitsplan</td><td>• Risicomanagementbeleid
• ICT-beveiligingsrichtlijnen en implementatie daarvan
• Risicoanalyses voor ICT
• Forensisch onderzoek
• ICT-incident/response- en/of -continuïteitsplan
• Kennisuitwisseling over ICT-beveiliging</td></tr>
<tr><td>Kerntaken</td><td colspan="3">• Volgt diepgaand technologische ontwikkelingen op het gebied van ICT-beveiliging
• Neemt kennis van actuele dreigingen en dreigingstrends en bepaalt de mogelijke impact hiervan op de organisatie
• Voorziet in een gedocumenteerde kennisverzameling voor ICT-beveiliging
• Stelt verbetervoorstellen op voor het beveiligen van de ICT
• Stelt voorstellen op voor integratie van nieuwe informatietechnologie
• Ontwerpt technische ICT-beveiligingsoplossingen
• Presenteert ICT-beveiligingsoplossingen aan collega’s en leidinggevenden
• Realiseert technische beveiligingsmaatregelen en beveiligingsupdates in systemen en netwerken
• Selecteert en implementeert beveiligingshulpmiddelen
• Realiseert en monitort ICT-beveiligingsassessments, -tests, -reviews en -audits
• Draagt bij aan forensisch onderzoek
• Monitort en borgt de technische beveiligingsmaatregelen voor de ICT en evalueert ICT-beveiligingsrisico’s
• Test het ICT-incident/response- en/of -continuïteitsplan
• Begeleidt minder ervaren collega’s in de ICT-beveiliging
• Presenteert verbetervoorstellen aan het lijnmanagement met betrekking tot ICT-beveiliging en -risico’s</td></tr>
</table>

e-Competenties (uit e-CF)	A.7. Volgen van technologische ontwikkelingen	Niveau 4
	B.4. Oplossingen implementeren	Niveau 4
	E.3. Risicomanagement	Niveau 3
	E.8. Informatiebeveiligingsmanagement	Niveau 3
Algemene competenties	G.3. Communicatie en overtuigingskracht	Niveau 2
	G.4. Onderzoek	Niveau 4
	G.7. Analytisch vermogen	Niveau 4
	G.8. Integriteit	Niveau 2
Opleiding en ervaring	Een afgeronde Master-opleiding in het ICT-domein of een vergelijkbaar niveau van kennis en vaardigheden	
KPI	De benodigde ICT-beveiligingsmaatregelen zijn op doeltreffende wijze getroffen	

ICT-beveiligingsspecialist 2

<table>
<tr><td>Profieltitel</td><td colspan="3">ICT-BEVEILIGINGSSPECIALIST 2</td></tr>
<tr><td>Samenvatting</td><td colspan="3">Geeft invulling aan de ICT-beveiligingsrichtlijnen van de organisatie.</td></tr>
<tr><td>Missie</td><td colspan="3">Doet voorstellen voor en implementeert technische beveiligingsmaatregelen voor de ICT. Adviseert en ondersteunt om ICT veilig te laten werken. Neemt directe actie om systemen en netwerken of delen daarvan te beveiligen.</td></tr>
<tr><td>Producten</td><td>Eindverantwoordelijk</td><td>Realiseert</td><td>Draagt bij</td></tr>
<tr><td></td><td>• Gedocumenteerde kennisverzameling voor ICT-beveiliging</td><td>• Verbetervoorstellen voor beveiliging van ICT
• Technische ICT-beveiligingsoplossingen, -maatregelen en -updates
• Selectie en implementatie van beveiligingshulpmiddelen
• ICT-beveiligingsassessments, -tests en -reviews
• Monitoring en borging van de technische beveiligingsmaatregelen voor de ICT</td><td>• ICT-beveiligingsrichtlijnen en implementatie daarvan
• Risicoanalyses voor ICT
• Forensisch onderzoek
• ICT-incident/response- en/of -continuïteitsplan
• Kennisuitwisseling over ICT-beveiliging</td></tr>
<tr><td>Kerntaken</td><td colspan="3">• Volgt technologische ontwikkelingen op het gebied van ICT-beveiliging
• Neemt kennis van actuele dreigingen en dreigingstrends en bepaalt de mogelijke impact hiervan op de organisatie
• Voorziet in een gedocumenteerde kennisverzameling voor ICT-beveiliging
• Stelt verbetervoorstellen op voor het beveiligen van de ICT
• Ontwerpt technische ICT-beveiligingsoplossingen
• Presenteert ICT-beveiligingsoplossingen aan collega’s en leidinggevenden
• Realiseert technische beveiligingsmaatregelen en beveiligingsupdates in systemen en tewerken
• Selecteert en implementeert beveiligingshulpmiddelen
• Realiseert en monitort ICT-beveiligingsassessments, -tests en -reviews
• Draagt bij aan forensisch onderzoek
• Monitort en borgt de technische beveiligingsmaatregelen voor de ICT en evalueert ICT-beveiligingsrisico’s
• Test onderdelen van het ICT- incident/response- en/of -continuïteitsplan
• Presenteert verbetervoorstellen aan het lijnmanagement met betrekking tot ICT-beveiliging en -risico’s</td></tr>
<tr><td rowspan="3">e-Competenties (uit e-CF)</td><td colspan="2">A.7. Volgen van technologische ontwikkelingen</td><td>Niveau 3</td></tr>
<tr><td colspan="2">B.4. Oplossingen implementeren</td><td>Niveau 3</td></tr>
<tr><td colspan="2">E.8. Informatiebeveiligingsmanagement</td><td>Niveau 2</td></tr>
</table>

Algemene competenties	G.3. Communicatie en overtuigingskracht	Niveau 2
	G.4. Onderzoek	Niveau 3
	G.7. Analytisch vermogen	Niveau 3
	G.8. Integriteit	Niveau 2
Opleiding en ervaring	Een afgeronde hbo-opleiding in het ICT-domein of een vergelijkbaar niveau van kennis en vaardigheden	
KPI	De benodigde ICT-beveiligingsmaatregelen zijn op doeltreffende wijze getroffen	

ICT-beveiligingsspecialist 1

Profieltitel	**ICT-BEVEILIGINGSSPECIALIST 1**		
Samenvatting	Realiseert technische beveiligingsmaatregelen voor de ICT en monitort de ICT-beveiliging van de organisatie.		
Missie	Implementeert de benodigde beveiligingsmaatregelen in de ICT. Ondersteunt en informeert om ICT veilig te laten werken. Neemt directe actie om systemen en netwerken of delen daarvan te beveiligen.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
		• Technische ICT-beveiligings-maatregelen en -updates • Selectie en implementatie van beveiligingshulpmiddelen • Monitoring van de technische beveiligingsmaatregelen voor de ICT	• ICT-beveiligings-richtlijnen en imple-mentatie daarvan • Risicoanalyses voor ICT
Kerntaken	• Volgt de belangrijkste technologische ontwikkelingen op het gebied van ICT-beveiliging • Realiseert technische ICT-beveiligingsmaatregelen en beveiligingsupdates in systemen en netwerken • Selecteert en implementeert beveiligingshulpmiddelen • Monitort de technische beveiligingsmaatregelen voor de ICT en evalueert ICT-beveiligingsrisico's • Rapporteert over de werking van ICT-beveiligingsmaatregelen		
e-Competenties (uit e-CF)	A.7. Volgen van technologische ontwikkelingen		Niveau 2
	B.4. Oplossingen implementeren		Niveau 2
	E.8. Informatiebeveiligingsmanagement		Niveau 2
Algemene competenties	G.3. Communicatie en overtuigingskracht		Niveau 1
	G.4. Onderzoek		Niveau 2
	G.8. Integriteit		Niveau 2
Opleiding en ervaring	Een afgeronde mbo 4-opleiding in het ICT-domein of een vergelijkbaar niveau van kennis en vaardigheden		
KPI	De gangbare ICT-beveiligingsmaatregelen zijn getroffen		

Gebruik van de profielen

Profielen en functies

Binnen het domein van de informatiebeveiliging zijn veel verschillende functieaanduidingen in omloop. Zo kan iemand die op strategisch niveau information risk management uitoefent de functie Chief Information Security Officer hebben, maar bijvoorbeeld ook Information Risk Manager, of Information Security Manager. In ieder van deze functies voert de betreffende persoon soortgelijke taken uit en heeft soortgelijke competenties nodig, namelijk de taken en competenties die zijn uitgewerkt in het standaard beroepsprofiel *Chief Information Security Officer*. Dit beroepsprofiel moet gezien worden als een kenmerkende beroepsomschrijving, geformuleerd in termen die binnen het vakgebied herkend worden.

Het beroepsprofiel is *geen* functiebeschrijving, maar een beschrijving die opgenomen *kan* worden in een functiebeschrijving. Daarentegen is het ook mogelijk om een functie op te bouwen uit meerdere beroepsprofielen, of juist uit een deel van één beroepsprofiel. Maar zelfs als een organisatie ervoor kiest om één op één een beroepsprofiel, bijvoorbeeld *Chief Information Security Officer*, over te nemen in één functie, dan kan deze functie een andere naam krijgen, bijvoorbeeld Information Security Manager (andere vlag, zelfde lading). Een organisatie kan er ook voor kiezen om een Chief Information Security Officer te benoemen op basis van het beroepsprofiel Information Security Officer.

In de praktijk zal iedere organisatie een bepaalde informatiebeveiligingsfunctie opbouwen uit één of meer (delen van) beroepsprofielen en daar dan een eigen functienaam voor kiezen. Vervolgens zal de organisatie ook nog een eigen sausje willen gieten over de invulling van de betreffende functie. Dat is geen willekeur, maar vooral nuttig. Zo zal de organisatie wellicht bepaalde kennis van de organisatie en de branche in de functiebeschrijving willen vastleggen. Bovendien heeft elke organisatie specifieke kenmerken die aanpassing van de functie nodig maken. Daarnaast zijn er ‘kleinere’ al dan niet organisatiespecifieke zaken (bijvoorbeeld taken of competenties) die in de functiebeschrijving geregeld moeten worden, maar die ‘te klein’ zijn om in het beroepsprofiel te staan. Door deze opbouw van een functiebeschrijving zal deze normaal gesproken verschillen van de standaard beroepsprofielen. Zolang de verschillen niet te groot worden (80/20-regel) blijven de standaard beroepsprofielen een goede indicatie geven van de informatiebeveiligingsfuncties en de eisen die daaraan worden gesteld.

Eenvoudige en complexe organisaties

De beschreven beroepsprofielen zijn in eerste instantie opgesteld voor middelgrote informatieverwerkende organisaties waarin informatiebeveiliging een prominente rol speelt. Het gaat dan bijvoorbeeld om ministeries, uitvoeringsorganisaties, middelgrote banken en middelgrote industriële organisaties met belangrijke informatievoorziening.

Organisaties die minder complex zijn op het gebied van informatiebeveiliging stellen in het algemeen minder hoge eisen aan hun informatiebeveiligingsfuncties. Dit geldt bijvoorbeeld voor kleine gemeenten, of productiebedrijven met een relatief beperkte informatievoorziening. Zij kunnen in hun functiebeschrijvingen voor de informatiebeveiligingsfuncties voor een aantal competenties lagere niveaus specificeren dan in het onderliggende beroepsprofiel, of bepaalde competenties zelfs schrappen.

Organisaties die daarentegen complexer zijn op het gebied van informatiebeveiliging zullen in het algemeen juist zwaardere eisen stellen aan hun informatiebeveiligingsfuncties. Dit geldt bijvoorbeeld voor grote internationaal opererende banken en grote multinationals die sterk afhankelijk zijn van hun informatievoorziening. Zij kunnen in hun functiebeschrijvingen voor de informatiebeveiligingsfuncties voor sommige competenties hogere niveaus specificeren dan in het onderliggende beroepsprofiel en/of aanvullende competenties toevoegen.

Opleidingen en examens

In de beschreven beroepsprofielen worden competenties genoemd die een beoefenaar van het betreffende beroep zou moeten bezitten. Een beoefenaar moet de genoemde competenties kunnen verwerven. Daarvoor zijn in principe twee mogelijkheden, namelijk het volgen van onderwijs en het leren in de praktijk. Een combinatie hiervan is ook mogelijk.

Het volgen van onderwijs en het leren in de praktijk hebben beide voor- en nadelen. Zo brengt het volgen van onderwijs de beoogde competenties sneller binnen bereik, maar het leereffect blijft veelal beperkt tot de beoogde competenties. Met leren in de praktijk kost het veelal meer tijd om de beoogde competenties te verwerven, maar daarnaast worden ook andere competenties verworven die wellicht niet direct nodig zijn, maar de persoon in kwestie wel een bredere basis geven en daarmee meer flexibiliteit in inzicht en handelen. Vanwege de verschillende voor- en nadelen is het wenselijk om beide mogelijkheden beschikbaar te hebben.

Geschikt onderwijs voor informatiebeveiligers in spe kan aangeboden worden door opleidingsinstellingen. Zij kunnen nieuwe opleidingen en cursussen opzetten op basis van de in de beroepsprofielen genoemde competenties. De competenties worden dan gebruikt als eindtermen van de nieuwe opleidingen en cursussen. De competenties kunnen ook gebruikt worden om van reeds bestaande opleidingen en cursussen na te gaan of deze de gevraagde competenties ontwikkelen. Ook examens kunnen gebaseerd worden op de genoemde competenties.

In het algemeen geldt dat initiële opleidingen (universiteit, hbo, mbo) niet zonder meer geschikt zijn om voor elk beroepsprofiel op te leiden. Zo worden aan de ‘zware’ beroepsprofielen (*Chief Information Security Officer* en *ICT Security Manager*) hogere eisen gesteld dan deelnemers in een initiële opleiding kunnen verwerven. Dergelijke opleidingen kunnen wel geschikt zijn om een stevig fundament te leggen, waarna afgestudeerden alsnog de benodigde aanvullende competenties voor één van de ‘zware’ beroepsprofielen kunnen verwerven door werkervaring op te doen en extra cursussen te volgen.

Voor het leren in de praktijk hoeft weinig geregeld te worden. In principe biedt de grote variatie aan bedrijven en instanties voldoende mogelijkheden om in de praktijk de benodigde competenties te kunnen verwerven. Wel moet er een mechanisme zijn waarmee de verworven competenties getoetst kunnen worden, zodat mensen zich kunnen kwalificeren voor bepaalde beroepsprofielen. De toetsing kan gebaseerd worden op de voor de beroepsprofielen genoemde competenties. Hiervoor dient een toetsingsproces te worden ingericht met eenduidige toetscriteria en ondergebracht bij één of meer toetsinstanties.

In principe zijn het volgen van onderwijs en het leren in de praktijk in allerlei verhoudingen te combineren. In sommige gevallen zijn de beide mogelijkheden uitwisselbaar. Zo kan bijvoorbeeld iemand met een aantal jaren werkervaring vrijstelling krijgen voor een deel van een opleiding. In andere gevallen

vullen de beide mogelijkheden elkaar aan. Een voorbeeld hiervan is het hierboven genoemde verwerven van aanvullende competenties voor een van de ‘zware’ beroepsprofielen door werkervaring op te doen en extra cursussen te volgen na het volgen van een initiële opleiding.

Doorleren en doorgroeien

Een professional die zich heeft gekwalificeerd voor één van de beroepen in dit document zal in de loop van de tijd extra kennis en vaardigheden op (moeten) doen. Van elke professional wordt vereist dat hij zijn vakmanschap op peil houdt (‘life long learning’), door kennis en vaardigheden op te doen die nodig zijn voor het anticiperen op de relevante maatschappelijke en technische ontwikkelingen. Daarmee blijft de professional steeds in staat om zijn beroep goed uit te voeren in een veranderende wereld.

Bovenop het op peil houden van het vakmanschap kan een professional ervoor kiezen om in een bepaald subdomein extra kennis en vaardigheden te verwerven, om zich zo te specialiseren in het betreffende subdomein. Met deze extra expertise verkrijgt de professional een specialisatie bovenop de standaard beroepskwalificatie. Zo kan bijvoorbeeld een ICT-beveiligingsspecialist 2 zich verder specialiseren in ethisch hacken. De betreffende professional is dan in staat om binnen zijn specialisatie taken uit te voeren die niet door een gemiddelde beoefenaar van het betreffende beroep uitgevoerd kunnen worden. Specialisaties maken geen deel uit van beroepsprofielen, maar kunnen wel vereist zijn in een bepaalde functiebeschrijving.

De uitzondering hierop is degene die zich in eerste instantie heeft gekwalificeerd voor een van de standaard beroepsprofielen en vervolgens alle aanvullend benodigde kennis en vaardigheden verwerft voor een ander standaard beroepsprofiel. In dat geval is het voor diegene mogelijk om zich te laten kwalificeren voor het nieuw behaalde beroepsprofiel. Voor de hand liggende doorgroeipaden zijn die van ISO naar CISO en die van ICT-beveiligingsspecialist 1 naar ICT-beveiligingsspecialist 2 en van ICT-beveiligingsspecialist 2 naar ICT-beveiligingsspecialist 3.

Bijlage A: Legenda beroepsprofieltabel

Term	Beschrijving [22]
Profieltitel	Geeft een gangbare naam aan het profiel.
Samenvatting	Geeft een indicatie van de belangrijkste elementen van het profiel. Het doel hiervan is stakeholders en gebruikers een kort en bondig overzicht van het profiel te geven. De beschrijving moet begrijpelijk zijn voor zowel professionals, managers, als medewerkers van HRM (Human Resource Management).
Missie	Beschrijft de hoofddoelstelling. Het doel hiervan is het in het profiel beschreven beroep te specificeren.
Producten	Benoemt de belangrijkste producten. Tevens wordt aangegeven welke plaats in het RACI-model wordt ingenomen met betrekking tot de gegeven producten. Daarbij wordt onderscheid gemaakt naar A: eindverantwoordelijk (accountable), R: realisatie (responsible), C: bijdragend (contributor).
Kerntaken	Benoemt de belangrijkste taken. Een taak is een activiteit die wordt uitgevoerd om een bepaald resultaat te behalen.
e-Competenties	Geeft een opsomming van benodigde e-competenties (uit het e-CF) die nodig zijn om de missie uit te kunnen voeren. Belangrijk is dat hierbij ook de benodigde competentieniveaus worden gespecificeerd.
Algemene competenties	Geeft een opsomming van benodigde algemene competenties die nodig zijn om de missie uit te kunnen voeren. Belangrijk is dat hierbij ook de benodigde competentieniveaus worden gespecificeerd.
Opleiding en ervaring	Specificeert het minimumniveau voor benodigde vooropleiding en ervaring.
KPI	Geeft de belangrijkste prestatie-indicator (KPI – Key Performance Indicator).

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

Bijlage B: Competentieniveaus

In de profielen van de informatiebeveiligingsberoepen worden competenties, ofwel kennis en vaardigheden, gespecificeerd voor de informatiebeveiligingsprofessionals. Voor iedere competentie wordt aangegeven op welk niveau de betreffende competentie beheerst dient te worden. In navolging van e-CF kan het competentieniveau een waarde van 1 (laag) tot 5 (hoog) hebben.[23] De gebruikte competentieniveaus worden hieronder toegelicht.

Competentieniveaus met betrekking tot kennis

Een competentieniveau met betrekking tot de kennis die een professional van een bepaald kennisdomein heeft, wordt afgemeten aan twee aspecten, te weten de *compleetheid* van de kennis van het betreffende kennisdomein, alsmede het *beheersingsniveau* van deze kennis. Het beheersingsniveau is gebaseerd op de taxonomie van Bloom (zie de toelichting aan het eind van deze bijlage).

Competentieniveau kennis *		Compleetheid van het kennisdomein		
		Enkele belangrijke elementen	Alle belangrijke elementen	Zeer uitgebreid
Beheersingsniveau van de kennis	Analyseren, evalueren en innoveren		**4**	**5**
	Selecteren en toepassen		**3**	
	Reproduceren en verklaren	**1**	**2**	

* Een score in een blanco cel worden afgerond naar de eerstvolgende waarde beneden of links.

In het algemeen kunnen we stellen dat kennis van een bepaald domein met name zinvol is als de professional alle belangrijke elementen uit het betreffende domein kent.
Bij het bepalen van een kennisniveau zullen we in eerste instantie dan ook uitgaan van het kennen van *alle belangrijke elementen* van het betreffende kennisdomein. Het niveau geeft dan aan hoe goed de professional daarmee uit de voeten kan. De schaal loopt van niveau 2 – het kunnen reproduceren en verklaren van alle belangrijke elementen – tot niveau 4 – het kunnen analyseren, evalueren en innoveren van alle belangrijke elementen.
Als een professional het niveau ‘reproduceren en verklaren’ nog niet voor alle belangrijke elementen beheerst, dan is er sprake van het minimumniveau, namelijk niveau 1.
Als een professional meer kennis heeft dan ‘het kunnen analyseren, evalueren en innoveren van alle belangrijke elementen’ dan is er sprake van het maximumniveau, namelijk niveau 5.

Voorbeeld: Een professional die alle belangrijke elementen van een gegeven kennisdomein (bijvoorbeeld "best practices in en standaarden voor informatiebeveiligingsmanagement") niet alleen kan re-

[23] In e-CF zijn de niveaus in feite verantwoordelijkheidsniveaus en geen competentieniveaus. Daarom is de beschrijving van de niveaus zodanig aangepast dat er sprake is van competentieniveaus.

produceren, verklaren, selecteren en toepassen, maar deze ook kan analyseren, evalueren en innoveren, beheerst deze kennis op niveau 4.

Competentieniveaus met betrekking tot vaardigheden

Een competentieniveau met betrekking tot de vaardigheid waarmee een professional een bepaalde activiteit uit kan voeren, wordt afgemeten aan twee aspecten, te weten de *complexiteit* van de betreffende activiteit en de mate van *zelfstandigheid* waarmee de professional deze activiteit uit kan voeren.

Competentiniveau vaardigheden *		Complexiteit van de activiteit		
		Gestructureerd en voorspelbaar	**On**gestructureerd **of** **on**voorspelbaar	**On**gestructureerd **en** **on**voorspelbaar
Zelfstandigheid van de uitvoering	Geeft begeleiding			**5**
	Zelfstandig	**2**	**3**	**4**
	Onder begeleiding	**1**		

* Een score in een blanco cel worden afgerond naar de eerstvolgende waarde beneden of links.

In het algemeen kunnen we stellen dat de vaardigheid om een bepaalde activiteit te kunnen uitvoeren met name zinvol is als de betreffende activiteit door de professional zelf zelfstandig uitgevoerd kan worden.
Bij het bepalen van een vaardigheidsniveau zullen we dan ook uitgaan van het *zelfstandig* kunnen uitvoeren van de betreffende activiteit. De schaal loopt van niveau 2 – het zelfstandig kunnen uitvoeren van de activiteit in een gestructureerde en voorspelbare omgeving – tot niveau 4 – het uitvoeren van de activiteit in een **on**gestructureerde en **on**voorspelbare omgeving.
Als een professional de activiteit in een gestructureerde en voorspelbare omgeving nog niet zelfstandig uit kan voeren dan is er sprake van het minimumniveau, namelijk niveau 1.
Als een professional in een **on**gestructureerde en **on**voorspelbare omgeving zelfs anderen kan begeleiden bij het uitvoeren van de activiteit dan is er sprake van het maximumniveau, namelijk niveau 5.

Voorbeeld: Een professional die zelfstandig de activiteit "uitvoeren van beveiligingsaudits" kan uitvoeren in een ongestructureerde en onvoorspelbare omgeving (bijvoorbeeld een middelgrote tot grote organisatie) beheerst deze vaardigheid op niveau 4.

Beheersingsniveau van kennis en taxonomie van Bloom

Het *beheersingsniveau* van kennis is gebaseerd op de taxonomie van Bloom.[24] De taxonomie is teruggebracht tot drie niveaus, zoals geschetst in onderstaande tabel.

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

Taxonomie van Bloom	Beheersingsniveau van kennis
Creëren	Analyseren, evalueren en innoveren
Evalueren	
Analyseren	
Toepassen	Selecteren en toepassen
Verklaren	Reproduceren en verklaren
Reproduceren	

BijlageC: Begrippenlijst

Term	Definitie / beschrijving
Eindverantwoordelijk (accountable)	Degene die eindverantwoordelijk is, is de ‘eigenaar’ van een taak of product. De eigenaar is degene die goedkeurt of tekent voor het behaalde resultaat. De eigenaar is er ook voor verantwoordelijk dat voor de realisatie van de taak of het product mensen worden aangewezen. Er kan slecht één persoon eindverantwoordelijk zijn voor een taak of product. [CWA 16458]
Competentie(niveau)	Competentie is het vermogen om kennis, vaardigheden en houding toe te passen om bepaalde resultaten te behalen. Een competentie kan een niveau van 1 tot 5 hebben. [CWA16234-1]
Draagt bij (contributor)	Degene die bijdraagt, geeft input voor een taak of product. Meerdere mensen kunnen gezamenlijk bijdragen aan één taak of product. [CWA 16458]
e-competentie(niveau)	Een competentie in het ICT-domein. Een e-competentie kan een niveau van 1 tot 5 hebben.
Producten	Een van tevoren gedefinieerd resultaat van een taak in een werkomgeving. [CWA 16458]
Opleidingsprofiel	Een formele beschrijving van een curriculum. Het curriculum omvat de kennis, vaardigheden en houding die nodig zijn voor het betreffende beroepsprofiel.
Ervaring	Praktijkcontact met en observaties van feiten en gebeurtenissen. [Oxford Dictionaries]
Algemene competentie	Een competentie die niet specifiek is voor het ICT-domein. Een algemene competentie kan een niveau van 1 tot 5 hebben.
Informatierisico-management	Gecoördineerde activiteiten om een organisatie met betrekking tot de risico's van haar informatievoorziening te sturen en te beheersen. [ISO Guide 73]
ICT-beveiliging	Het beschermen van vertrouwelijkheid, integriteit en beschikbaarheid van ICT. [gebaseerd op de definitie van informatiebeveiliging]
Informatiebeveiliging	Het beschermen van vertrouwelijkheid, integriteit en beschikbaarheid van informatie. [ISO 27000]
Beroepsprofiel	Een formele beschrijving van een beroep. Het beschrijft de missie, taken en verantwoordelijkheden van een beoefenaar van het betreffende beroep en specificeert de competenties die de beoefenaar dient te hebben.
Kennis	De verzameling “wetenwat" (bijvoorbeeld programmeertalen, ...). [CWA 16458]

Term	Definitie / beschrijving
Kwalificatie	Een formeel resultaat van een beoordelings- en validatieproces, dat wordt verworven wanneer een bevoegde instantie bepaalt dat de leerresultaten die een individu heeft bereikt, aan gegeven normen voldoen. [European Qualifications Framework, Key Terms]
Realisatie (responsible)	Degene die het werk uitvoert. Meerdere mensen kunnen gezamenlijk bezig zijn met de realisatie van één taak of product. [CWA 16458]
Vaardigheid	Het vermogen om bepaalde taken uit te voeren. [CWA 16458]
Taak	Een activiteit die wordt uitgevoerd om een bepaald resultaat te behalen. Een taak kan geassocieerd worden met deadlines, middelen, doelen, specificaties en/of verwachte resultaten. [CWA 16458]

Over PvIB

PvIB (Platform voor Informatiebeveiliging) is met ruim 1400 leden hèt kennisplatform op het gebied van informatiebeveiliging in Nederland. Het platform is een open, breed samengestelde vereniging van professionals die actief inhoud geven aan informatiebeveiliging, door het uitwisselen van kennis en ervaring. Daarnaast bevordert PvIB het ‘netwerken’ van personen die in het vakgebied werkzaam zijn.

De doelgroep van PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. De leden van PvIB komen voort uit alle soorten en maten van bedrijven, overheden en opleidingsinstellingen. De producten en diensten van PvIB zijn vakinhoudelijk en niet commercieel.

PvIB streeft naar maatschappelijke profilering van het vakgebied informatiebeveiliging en het professionaliseren van de beroepsgroep van informatiebeveiligers, onder meer door zich in te zetten voor de ontwikkeling van een erkende kwalificatiestructuur. Er wordt gestreefd naar afstemming op Europees niveau.