# Kwalificatie en certificatie van informatiebeveiligers

*In de huidige informatiemaatschappij waarin informatie zowel economisch als maatschappelijk van cruciaal belang is, wordt het steeds belangrijker dat informatiebeveiligers acteren op een herkenbaar en erkend niveau van vakbekwaamheid. Dit is nog geenszins het geval. In tegendeel, informatiebeveiligers kunnen zich kwalificeren door middel van een grote variëteit aan onderling onvergelijkbare opleidingen, certificaten en titels. Het is daardoor onduidelijk welke kennis en ervaring een informatiebeveiliger heeft. Dit artikel schetst de resultaten van een onderzoek naar het nut en de haalbaarheid van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers.*

*Auteurs:* **Marcel Spruit** is lector Cyber security & safety aan de Haagse Hogeschool en senior consultant bij Het Expertise Centrum. Hij is te bereiken op m.e.m.spruit@hhs.nl.
**Fred van Noord** is voorzitter van het Platform voor Informatiebeveiliging (PvIB) en management consultant bij Verdonck, Klooster & Associates. Hij is te bereiken op fred.vannoord@vka.nl.

## Inleiding

Informatie speelt een belangrijke rol in de samenleving. Het economische en maatschappelijke belang van informatie en de afhankelijkheid ervan worden steeds groter. Onze economie en onze maatschappij moeten kunnen vertrouwen op het juist functioneren van de informatievoorziening. Daarmee wordt informatiebeveiliging steeds belangrijker en wordt het ook belangrijker dat informatiebeveiligers een herkenbaar en erkend niveau van vakbekwaamheid hebben dat toepasbaar is in alle sectoren van de overheid en het bedrijfsleven.

Organisaties die informatiebeveiligers willen aanstellen, kunnen door de verscheidenheid aan opleidingen, certificaten en titels op het gebied van informatiebeveiliging op dit moment moeilijk bepalen of informatiebeveiligers met een bepaalde opleiding of titel voldoende competenties in huis hebben en met welke opleiding(en) eventuele hiaten in kennis en vaardigheden opgevuld kunnen worden.

Dit probleem wordt onder meer veroorzaakt doordat instellingen voor middelbaar en hoger onderwijs en commerciële opleiders hun opleidingen op het gebied van informatiebeveiliging niet of nauwelijks gestandaardiseerd en geharmoniseerd hebben. Daardoor is het onduidelijk in hoeverre verschillende opleidingen met elkaar te vergelijken zijn en welke in het kader van doorstroming goed op elkaar aansluiten.

Daarnaast geven zowel opleiders als andere organisaties, zoals beroepsverenigingen, certificaten en titels uit, die soms op opleidingen zijn gestoeld, soms op beroepservaring en soms op beide.

De vraag is in hoeverre een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers van nut kan zijn voor bedrijven en overheidsorganisaties die werken met informatiebeveiligers, de aanbieders van opleidingen op het gebied van informatiebeveiliging en de informatiebeveiligers zelf.

Om antwoord te kunnen geven op deze vraag hebben de auteurs in opdracht van het Nederlandse Centre for Protection of National Infrastructure (CPNI.NL) onderzoek gedaan naar de wenselijkheid en de haalbaarheid van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland (Spruit en Van Noord, 2011). Daarbij is ook gekeken naar de wijze waarop een dergelijk stelsel ingevoerd en beheerd kan worden.

Het onderzoek betrof de volle breedte van het vakgebied informatiebeveiliging, maar beperkte zich tot een kwalificatie- en certificatiestelsel voor Nederland. In een later stadium kan aansluiting gezocht worden bij internationale gremia, of kan de Nederlandse aanpak in het buitenland gebruikt worden. Wel zijn relevante buitenlandse kwalificaties en certificaten (zoals van $(ISC)^2$ en ISACA) in het onderzoek meegenomen.

## Wenselijkheid en haalbaarheid van kwalificatie en certificatie

Om inzicht te krijgen in de wenselijkheid en de haalbaarheid van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers zijn circa vijftig mensen geïnterviewd. De geïnterviewden hadden in hun werksituatie direct te maken met informatiebeveiliging (of informatiebeveiligers) en waren afkomstig uit het bedrijfsleven, overheid, onderwijs en certificatie-instanties.

Uit de interviews bleek dat er consensus bestaat over het groeiende economische en maatschappelijke belang van informatiebeveiliging en de noodzaak om geen twijfel te laten bestaan over de vakbekwaamheid van haar professionals. Bovendien vond men dat mensen opgeleid moeten kunnen worden voor de beroepen in het vakgebied informatiebeveiliging. Men gaf aan dat kwalificatie voor informatiebeveiligers op basis van opleiding en ervaring wenselijk zo niet noodzakelijk is en dat de huidige situatie met betrekking tot kwalificatie van professionals niet voldoet. Dit beeld stemt overeen met het beeld dat is geschetst in een position paper van de Commissie Informatiebeveiliging van VNO-NCW (VNO-NCW, 2010) en de Nationale Cyber Security Strategie (NCSS, 2011). Ook mw. Kroes, de Europese Commissaris voor ICT en Telecom, gaf aan dat zij kwalificatie van informatiebeveiligers belangrijk vindt (Kroes, 2010).

Uit de interviews bleek dat in de huidige tijdgeest kwalificatie zonder ‘bewijs’, dus zonder certificatie met formele registratie, steeds minder als een reële optie wordt beschouwd. Temeer daar registratie in een register duidelijk kan maken dat men niet alleen ooit een relevante opleiding heeft gedaan, maar sindsdien de eigen kennis en ervaring steeds heeft bijgehouden. Ook eurocommissaris mw. Kroes gaf aan dat zij certificatie met formele registratie nuttig vindt, maar dat er wel voldoende aandacht moet worden besteed aan de uitwisselbaarheid en de wederzijdse erkenning van registers in andere landen van de Europese Unie.

Een aantal geïnterviewden gaf aan het beter te vinden om pas in een later stadium te kiezen om certificatie met formele registratie al dan niet in te voeren, namelijk pas nadat kwalificatie van informatiebeveiligers succesvol ingevoerd is.

Al met al vond men dat een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers nodig is. De relevante bestaande kwalificaties en certificaten, ook uit het buitenland, moeten daarin worden meegenomen en de nationale kwalificaties en certificaten moeten internationaal worden erkend.

De meerderheid van de geïnterviewden denkt dat een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland haalbaar is, met de kanttekeningen dat voor certificatie met formele registratie voldoende aantallen nodig zijn en dat de kosten mogelijk een belemmerende factor kunnen zijn. Certificatie met formele registratie bestaat al voor een aantal andere

vakgebieden dan wel beroepen, zoals accountant, IT-auditor, (tand)arts en beveiliger. Enerzijds geeft dit aan dat certificatie met formele registratie in principe haalbaar is en anderzijds geeft het de mogelijkheid om best practices te vinden voor certificatie van informatiebeveiligers.

De geïnterviewden gaven in meerderheid aan dat het regelen van de ontwikkeling, het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers opgepakt moet worden door één of meer van de beroepsorganisaties. Welke van de beroepsorganisaties het stokje op gaat pakken, werd nog niet duidelijk, hoewel men er in het algemeen van uitgaat dat het PvIB (Platform voor Informatiebeveiliging) hierin in ieder geval een rol zal moeten spelen. Het is echter nog onduidelijk in hoeverre de beroepsorganisaties en/of de overheid de kosten willen dragen voor het ontwikkeltraject.

## Kwalificatie van informatiebeveiligers

Het vakgebied informatiebeveiliging is een tamelijk breed vakgebied. Te breed om als één kwalificatiedomein te beschouwen. Uit het onderzoek bleek dat onderscheid wenselijk is tussen informatierisicomanagement (IRM) en ICT-beveiliging:

- IRM (Engels: IRM, information risk management) omvat het gehele proces om een betrouwbare informatievoorziening te waarborgen. Dit proces heeft een brede scope waar informatievoorziening, informatiebeveiliging en risicomanagement als een integraal geheel beschouwd worden. In de praktijk werken hierin vooral generalisten.
- ICT-beveiliging (Engels: IT security) omvat het ontwerpen en implementeren van ICT-beveiligingsmaatregelen. Dit is een gebied waarin specialistische kennis en ervaring een belangrijke rol spelen. Naast een beperkt aantal breed inzetbare professionals zijn hiervoor vooral specialisten nodig.

Binnen het vakgebied informatiebeveiliging, maar naast IRM en ICT-beveiliging, zijn bovendien twee domeinen die al met eigen kwalificatie en certificatie werken, namelijk IT-audit en forensisch onderzoek (digitaal rechercheren). Daarnaast zijn er kleinschalige specialistische beroepen, zoals cryptoloog, die slechts door een relatief klein aantal professionals worden uitgevoerd en waarvoor het dan ook niet zinvol is om te investeren in uniforme kwalificatie en certificatie. Voor deze beroepen kan beter gericht worden geworven met individuele kwalificatie en maatwerk voor het opbouwen en bijhouden van kennis en ervaring.

Het vakgebied informatiebeveiliging, in dit geval toegespitst op IRM en ICT-beveiliging, kan op meer opleiding- en ervaringsniveaus worden uitgevoerd. Het ligt dan ook voor de hand om op meer opleiding- en ervaringsniveaus te kwalificeren. Het reguliere onderwijssysteem in Nederland kent drie niveaus voor het opleiden voor beroepen: mbo (middelbaar beroepsonderwijs), hbo (hoger beroepsonderwijs) en wo (wetenschappelijk, of universitair onderwijs). Hoewel dit in eerste instantie drie opleidingsniveaus zijn, worden deze niveaus in de praktijk vaak doorgetrokken naar denk- en ervaringsniveaus.

De driedeling mbo-hbo-wo functioneert in de praktijk naar tevredenheid en kan goed toegepast worden op IRM en ICT-beveiliging.

Professionals die al langdurig binnen het domein informatiebeveiliging werken, kunnen ook zonder relevante vooropleiding op één van de kwalificatieniveaus uitkomen. Een nieuw stelsel voor kwalificatie moet professionals de mogelijkheid bieden om zich te kwalificeren door het aantonen van opgebouwde kennis en ervaring.

Er bestaat al een groot aantal kwalificaties binnen het domein van de informatiebeveiliging, waaronder CISSP, CISA, CISM, MISM, MSIT, enzovoorts. Van deze kwalificaties is niet zonder meer duidelijk hoe ze relateren aan IRM en ICT-beveiliging op mbo-, hbo- en wo-niveau. Om bestaande kwalificaties mee te kunnen nemen in een nieuw stelsel voor kwalificatie, is het nodig om de bestaande kwalificaties op dit stelsel te 'mappen'. Hierdoor ontstaat bovendien aansluiting op buitenlandse kwalificatiestelsels.

## Certificatie van informatiebeveiligers

Aangezien voor kwalificatie van informatiebeveiligers onderscheid wordt gemaakt tussen IRM en ICT-beveiliging op mbo-, hbo- en wo-niveau, ligt het voor de hand om dit onderscheid ook toe te passen voor certificatie met formele registratie. Zo nodig kunnen daar andere aanduidingen aan worden verbonden, bijvoorbeeld junior, medior en senior. Dit sluit ook aan bij ideeën die in het buitenland leven, zoals van de Britse IISP (The Institute of Information Security Professionals, *www.instisp.org*).

Wanneer we andere beroepen beschouwen die certificatie met formele registratie toepassen, zoals accountant, IT-auditor, (tand)arts en beveiliger, dan blijkt dat steeds een aantal kenmerken aanwezig is:

- Er is een beroepsprofiel, waarin het beroep en het bijbehorende takenpakket duidelijk zijn beschreven, alsook de competenties die de beroepsbeoefenaar moet bezitten.
- Er is een onafhankelijke certificatie-instantie die daarvoor door de beroepsgroep of de overheid is aangewezen en die werkt conform een kwalificatie- en certificatieschema.
- Er is een certificatieregister waarin alle voor het betreffende beroep gecertificeerde beroepsbeoefenaren zijn opgenomen.
- Er zijn door de certificatie-instantie of de overheid erkende opleidingen waarmee een basiskwalificatie voor het betreffende beroep behaald kan worden.
- Er zijn gedrag- en beroepsregels waaraan de gecertificeerde beroepsbeoefenaren zijn gebonden.
- Er zijn eisen voor bij- en nascholing waarmee de gecertificeerde beroepsbeoefenaren hun kennis en vaardigheden aantoonbaar op peil houden.
- Er is tuchtrecht en er is een Raad van Tucht voor het aanpakken van gecertificeerde beroepsbeoefenaren die zich niet aan de gedrag- en beroepsregels houden. Hierbij moet de reële mogelijkheid bestaan om te worden geschrapt uit het register, bijvoorbeeld na wanprestatie.

Tevens is het van belang dat er voldoende aandacht wordt besteed aan de uitwisselbaarheid en wederzijdse erkenning van registers in andere landen.

## Scenario voor invoering

Het scenario voor invoering van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers doorloopt een aantal stappen die in onderstaande tabel zijn weergegeven. Om een goede afstemming met de beroepspraktijk te krijgen, ligt de trekkersrol bij voorkeur bij één of meer van de beroepsorganisaties. Het meest voor de hand ligt het PvIB (Platform voor Informatiebeveiliging), al dan niet in samenwerking met één of meer van de andere beroepsorganisaties, zoals NGI, NGN, NOREA en ISACA.

| Stap | Omschrijving | Uitvoerende partij |
|---|---|---|
| 1 | Het opstellen van een plan van aanpak voor het invoeren van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Bij het opstellen van het plan worden ook werkgevers en opleiders betrokken. | Beroepsorganisatie(s) |
| 2 | Het opstellen van beroeps- en opleidingsprofielen voor informatiebeveiligingsberoepen.<br>Een eerste aanzet hiervoor is gemaakt in het onderzoeksrapport (Spruit en Van Noord, 2011). | Beroepsorganisatie(s) en andere stakeholders |
| 3 | Het opstellen van kwalificatieschema's.<br>Per informatiebeveiligingsberoep wordt een schema opgesteld op basis van het betreffende beroeps- en opleidingsprofiel.<br>Bijzondere aandacht is nodig voor de mate waarin aanvullend ervaring nodig is voor kwalificatie.<br>Desgewenst kunnen verschillende niveaus worden onderscheiden, bijvoorbeeld junior, medior en senior. | Beroepsorganisatie(s) en opleiders |
| 4 | Het afstemmen van de kwalificatieschema's met de schema's die in andere landen gebruikt worden. | Beroepsorganisatie(s) |
| 5 | Het beheren en periodiek actualiseren van kwalificatieschema's. | Beroepsorganisatie(s) |
| 6 | Het definiëren van erkende opleidingen.<br>Per beroep met een kwalificatieprofiel worden één of meer opleidingen gedefinieerd op basis van het betreffende opleidingsprofiel.<br>Per opleiding moet een marktonderzoek uitgevoerd worden om aan te kunnen geven of er voldoende vraag is naar de betreffende opleiding. | Beroepsorganisatie(s) en opleiders |
| 7 | Het inrichten van erkende opleidingen. | Opleiders |
| 8 | Het nagaan in hoeverre certificatie door de beroepsorganisaties en andere stakeholders (werkgevers, opleidingsinstellingen en betrokken ministeries) nog steeds gewenst en haalbaar gevonden wordt.<br>Als dat het geval is, kan een go gegeven worden voor de volgende stappen. | Beroepsorganisaties en andere stakeholders |
| 9 | Het aanwijzen van een certificatie-instantie.<br>Bij deze instantie hoort ook een Raad van Tucht. | Beroepsorganisatie(s) |
| 10 | Het opstellen van certificatieschema's.<br>Per informatiebeveiligingsberoep wordt een schema opgesteld op basis van het betreffende kwalificatieprofiel.<br>Er dient aandacht besteed te worden aan het certificeren van de huidige professionals. | Certificatie-instantie |
| 11 | Het inrichten van één of meer registers.<br>Hierbij horen de gedrag- en beroepsregels en koppeling met bijbehorende certificatieschema(s). | Certificatie-instantie |
| 12 | Het implementeren en beheren van certificatieschema's. | Certificatie-instantie |
| 13 | Het periodiek evalueren van het kwalificatie- en certificatiestelsel voor informatiebeveiligers. | Beroepsorganisatie(s) |

Inmiddels worden voorbereidingen getroffen voor de eerste twee stappen van dit scenario. Zo stelt het PvIB een werkgroep samen en start de Haagse Hogeschool een onderzoeksproject om

invulling te geven aan deze stappen. De bemensing en de financiering van de overige stappen moet nog worden geregeld.

## Conclusie

Het vakgebied informatiebeveiliging is volwassen geworden, maar de kwalificatie van de beroepsbeoefenaren is nog niet goed geregeld. Uit een groot aantal interviews bleek dat men het zeer wenselijk vindt dat er een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland komt. De relevante bestaande kwalificaties en certificaten, ook uit het buitenland, moeten daarin worden meegenomen en de nationale kwalificaties en certificaten moeten internationaal worden erkend.

Certificatie met formele registratie kan op een groot draagvlak rekenen, maar een aantal geïnterviewden geeft er de voorkeur aan dat pas in een later stadium wordt gekozen om dit al dan niet in te voeren, namelijk pas nadat kwalificatie van informatiebeveiligers succesvol is ingevoerd.

Hoewel het invoeren van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers in principe haalbaar zou moeten zijn, is het nog geen uitgemaakte zaak wie de ontwikkeling, het beheer en de bekostiging ervan gaat realiseren.

In dit artikel is een scenario voor invoering van een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers beschreven. De voorbereidingen voor de uitvoering van de eerste stappen worden getroffen. In een later stadium kan aansluiting gezocht worden bij internationale gremia, of kan de Nederlandse aanpak in het buitenland gebruikt worden.

## Literatuur

M. Spruit en F. van Noord, *Onderzoek naar kwalificatie en certificatie van informatiebeveiligers*, Rapport VKA/HEC/CPNI, versie 1.0, 2011 (te downloaden van *www.pvib.nl* en *www.cpni.nl*).

N. Kroes, *Trust and Security in the Digital Agenda*, Informatiebeveiliging, nr. 8, 2010.

NCSS, *Nationale Cyber Security Strategie*, 2011.

VNO-NCW, *Kwalificatie van Professionals informatiebeveiliging*, VNO-NCW Commissie Informatiebeveiliging, 2010.