VERDONCK KLOOSTER & ASSOCIATES

PLATFORM VOOR CYBERSECURITY
CPNI.NL

Onderzoek naar kwalificatie en certificatie van informatiebeveiligers

Marcel Spruit
Fred van Noord

status	Definitief
versie	1.0
datum	11 april 2011

Inhoudsopgave

Inhoudsopgave ii

Samenvatting iv

1. Inleiding 1

1.1 Aanleiding 1
1.2 Probleemstelling 1
1.3 Doelstelling en afbakening 1
1.4 Aanpak en organisatie 2

2. Desk research 4

2.1 Informatiebeveiliging 4
2.2 Kwalificatie, certificatie en accreditatie 5
2.3 Certificatieschema en instanties voor persoonscertificatie 6
2.4 Certificatie van verschillende beroepen 7
2.5 Kenmerken van gecertificeerde beroepen 8
2.6 Certificatie van informatiebeveiligers 10
2.7 Conclusies 11

3. Veldonderzoek 13

3.1 Nut van kwalificatie en certificatie 13
3.2 Haalbaarheid van kwalificatie- en certificatiestelsel 15
3.3 Ontwikkeling, beheer en bekostiging van stelsel 15
3.4 Conclusies 16

4. Beroepsprofielen 18

4.1 Functies 18
4.2 Kerntaken 19

5. Opleidingsprofielen 21

5.1 Competentieniveaus 21
5.2 Informatierisicomanager 22
5.3 ICT-beveiliger 23
5.4 Opleidingsprofielen en opleidingen 26

6. Voorstel voor kwalificatie- en certificatiestelsel 27

6.1 Kwalificatie van informatiebeveiligers 27
6.2 Certificatie van informatiebeveiligers 28
6.3 Scenario voor invoering 31
6.4 Conclusies 33

7. Conclusies en aanbevelingen 35

7.1 Conclusies 35
7.2 Aanbevelingen 36

Bijlage A: Interviewvragen 38
Bijlage B: Geraadpleegde personen 39
Bijlage C: Geraadpleegde documentatie 41
Bijlage D: Leden klankbordgroep 42
Bijlage E: Beroepsorganisaties informatiebeveiliging 43
Bijlage F: Kwalificatie- en certificatie-instanties in Nederland 45
Bijlage G: Internationale certificatie-instanties 47
Bijlage H: Huidige kwalificatie van informatiebeveiligers in Nederland 50
Bijlage I: Kwalificatie voor andere beroepen 52
Bijlage J: Interview mw. Neelie Kroes 56
Bijlage K: Enquêteresultaten 58
Bijlage L: Afkortingen 59
Bijlage M: Afkortingen van certificeringen informatiebeveiliging 61
Bijlage N: Terminologie en definities 62

Samenvatting

Organisaties die informatiebeveiligers willen aanstellen, kunnen door de verscheidenheid aan opleidingen, certificaten en titels op het gebied van informatiebeveiliging 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 aangepakt kunnen worden.

Dit wordt vooral veroorzaakt doordat het initiële en post-initiële middelbaar en hoger onderwijs in Nederland de eindtermen van de opleidingen op het gebied van informatiebeveiliging nauwelijks gestandaardiseerd en geharmoniseerd heeft. Daardoor is het onduidelijk in hoeverre verschillende opleidingen met elkaar te vergelijken zijn en welke opleidingen in het kader van doorstroming goed op elkaar aansluiten.

Daarnaast geven zowel opleidingsinstellingen 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 enerzijds bedrijven en overheidsorganisaties die werken met informatiebeveiligers en anderzijds de aanbieders van onderwijs op het gebied van informatiebeveiliging.

Het onderzoek dat in dit rapport beschreven is, beoogt antwoord te geven op de volgende onderzoeksvragen:

- Is het nuttig en haalbaar om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren?
- Hoe kan een kwalificatie- en certificatiestelsel in Nederland met voldoende relevantie en draagvlak gerealiseerd worden?
- Hoe zijn het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers te realiseren?

Het onderzoek beperkt 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.

Is het nuttig en haalbaar om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren?

Binnen het vakgebied informatiebeveiliging bestaat een chaotische situatie met betrekking tot kwalificatie en certificatie van professionals. Om binnen het vakgebied te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de sa-

menleving, is het nuttig om in Nederland een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers op te zetten op basis van opleiding en ervaring. De voordelen hiervan zijn:

- Organisaties kunnen op basis van behaalde kwalificaties en certificaten beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties.
- De aanbieders van onderwijs kunnen de gedefinieerde kwalificatie- en certificatieniveaus gebruiken om hun opleidingen op af te stemmen.
- Professionals kunnen met erkende kwalificaties en certificaten eenvoudiger aantonen welke specifieke competenties ze met betrekking tot informatiebeveiliging hebben.

Uniforme kwalificatie en certificatie is vooral zinvol en wellicht zelfs noodzakelijk voor de volgende beroepen:

- Informatierisicomanager op strategisch en tactisch niveau.
- ICT-beveiliger op strategisch, tactisch en operationeel niveau.
- Relatief grootschalige specialistische beroepen op het gebied van informatierisicomanagement en ICT-beveiliging. Sommige van deze beroepen, zoals IT-auditor en digitaal forensisch onderzoeker, werken al met kwalificatie en certificatie.

Een kwalificatie- en certificatiestelsel voor informatiebeveiligers is niet alleen nuttig en nodig, maar wordt ook haalbaar gevonden, mits duidelijk wordt dat te kleine aantallen kandidaten en te hoge kosten geen belemmerende factoren zullen zijn.
Een aantal geraadpleegde personen ziet bij voorkeur dat de beslissing om certificatie al dan niet in te voeren pas wordt genomen nadat kwalificatie van informatiebeveiligers geregeld is.

Desgewenst kunnen in een kwalificatie- en certificatiestelsel voor informatiebeveiligers meerdere niveaus onderscheiden worden, bijvoorbeeld junior, medior en senior. Daarnaast moet de reële mogelijkheid bestaan om geschrapt te worden uit het certificatieregister, bijvoorbeeld na wanprestatie.

Het is nodig dat de relevante bestaande kwalificaties en certificaten, ook uit het buitenland, in een nieuw kwalificatie- en certificatiestelsel voor informatiebeveiliging meegenomen worden. Ook is het van belang om nationale kwalificaties en certificaten internationaal te (laten) erkennen.

Hoe kan een kwalificatie- en certificatiestelsel in Nederland met voldoende relevantie en draagvlak gerealiseerd worden?

In paragraaf 6.3 is een scenario beschreven voor de invoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Om een goede afstemming met de beroepspraktijk te krijgen ligt de trekkersrol voor dit scenario bij voorkeur bij één of meer van de beroepsorganisaties. Het meest voor de hand ligt de PvIB (Platform voor Informatiebeveiliging), al dan niet met één of meer van de andere beroepsorganisaties (zie bijlage E).

De certificatie-instantie is bij voorkeur een onafhankelijke organisatie die daarvoor door de beroepsorganisaties is opgezet, of aangewezen. De certificatie-instantie kan al dan niet geaccredi-

teerd zijn. De niet-geaccrediteerde instantie scoort qua kosten beter en heeft daarom voor-alsnog de voorkeur.

Hoe zijn het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers te realiseren?

De ontwikkeling van een kwalificatie- en certificatiestelsel voor informatiebeveiligers zal vooral getrokken moeten worden door één of meer van de beroepsorganisaties. Wie het beheer ervan op zich kan nemen is nog geen uitgemaakte zaak. Er zijn weliswaar partijen genoemd die het beheer op zich zouden kunnen nemen, maar er is nog geen uitsluitsel of dat ook gerealiseerd kan worden. Bovendien is er nog geen goed financieel plaatje voor het kwalificatie- en certificatiestelsel beschikbaar.

Aanbevelingen ten behoeve van het binnen afzienbare termijn realiseren van een kwalificatie- en certificatiestelsel voor informatiebeveiligers:

- Het mobiliseren van de beroepsorganisatie PvIB om gezamenlijk met de andere beroepsorganisaties (zie bijlage E) de taakverdeling te bepalen voor het ontwikkelen van een kwalificatie- en certificatiestelsel voor informatiebeveiligers.
- Het opstellen van een financieel overzicht voor een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Hierin wordt ook aangegeven wat de eenmalige en jaarlijkse kosten zijn voor degenen die van de kwalificatie- en certificatiediensten gebruik gaan maken. Hierbij valt te denken aan een jaarlijkse bijdrage van € 50 tot € 150, plus de kosten van eventuele examens. Bovendien maakt het financieel overzicht duidelijk in hoeverre formele accreditatie van de certificatie-instantie qua kosten wellicht toch haalbaar is.
- Het onderzoeken of subsidie verkregen kan worden voor het opzetten van een kwalificatie- en certificatiestelsel voor informatiebeveiligers en de daarvoor benodigde onderzoeksstappen.
- Het onderzoeken welke partij(en) het beheer en de uitvoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers op zich kunnen nemen. De te selecteren partij(en) moeten voldoende garanties kunnen bieden met betrekking tot de continuïteit van het kwalificatie- en certificatiestelsel.
- Het uitwerken van een kwalificatie- en certificatiestelsel voor informatiebeveiligers volgens het scenario dat beschreven is in paragraaf 6.3. Onderdeel hiervan is het door de beroepsorganisaties en andere stakeholders (werkgevers, opleidingsinstellingen en betrokken ministeries) uitwerken van de benodigde beroeps- en opleidingsprofielen en de toelatingseisen voor de huidige professionals. Tevens dienen de relevante bestaande kwalificaties en certificaten, ook uit het buitenland, te worden geïnventariseerd en ‘gemapt’ op de kwalificatie- en certificatieschema’s.
- Het inventariseren van relevante kwalificatie- en certificatiestelsels in het buitenland, om daar zo goed mogelijk op aan te kunnen sluiten en in een later stadium wederzijdse erkenning van kwalificaties en certificaten mogelijk te maken.

1. Inleiding

1.1 Aanleiding

Informatie speelt een belangrijke rol in de samenleving. Onze economie en onze maatschappij moeten kunnen vertrouwen op het juist functioneren van de informatievoorziening. Gelet op de groeiende economische en maatschappelijke belangen en de toenemende afhankelijkheid van informatie, wordt het steeds belangrijker dat informatiebeveiligers een herkenbaar en erkend niveau van vakbekwaamheid hebben dat toepasbaar is in alle sectoren van de samenleving. VNO-NCW heeft via de commissie Informatiebeveiliging de behoefte aan gekwalificeerde informatiebeveiligers verwoord in een position paper. Dat is voor CPNI.NL (voorheen NICC) aanleiding geweest om een onderzoek te starten naar de wenselijkheid en haalbaarheid van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Dit rapport beschrijft de resultaten van het onderzoek.

1.2 Probleemstelling

Organisaties die informatiebeveiligers willen aanstellen, kunnen door de verscheidenheid aan opleidingen, certificaten en titels op het gebied van informatiebeveiliging 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 aangepakt kunnen worden.

Dit wordt vooral veroorzaakt doordat het initiële en post-initiële middelbaar en hoger onderwijs in Nederland de eindtermen van de opleidingen op het gebied van informatiebeveiliging nauwelijks gestandaardiseerd en geharmoniseerd heeft. Daardoor is het onduidelijk in hoeverre verschillende opleidingen met elkaar te vergelijken zijn en welke opleidingen in het kader van doorstroming goed op elkaar aansluiten.

Daarnaast geven zowel opleidingsinstellingen 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 enerzijds bedrijven en overheidsorganisaties die werken met informatiebeveiligers en anderzijds de aanbieders van onderwijs op het gebied van informatiebeveiliging.

1.3 Doelstelling en afbakening

Het primaire doel van dit onderzoek is in beeld te krijgen in hoeverre de relevante spelers en stakeholders in Nederland het nuttig en haalbaar vinden om een kwalificatie- en certificatiestel-

sel voor informatiebeveiligers in Nederland in te voeren. Als er voldoende draagvlak lijkt te zijn voor een dergelijk stelsel, dan is het secundaire doel van het onderzoek om te komen tot een voorstel voor een dergelijk stelsel en te inventariseren hoe het beheer en de bekostiging ervan te realiseren zijn.

De onderzoeksvragen voor dit onderzoek zijn:

- Is het nuttig en haalbaar om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren?
- Hoe kan een kwalificatie- en certificatiestelsel in Nederland met voldoende relevantie en draagvlak gerealiseerd worden?
- Hoe zijn het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers te realiseren?

Het onderzoek betreft de volle breedte van het vakgebied informatiebeveiliging. Het beperkt 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.

In het onderzoek wordt gekeken welke relevante kwalificaties en certificaten in het binnen- en buitenland in omloop zijn (zoals van EXIN, $(ISC)^2$ en ISACA) en in welke mate een Nederlands kwalificatie- en certificatiestelsel hierop kan aansluiten, of de best practice ervan kan gebruiken.

1.4 Aanpak en organisatie

Voor het onderzoek is de volgende aanpak gevolgd:

- Het formuleren van de vragen die aan de te interviewen personen voorgelegd zouden worden (zie bijlage A).
- Het selecteren van de te interviewen personen (zie bijlage B). Deze personen zijn gekozen uit de volgende groepen:
    - Werkgevers (publiek, privaat en specialistische organisaties).
    - Opleidingsinstellingen.
    - Specialisten.
    - Certificatie-instanties.
- Desk research. Onderzoek naar achtergronden van kwalificatie en certificatie, bestaande kwalificatie en certificatie op het gebied van informatiebeveiliging en ervaring met kwalificatie en certificatie bij verschillend beroepen buiten de informatiebeveiliging.
- Veldonderzoek, met onder meer interviews onder werkgevers, opleidingsinstellingen, informatiebeveiligingsspecialisten en certificatie-instanties. Van ieder interview is een beknopt verslag gemaakt voor gebruik binnen het onderzoeksteam. De verslagen zijn gebruikt voor de analyse, maar zijn niet opgenomen in deze rapportage. Naast de interviews zijn een enquête en een workshop gehouden over de wenselijkheid en haalbaarheid van een kwalificatie- en certificatiestelsel voor informatiebeveiligers.
- De analyse. Op basis van de desk research, het veldonderzoek, de tijdens het onderzoek verkregen documentatie (zie bijlage C), alsmede naspeuring door de onderzoe-

kers, is bepaald in hoeverre kwalificatie en certificatie tot de mogelijkheden behoort en welke scenario's daarbij gevolgd kunnen worden.
Aangezien de analyse voor een aanzienlijk deel stoelt op meningen uit interviews, een enquête en een workshop, geeft het resultaat vooral een indicatief beeld van hoe de beroepsgroep van informatiebeveiligers en de andere stakeholders tegen kwalificatie en certificatie van informatiebeveiligers aankijken.

- Het presenteren van de onderzoeksresultaten tijdens een bijeenkomst van de commissie Informatiebeveiliging van VNO-NCW op 18 februari 2011 om de noodzaak en de uitvoering van de voorgestelde aanpak voor kwalificatie en certificatie toe te lichten.
- Het opstellen van het voorliggende rapport.

Het onderzoek is in opdracht van mw. A. Zielstra, Director CPNI.NL, uitgevoerd in de periode september 2010 – februari 2011 door adviseurs van Het Expertise Centrum (HEC) te Den Haag en Verdonck, Klooster & Associates (VKA) te Zoetermeer.

Om de aanpak van het onderzoek te begeleiden en de weergave van de resultaten kritisch te beoordelen is een klankbordgroep ingesteld. De leden hiervan zijn vermeld in bijlage D.

2. Desk research

Dit hoofdstuk bevat de bevindingen van de desk research die is uitgevoerd naar kwalificatie en certificatie van informatiebeveiligers. Allereerst gaan we in paragraaf 2.1 in op het vakgebied informatiebeveiliging. Vervolgens gaan we in paragraaf 2.2 in op de begrippen kwalificatie, certificatie en accreditatie en in paragraaf 2.3 op certificatieschema en instanties voor persoonscertificatie. In paragraaf 2.4 beschrijven we de certificatie van enkele beroepen buiten de informatiebeveiliging, in paragraaf 2.5 geven we enkele kenmerken van gecertificeerde beroepen en in paragraaf 2.6 bespreken we certificatie van informatiebeveiligers. Ten slotte geven we in paragraaf 2.7 de conclusies uit dit hoofdstuk.

2.1 Informatiebeveiliging

Informatiebeveiliging wordt gedefinieerd als het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening te waarborgen.[1]

In de praktijk komen twee interpretaties van informatiebeveiliging voor. In de eerste is informatiebeveiliging het proces dat zich richt op het waarborgen van de betrouwbaarheid van de informatievoorziening. In de tweede beperkt informatiebeveiliging zich tot het ontwerpen en implementeren van ICT-beveiligingsmaatregelen. In het kader van opleidingen op het gebied van informatiebeveiliging en het aannemen van medewerkers op informatiebeveiligingsfuncties zijn beide interpretaties relevant.

Het ligt dan ook voor de hand om binnen het gebied informatiebeveiliging twee domeinen te hanteren die ieder één van de hiervoor geschetste interpretaties van informatiebeveiliging afdekken. We noemen deze domeinen informatierisicomanagement en ICT-beveiliging:

- *Informatierisicomanagement* (information risk management, IRM) omvat het gehele proces om een betrouwbare informatievoorziening te waarborgen. Dit proces heeft een tamelijk brede scope waar informatievoorziening, informatiebeveiliging en risicomanagement als een integraal geheel beschouwd worden. In de praktijk werken hierin vooral generalisten.
- *ICT-beveiliging* (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.

Zowel voor informatierisicomanagement als ICT-beveiliging is het nuttig om onderscheid te maken tussen strategisch, tactisch en operationeel niveau. Informatierisicomanagement speelt

[1] Overbeek e.a., *Informatiebeveiliging onder controle*, Pearson Education, Amsterdam, 2005.

vooral op strategisch en tactisch niveau. Binnen informatierisicomanagement wordt informatiebeveiliging, of risicomanagement, benaderd als een integraal vak, dat de verschillende onderdelen van informatiebeveiliging met elkaar integreert, maar zelf ook een geïntegreerd onderdeel is van een organisatie. ICT-beveiliging speelt zowel op alle strategisch, tactisch als operationeel niveau. Binnen ICT-beveiliging zijn vooral specialisten nodig.

2.2 Kwalificatie, certificatie en accreditatie

2.2.1 Kwalificatie

Kwalificatie is een formeel resultaat van een beoordelings- en validatieproces, dat wordt verworven wanneer een bevoegde instantie bepaalt dat de capaciteiten van een product, dienst, of persoon aan bepaalde eisen beantwoorden.
In dit rapport heeft kwalificatie betrekking op de capaciteiten van personen. Kwalificatie van personen kan plaatsvinden volgens diverse normen of codes. Het beoordelings- en validatieproces is in het algemeen gebaseerd op toetsing door middel van een examen, of het beoordelen van een portfolio.

2.2.2 Certificatie

Zowel nationaal als internationaal hebben afnemers behoefte aan zekerheid over de kwaliteit van geleverde producten, diensten, of personen. Certificatie kan deze zekerheid geven.
Certificatie is een procedure waarbij een onpartijdige, competente en daartoe bevoegde organisatie een document (certificaat) afgeeft als officiële verklaring dat een product, dienst, of persoon aan specifieke eisen voldoet.
De organisatie die een certificaat afgeeft is een certificatie-instantie. Zij baseert haar beslissing om het certificaat af te geven op een eisenstellend document, oftewel een norm. Bij een positieve beoordeling verstrekt de certificatie-instantie het certificaat, oftewel een conformiteitsverklaring van het betreffende product, de dienst, of de persoon.
In dit rapport heeft certificatie betrekking op personen, of specifieker geformuleerd: de vakbekwaamheid van personen. De vakbekwaamheid van een persoon wordt dan beoordeeld door een certificatie-instantie. Bij een positieve beoordeling verstrekt de certificatie-instantie een certificaat van vakbekwaamheid. Dit wordt ook wel een persoonscertificaat genoemd.
Er kunnen voorwaarden verbonden zijn aan een persoonscertificaat, bijvoorbeeld bijscholingsverplichting. Bovendien heeft een certificaat in het algemeen een beperkte geldigheidsduur. Na het verstrijken van de geldigheidsduur kan het certificaat meestal verlengd worden na hernieuwde en positieve beoordeling.

2.2.3 Accreditatie

De onpartijdigheid en competentie van een certificatie-instantie zijn niet vanzelfsprekend. Dit moet worden geborgd door een organisatie die toezicht houdt op de certificatie-instantie, een zogenaamde accreditatieorganisatie. Een accreditatieorganisatie beoordeelt op regelmatige basis zowel de onpartijdigheid en competentie van de certificatie-instantie, als het managementsysteem dat gebruikt wordt.

In Nederland zijn verscheidene accreditatieorganisaties. De overheid heeft voor het publieke domein de Raad van Accreditatie (RvA) aangewezen als de centrale accreditatieorganisatie, maar maakt desalniettemin zelf ook gebruik van andere accreditatieorganisaties, zoals de Nederlands-Vlaamse Acceditatieorganisatie (NVAO) voor opleidingen in het hoger onderwijs.
In Europa is de European co-operation for Accreditation (EA) opgericht door de Europese Commissie als de officiële Europese accreditatie-infrastructuur. EA is het Europese netwerk van nationaal erkende accreditatieorganisaties. De Nederlandse Raad van Accreditatie is lid van de EA, maar vertegenwoordigt daarin niet de andere Nederlandse accreditatieorganisaties.

2.3 Certificatieschema en instanties voor persoonscertificatie

2.3.1 Certificatieschema

Een certificatie-instantie, die de vakbekwaamheid van een persoon beoordeelt op basis van een gegeven norm, gebruikt voor het certificatieproces bepaalde criteria en procedures. Deze worden tezamen het certificatieschema genoemd.
Als meerdere certificatie-instanties dezelfde norm als basis voor de beoordeling gebruiken, maar verschillende certificatieschema's, dan kan dit leiden tot verschillende beoordelingen. Daarom is het gebruikelijk dat verschillende certificatie-instanties niet alleen dezelfde norm gebruiken, maar ook een uniform certificatieschema. In dat geval beoordelen alle betrokken certificatie-instanties de vakbekwaamheid van personen aan de hand van dezelfde norm en dezelfde criteria en procedures.

2.3.2 ISO/IEC 17024

Een certificatie-instantie voor persoonscertificatie kan haar certificatieschema desgewenst conformeren aan de standaard ISO/IEC 17024: 2003, Conformity assessment – General requirements for bodies operating certification of persons. Deze standaard specificeert de eisen die zeker stellen dat certificatie-instanties hun certificatieschema's voor persoonscertificatie op een consistente, vergelijkbare en betrouwbare manier uitvoeren, met gebruikmaking van objectieve criteria voor competenties en waardering, teneinde onpartijdigheid van de uitvoering zeker te stellen en belangenconflicten te vermijden. De eisen hebben onder meer betrekking op de structuur en de besturing van de certificatie-instantie en de kenmerken van het certificatieproces.

2.3.3 Certificatie-instanties in Nederland

Certificatie-instanties die in Nederland personen op basis van de norm ISO/IEC 17024 kunnen certificeren, zijn bijvoorbeeld:

- DNV (Det Norske Veritas).
- DEKRA (samen met KEMA Quality).
- LRQA (Lloyds Register Quality Assurance).
- Certiked (onderdeel van Lloyds Register Group).

2.3.4 Grandfathering

Een certificatieschema kan wellicht na het lanceren moeilijk van de grond komen. In het begin heeft namelijk vrijwel niemand het betreffende certificaat, waardoor het certificaat weinig bekendheid geniet en weinigen moeite willen doen om het certificaat te behalen. Dit is een vicieuze cirkel. Om dat te doorbreken kan grandfathering worden toegepast.
Grandfathering is het voor bepaalde tijd en/of bepaalde groep laten gelden van de oude regelgeving, terwijl voor alle andere gevallen de nieuwe regelgeving van toepassing is.
Bij het invoeren van een certificatieschema kan grandfathering gebruikt worden om de huidige professionals conform de bestaande situatie, dus met geen of marginale toetsing, toe te laten, terwijl voor alle toekomstige professionals wel de toetsing conform het certificatieschema geldt. Hierdoor ontstaat relatief snel een kritische massa aan gecertificeerden. Het nadeel is echter dat het certificaat een tijd lang van weinig waarde is. Het kan jaren duren voordat het negatieve imago opgekrikt is en er voldoende aanwas is volgens de ‘gewone’ certificatie.

2.4 Certificatie van verschillende beroepen

Er zijn in Nederland veel beroepen waarvoor personen zich kunnen certificeren. Veelal zijn de normen hiervoor gedefinieerd door een beroepsorganisatie. Voor sommige beroepen, zoals accountant, ligt hieraan een wettelijk kader ten grondslag. Voor een aantal beroepen, zoals lasser, werkt de certificatie-instantie conform de norm ISO/IEC 17024.

Om te onderzoeken of ook voor de beroepen binnen de informatiebeveiliging certificatie een reële mogelijkheid is, is gekeken naar de ervaring met certificatie bij een aantal beroepen buiten de informatiebeveiliging. Er is vooral gekeken naar hoe men daarbij omgaat met kwalificatie en certificatie van de professionals. De selectie van deze voorbeeldberoepen is gedaan op grond van:

- De relatie met het vakgebied informatiebeveiliging.
- Het maatschappelijk aanzien van de beroepsgroep.
- Het maatschappelijk vertrouwen ten aanzien van de beroepsgroep.
- Langdurige ervaring met een kwalificatie- en certificatieschema.

Op basis van deze criteria hebben we de volgende beroepen geselecteerd:

- Accountant.
- IT-auditor.
- Beroepen in de beveiligingsbranche.
- Beroepen in de gezondheidszorg.
- Tandarts.
- Advocaat.
- Ingenieur.
- Technisch personeel luchtvaart.

In bijlage I is de wijze waarop binnen deze beroepen met kwalificatie en certificatie gewerkt wordt beknopt beschreven.

2.5 Kenmerken van gecertificeerde beroepen

Uit het beschouwen van de kwalificatie en certificatie van de in de vorige paragraaf genoemde beroepen volgt dat in alle gevallen een aantal kenmerken aanwezig is:

- Er is een beroepsprofiel.
- Er is een onafhankelijke certificatie-instantie.
- Er is een certificatieregister.
- Er zijn opleidingen.
- Er zijn gedrag- en beroepsregels.
- Er zijn eisen voor bij- en nascholing.
- Er is tuchtrecht.

In de volgende subparagrafen worden deze kenmerken verder uitgewerkt.

2.5.1 Beroepsprofiel

Om tot kwalificatie en certificatie van een professional in de informatiebeveiliging te komen, is het noodzakelijk dat het beroep duidelijk beschreven is, alsook de eisen die aan de beroepsbeoefenaar gesteld worden. Dit wordt het beroepsprofiel genoemd. Binnen de beroepsgroep moet consensus bestaan over de toepasbaarheid van het beroepsprofiel.

Het beroepsprofiel bevat:

- De taken die de beroepsbeoefenaar moet kunnen uitvoeren.
- De competenties (kennis, inzicht, vaardigheden en houding) die de beroepsbeoefenaar moet bezitten.

2.5.2 Onafhankelijke certificatie-instantie

Als een beroepsgroep met certificatie werkt dan wordt dat gedaan door een certificatie-instantie die daarvoor door de beroepsgroep of de overheid is aangewezen. In verscheidene gevallen is dat de beroepsorganisatie, in andere gevallen een derde partij, bijvoorbeeld een gespecialiseerde certificatie-instantie.

De certificatie-instantie werkt met een kwalificatie- en certificatieschema.[2] Het schema beschrijft de volgende zaken:

- De objectief meetbare criteria waaraan de beroepsbeoefenaar moet voldoen.
- Het beoordelingsproces.
- De beoordelingsinstrumenten waarmee men bepaalt of aan de criteria voldaan wordt.
- De klachtenregeling.
- De tuchtregeling.

[2] Het kwalificatie- en certificatieschema kan opgezet zijn en beheerd worden door de certificatie-instantie, of door een andere partij, bijvoorbeeld een beroepsorganisatie.

De certificatie-instantie moet onafhankelijk en competent zijn. Als de certificatie-instantie werkt conform ISO/IEC 17024 dan moet de certificatie-instantie geaccrediteerd worden. Een certificatie-instantie kan ook andere redenen hebben, bijvoorbeeld imago, om zich te laten accrediteren.

2.5.3 Certificatieregister

Het opnemen van een beroepbeoefenaar in een centraal certificatieregister verleent duidelijkheid over de status van de betreffende beroepsbeoefenaar. Als een beroepsbeoefenaar zich voor een bepaald beroep kan laten certificeren, dan houdt de certificatie-instantie daarvan een register bij.

In een certificatieregister voor een bepaald beroep staan alle voor dat beroep gecertificeerde beroepsbeoefenaren. De informatie in het register wordt regelmatig bijgewerkt, bijvoorbeeld elke 24 uur. Een certificatieregister kan besloten of publiek zijn. Per geregistreerde persoon is slechts beperkte informatie opgenomen omwille van privacy. Iedere geregistreerde persoon kan een uittreksel uit het register aanvragen. Veelal kunnen derden dat ook, zodat door middel van het register duidelijk gemaakt kan worden wie een voor het betreffende beroep gekwalificeerde en gecertificeerde beroepsbeoefenaar is.

2.5.4 Opleidingen

Voor vrijwel alle gecertificeerde beroepen geldt dat een bepaalde opleiding gevraagd wordt. Deze moet goed toegankelijk zijn voor de beoogde beroepsbeoefenaren. Zo is het meestal noodzakelijk dat de betreffende opleiding regelmatig en op verschillende locaties in Nederland aangeboden wordt. Daarnaast moeten de instellingen die de opleiding bieden een uniform eindniveau halen, waarmee de beoogde beroepsbeoefenaar zich kwalificeert voor inschrijving in het beroepsregister. De opleidingen die hieraan voldoen, worden erkend voor de betreffende certificatie. Voor sommige gecertificeerde beroepen vindt de erkenning van de opleidingen plaats door de certificatie-instantie. Periodiek vindt een evaluatie plaats in het kader van het toezicht op de opleidingen. De normen en regels voor erkenning zijn vastgesteld in een Reglement van Toelating.

In veel gevallen kan met een bewijs van ‘vergelijkbare kennis en ervaring’ vrijstelling verkregen worden voor de gespecificeerde opleiding. Dit is onder meer nuttig als de gespecificeerde opleiding nog niet zo lang aangeboden wordt dat iedere beroepsbeoefenaar de opleiding heeft kunnen volgen.

2.5.5 Gedrag- en beroepsregels

Gecertificeerde beroepsbeoefenaren zijn gebonden aan gedrag- en beroepsregels. Deze regels bieden een leidraad voor het handelen van de beroepsbeoefenaar. In de gedrag- en beroepsregels zijn de fundamentele beginselen vastgelegd waaraan de beroepsbeoefenaar zich moet houden, bijvoorbeeld onafhankelijkheid en integriteit.

2.5.6 Eisen voor bij- en nascholing

Voor het op peil houden van kennis en vaardigheden wordt van een professional verwacht dat hij of zij vakinhoudelijk bij blijft. Dit kan gerealiseerd worden door onder meer werkervaring, het volgen van seminars en vakmatige bij- en nascholing. De regels hiervoor variëren sterk over de verschillende beroepen, zowel qua vorm als omvang.

2.5.7 Tuchtrecht

Gecertificeerde beroepsbeoefenaren zijn gebonden aan gedrag- en beroepsregels. Beroepsbeoefenaren die zich niet aan de regels voor hun beroep houden, moeten aan represailles kunnen worden onderworpen. Daarvoor is onafhankelijk tuchtrecht door een Raad van Tucht nodig.

Een Raad van Tucht is belast met de behandeling van klachten die tegen gecertificeerde beroepsbeoefenaren zijn ingediend. Veelal wordt vereist dat een klacht alleen betrekking kan hebben op het beroepsmatig handelen door de aangeklaagde beroepsbeoefenaar in strijd met de beroepsmatige gedragsregels. Een Raad van Tucht kan bijvoorbeeld de volgende sancties opleggen:

- Schriftelijke waarschuwing.
- Schriftelijke berisping.
- Schorsing voor bepaalde tijd.
- Ontzetting uit de beroepsgroep.

2.6 Certificatie van informatiebeveiligers

In het vakgebied bestaan veel mogelijkheden om certificaten te behalen. Veel certificaten geven het recht (eventueel met aanvullende eisen voor praktijkervaring) een titel achter de naam te zetten. Voorbeelden van titels zijn: ABCP, CAP, CBCP, CEH, CGEIT, CIA, CIPP, CISA, CISM, CISSP, CITP, CRISC, CSSLP, FBCI, FBCS, ISMAS, ISMES, ISSAP, ISSEP, ISSMP, MBCP, MISM, MSIT, OPSA, OPST, QiCA, RE, RIB, RO, RSE, SSCP, et cetera. De volledige namen van de hier genoemde (afgekorte) titels zijn vermeld in bijlage M. Een business card kan bijvoorbeeld de volgende naam tonen: “Piet Pietersen CISSP CISA QiCA CITP FBCS”. Vooral de laatste jaren komt het steeds meer in opgang om alle verworven titels op de business card te vermelden.

Door de grote verscheidenheid aan certificaten is het inschatten van de betekenis en waarde ervan tamelijk lastig. Aangezien de eindtermen van de cursussen en opleidingen onder de verschillende certificaten en titels nauwelijks gestandaardiseerd en geharmoniseerd zijn, is het onduidelijk wat de behaalde cursussen en opleidingen inhouden en hoeveel aanvullende praktijkervaring iemand heeft. Bovendien is het onduidelijk hoe termen als ‘R(egister)’, ‘C(ertified)’, ‘M(aster)’, ‘A(ssociate)’ en ‘F(ellow)’ zich tot elkaar verhouden. Kortom, binnen het vakgebied informatiebeveiliging is geen transparantie over de betekenis en kwaliteit van certificaten.

Om binnen het vakgebied informatiebeveiliging te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de samenleving, is het nodig om een uniform kwalificatie- en certificatiestelsel op te zetten. De voordelen hiervan zijn:

- Organisaties kunnen op basis van behaalde kwalificaties en certificaten beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties.
- De aanbieders van onderwijs kunnen de gedefinieerde kwalificatie- en certificatieniveaus gebruiken om hun opleidingen op af te stemmen.
- Professionals kunnen met erkende kwalificaties en certificaten eenvoudiger aantonen welke specifieke competenties ze met betrekking tot informatiebeveiliging hebben.

ENISA (European Network and Information Security Agency, agentschap van de Europese Unie) onderkent in haar rapport “Information Security Certifications” het belang van kwalificatie en certificatie van informatiebeveiligingsprofessionals. ENISA geeft daarbij de volgende aanbevelingen:

- Overheid en bedrijfsleven moeten de ontwikkeling aanmoedigen van kwalificatie- en certificatieschema’s voor professionals.
- Organisaties moeten hun informatiebeveiligingsprofessionals aanmoedigen om één of meer geschikte certificaten voor informatiebeveiliging te behalen.
- De instanties die kwalificeren en certificeren moeten meer aandacht besteden aan het versterken van de relaties met opleidingen en opleidingsinstellingen.
- Kwalificatie- en certificatieschema’s voor informatiebeveiligers moeten bij voorkeur uitgevoerd worden door geaccrediteerde instanties.

ENISA waarschuwt dat men in Europese landen voorzichtig moet zijn met het aansluiten op, of adopteren van, Amerikaanse kwalificatie- en certificatieschema’s. De Amerikaanse schema’s zijn op Amerikaanse leest geschoeid en benaderen bijvoorbeeld privacy anders dan we in Europese landen gewoon zijn.

2.7 Conclusies

Er zijn in Nederland veel beroepen waarvoor personen zich kunnen certificeren. Veelal zijn de normen hiervoor gedefinieerd door een beroepsorganisatie. Voor sommige beroepen, ligt hieraan een wettelijk kader ten grondslag. Voor een aantal beroepen werkt de certificatie-instantie conform de norm ISO/IEC 17024.

Om met kwalificatie en certificatie te kunnen werken, moet een aantal kenmerken aanwezig zijn:

- Er is een beroepsprofiel.
- Er is een onafhankelijk certificatie-instantie.
- Er is een certificatieregister.
- Er zijn opleidingen.
- Er zijn gedrag- en beroepsregels.
- Er zijn eisen voor bij- en nascholing.
- Er is een Raad van Tucht.

Binnen het vakgebied informatiebeveiliging bestaat een chaotische situatie met betrekking tot kwalificatie en certificatie van professionals. Om binnen het vakgebied te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de samenleving, is het nodig om een uniform kwalificatie- en certificatiestelsel op te zetten. De voordelen hiervan zijn:

- Organisaties kunnen op basis van behaalde kwalificaties en certificaten beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties.
- De aanbieders van onderwijs kunnen de gedefinieerde kwalificatie- en certificatieniveaus gebruiken om hun opleidingen op af te stemmen.
- Professionals kunnen met erkende kwalificaties en certificaten eenvoudiger aantonen welke specifieke competenties ze met betrekking tot informatiebeveiliging hebben.

Daarmee kunnen we de eerste onderzoeksvraag deels beantwoorden, namelijk dat het nuttig is om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren.

Ervaring van andere beroepen leert dat een kwalificatie- en certificatiestelsel in principe ook haalbaar zou moeten zijn, maar dat hangt ook van andere aspecten af, zoals aantallen en draagvlak.

3. Veldonderzoek

In het verlengde van de desk research is een veldonderzoek uitgevoerd. Het doel hiervan was drieledig:

- Nagaan of het nut van kwalificatie en certificatie dat uit de desk research bleek ook daadwerkelijk binnen de beroepsgroep ervaren wordt.
- Nagaan of een kwalificatie- en certificatiestelsel voor informatiebeveiligers haalbaar kan zijn en op een breed draagvlak kan rekenen.
- Nagaan welke partijen verantwoordelijk zouden kunnen of moeten zijn voor de ontwikkeling, het beheer en de bekostiging van een kwalificatie- en certificatiestelsel.

Dit hoofdstuk bevat de bevindingen van het veldonderzoek ten aanzien van de bovenstaande doelen. Hiervoor zijn interviews gehouden met werkgevers, opleidingsinstellingen, specialisten en certificatie-instanties. Bovendien zijn tijdens het GOVCERT.NL symposium in november 2010 met een groep vooraanstaande informatiebeveiligers een workshop en een enquête gehouden over kwalificatie en certificatie van informatiebeveiligers (zie bijlage K).

3.1 Nut van kwalificatie en certificatie

3.1.1 Kwalificatie

Uit de interviews, workshop en enquête blijkt dat binnen de geraadpleegde groep consensus bestaat over het groeiende maatschappelijke en economische belang van informatiebeveiliging en de noodzaak om geen twijfel te laten bestaan over de vakbekwaamheid van haar professionals. Bovendien moeten mensen opgeleid kunnen worden voor de beroepen in het vakgebied informatiebeveiliging. Men gaf aan kwalificatie voor informatiebeveiligers op basis van opleiding en ervaring nuttig te vinden. Ook mw. Kroes, de Europese Commissaris voor ICT en Telecom, gaf in een interview met PvIB (Platform voor Informatiebeveiliging) aan dat zij kwalificatie belangrijk vindt (zie bijlage J). Ten slotte geeft ook de nationale overheid in de Nationale Cyber Security Strategie (NCSS) aan: "Versterking van scholing op alle niveaus is noodzakelijk om weerstand te kunnen blijven bieden aan dreigingen en betrouwbare ICT te kunnen blijven maken en is een voorwaarde voor de groei van de digitale economie in Nederland."

Het onderscheid tussen enerzijds informatierisicomanagement en ICT-beveiliging en anderzijds verschillende niveaus (strategisch, tactisch en operationeel) werd door vrijwel alle geraadpleegde personen als zinvol gezien.

Een minderheid van de geraadpleegde personen gaf aan tevreden te zijn met bestaande kwalificaties, zoals CISSP, CISA, CISM, MISM of MSIT, maar was onderling verdeeld over welke hiervan de voorkeur hebben. Het merendeel vond dat van de bestaande kwalificaties niet zonder meer duidelijk is of ze voldoen en dat een nieuw uniform kwalificatiestelsel voor informatiebeveiliging nodig is. Men vond dat de genoemde kwalificaties an andere relevante bestaande

kwalificaties daarin meegenomen moeten worden. Door ook buitenlandse kwalificaties mee te nemen, ontstaat aansluiting met buitenlandse kwalificatiestelsels. Mw. Kroes benadrukte dat zij het belangrijk vindt om nationale kwalificaties internationaal te (laten) erkennen (zie bijlage J).

In aanvulling op het voorgaande werd verscheidene keren aangegeven dat controle van de kwaliteit een belangrijk element in het benodigde kwalificatiestelsel moet zijn. Zo kan bijvoorbeeld gewerkt worden met centrale accreditatie van de opleidingen voor informatiebeveiliger.

Het aantal personen dat onder een nieuw kwalificatiestelsel voor informatiebeveiligers gekwalificeerd zal gaan worden en het aantal opleidingen dat daarvoor nodig is, almede de omvang ervan, is moeilijk te bepalen. Verscheidene organisaties gaven aan dat zij behoefte hebben aan gekwalificeerde informatierisicomanagers en ICT-beveiligers, maar vooral de opleidingsinstellingen hebben door marktonderzoek onderbouwde aantallen nodig.

3.1.2 Certificatie

Met betrekking tot certificatie gaan we in dit onderzoek uit van formele registratie in een certificatieregister op basis van een certificatieschema. Enerzijds werd gesteld dat in de huidige tijdgeest kwalificatie zonder ‘bewijs’, dus zonder certificatieregister, 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. In dat geval is een certificatieregister onontkoombaar. Anderzijds werd gesteld dat het opnemen in een certificatieregister niet in alle organisaties even nodig is. In verscheidene organisaties volstaat het om op basis van een goed CV binnen te komen en vervolgens binnen en buiten de deur kennis en ervaring op te bouwen, zonder dat daarbij certificaten of een register nodig zijn. Daar staat tegenover dat verscheidene groepen organisaties werden genoemd, waaronder financiële instellingen, zorginstellingen, beveiligingsorganisaties en commerciële dienstverleners, waar certificaten en een register wel een rol van betekenis zouden kunnen spelen. Mw. Kroes gaf aan dat zij formele certificatieregister(s) nuttig vindt, maar dat er wel voldoende aandacht besteed moet worden aan uitwisselbaarheid en wederzijdse erkenning van registers in andere landen van de Europese Unie.

Men vond dat een certificatieschema desgewenst meerdere te certificeren niveaus kan onderscheiden, bijvoorbeeld junior, medior en senior. Dit onderscheid kan gebaseerd zijn op ervaring in de beroepspraktijk, zoals in het schema van de Britse IISP, of op basis van opleiding- en/of denkniveau. Als ervaring een rol speelt dan moet deze wel op een valide wijze gemeten worden, dus niet het tellen van gevolgde seminars.

Een punt dat belangrijk gevonden werd, was de reële mogelijkheid tot schrappen uit het register, bijvoorbeeld na wanprestatie. Zonder die mogelijkheid vindt men een register een wassen neus.

Al met al vond een meerderheid van de geraadpleegde personen formele registratie in een certificatieregister nuttig en een enkeling zelfs noodzakelijk. Degenen die het niet direct nuttig of

nodig vonden, waren niet per se tegen. Er lijkt dus een behoorlijk draagvlak voor een certificatieregister te zijn. Uit de gesprekken bleek dat het draagvlak nog vergroot kan worden als met name de overheid certificatieverplichtingen koppelt aan bepaalde beroepen.

3.2 Haalbaarheid van kwalificatie- en certificatiestelsel

Uit de gehouden interviews blijkt dat men in het algemeen vindt dat een kwalificatie- en certificatiestelsel voor informatiebeveiligers haalbaar is. Temeer daar verscheidene beroepen buiten de informatiebeveiliging ook werken met een kwalificatie- en certificatiestelsel (zie bijlage I). Wel wordt een aantal randvoorwaarden voor de haalbaarheid van het kwalificatie- en certificatiestelsel genoemd:

- Er moet voldoende draagvlak voor het stelsel zijn bij de beroepsgroep(en), maar vooral bij de betrokken beroepsorganisaties. Men denkt dat dit goed te organiseren is.
- Er moeten voldoende personen zijn die onder het stelsel gekwalificeerd en gecertificeerd zullen gaan worden. Voor kwalificatie lijkt dit geen probleem te zijn. Voor certificatie is nog niet duidelijk welke aantallen kunnen worden verwacht.
- Er moeten binnen afzienbare tijd voldoende erkende opleidingen beschikbaar komen. Dit is te realiseren mits de opleidingsinstellingen overtuigd zijn van voldoende kandidaten. Vooralsnog lijkt dit geen probleem te vormen.
- Er moet een relevante wijze worden gevonden waarop de huidige professionals zich eenvoudig binnen het stelsel kunnen kwalificeren en certificeren. Hiervoor zouden mogelijkheden tot vrijstelling op basis van eerder verworven competenties in het certificatieschema opgenomen kunnen worden, eventueel te beoordelen door een toetsingscommissie.
- Er moet een vergelijking komen met bekende buitenlandse kwalificaties en certificaten en vergelijkbare buitenlandse kwalificaties en certificaten moeten erkend worden. Men denkt dat dit goed te organiseren is.
- De kosten voor het stelsel moeten beheersbaar blijven. Er is nog onvoldoende duidelijkheid over de kosten voor het stelsel en of deze beheersbaar blijven.
- De continuïteit van het stelsel moet aannemelijk gemaakt worden. Dit hangt af van de organisatie(s) die voor het stelsel verantwoordelijk zullen worden.

Al met al lijkt het merendeel van de geraadpleegde personen het stelsel wel haalbaar te vinden, mits duidelijk wordt dat te kleine aantallen kandidaten en te hoge kosten geen belemmerende factoren zullen zijn.

3.3 Ontwikkeling, beheer en bekostiging van stelsel

Alle geraadpleegde personen die zich over ontwikkeling, beheer en bekostiging uitlieten, waren het erover eens dat de beroepsgroep, of preciezer de beroepsorganisatie(s), de voortrekker moeten zijn voor het realiseren van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Veelal werd expliciet verwezen naar PvIB (Platform voor Informatiebeveiliging), maar dat kan veroorzaakt worden doordat de andere beroepsorganisaties (zie bijlage E) minder op het netvlies van de geraadpleegde personen stonden. Mw. Kroes gaf aan dat zij PvIB de logische

kandidaat vindt om in Nederland een kwalificatie- en certificatiestelsel en het daarbij behorende certificatieregister te realiseren.

Voor de bekostiging van het stelsel werden de volgende mogelijkheden voorgesteld:

- Degenen die opgaan voor kwalificatie of certificatie kunnen daarvoor een kostendekkende eigen bijdrage betalen. Hierbij valt te denken aan een jaarlijkse bijdrage van € 50 tot € 150, plus de kosten van eventuele examens.[3]
- De brancheorganisatie(s) kunnen een eenmalige of jaarlijkse bijdrage doen.
- De overheid kan een (start)subsidie verstrekken.

Het ligt voor de hand om ten minste gebruik te maken van de mogelijkheid van de eigen bijdrage. De andere twee mogelijkheden kunnen de realisatie van het stelsel versnellen en de continuïteit van het stelsel verbeteren, maar het is nog onduidelijk in hoeverre op deze mogelijkheden van bekostiging gerekend kan worden.

3.4 Conclusies

Er blijkt consensus te bestaan over het groeiende belang van informatiebeveiliging en de noodzaak om geen twijfel te laten bestaan over de vakbekwaamheid van haar professionals. Bovendien moeten mensen opgeleid kunnen worden voor de beroepen in het vakgebied informatiebeveiliging. Men gaf aan kwalificatie voor informatiebeveiligers op basis van opleiding en ervaring nuttig te vinden. Men vond dat een nieuw uniform kwalificatie- en certificatiestelsel voor informatiebeveiliging nodig is en dat de relevante bestaande kwalificaties en certificaten, ook uit het buitenland, daarin meegenomen moeten worden. Ook is het van belang om nationale kwalificaties en certificaten internationaal te (laten) erkennen.

Certificatie, oftewel formele registratie in een certificatieregister op basis van een certificatieschema, kan op een tamelijk groot draagvlak rekenen. Desgewenst kan een certificatieschema meerdere te certificeren niveaus onderscheiden, bijvoorbeeld junior, medior en senior. Daarnaast moet er de reële mogelijkheid bestaan om geschrapt te worden 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.

In het algemeen denkt men dat een kwalificatie- en certificatiestelsel voor informatiebeveiligers haalbaar is, mits duidelijk wordt dat te kleine aantallen kandidaten en te hoge kosten geen belemmerende factoren zullen zijn.

Het lijkt duidelijk dat het regelen van de ontwikkeling, het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers door de beroepsorganisatie(s) opgepakt moet worden. Welke van de beroepsorganisaties het stokje op gaat pakken, is nog niet duidelijk. Bovendien is het nog onduidelijk in hoeverre één of meer beroepsorganisaties en/of de overheid een deel van de kosten willen dragen.

[3] Ter vergelijking: voor certificatie CISSP bedragen de jaarlijkse kosten circa € 60, exclusief examens.

Daarmee kunnen we het resterende deel van de eerste onderzoeksvraag beantwoorden, namelijk dat men het erover eens is dat het op het eerste gezicht haalbaar is om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren, maar dat het nog geen uitgemaakte zaak is wie de ontwikkeling, het beheer en de bekostiging ervan gaat c.q. gaan realiseren.

4. Beroepsprofielen

Uit de desk research en het veldonderzoek bleek dat er behoefte bestaat aan, en dat er draagvlak is voor, een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers. Om de tweede onderzoeksvraag, namelijk hoe een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland met voldoende relevantie en draagvlak gerealiseerd kan worden, te kunnen beantwoorden, dienen eerst beroepsprofielen voor informatiebeveiligers opgesteld te worden en vervolgens de daarop gebaseerde opleidingsprofielen. In dit hoofdstuk wordt een aanzet gegeven voor de beroepsprofielen voor informatiebeveiligers. In een later stadium dienen deze beroepsprofielen verder uitgewerkt en getoetst te worden.

4.1 Functies

In de huidige praktijk zijn veel verschillende functies in de informatiebeveiliging te zien. In analogie van de eerder onderscheiden domeinen informatierisicomanagement en ICT-beveiliging, onderscheiden we informatierisicomanagers en ICT-beveiligers. In beide domeinen kunnen in principe functies ingevuld worden op strategisch, tactisch en operationeel niveau. Deze niveaus vergen een denk- en/of opleidingsniveau van respectievelijk WO-niveau, hbo-niveau en mbo-niveau. Dit is samengevat in Tabel 1.

Functieniveau	IRM	ICT-beveiligers
Strategisch	WO	WO
Tactisch	Hbo	Hbo
Operationeel	(Zie tekst)	Mbo

Tabel 1: Denk- en/of opleidingsniveau van informatiebeveiligers.

Aangezien informatierisicomanagement een relatief hoog analytisch vermogen vraagt, ligt het voor de hand dat er geen informatierisicomanagers op operationeel niveau zijn.

Voorbeelden van functies die we in de praktijk tegenkomen zijn genoemd in Tabel 2.

Functieniveau	IRM	ICT-beveiligers
Strategisch (WO-niveau)	– Chief Information Security Officer – Information Risk Manager – Information Security Manager – Senior Information Security Consultant	– IT Security Manager – Senior IT Security consultant – Senior IT Security Specialist
Tactisch (hbo-niveau)	– Information Security Manager – Information Security Officer – Information Security Consultant	– IT Security Officer – IT Security Consultant – IT Security Specialist
Operationeel (mbo-niveau)		– IT Security Officer – IT Security Specialist

Tabel 2: Voorbeelden van functies in de informatiebeveiliging.

4.2 Kerntaken

Hoewel in elk van de functiegroepen (IRM en ICT-beveiligers op strategisch, tactisch en operationeel niveau) verschillende functies met verschillende taken voorkomen, kan voor elke functiegroep wel een aantal kerntaken bepaald worden die in alle functies in de gegeven functiegroep in meerdere of mindere mate voorkomen. In Tabel 3 zijn voor de verschillende functiegroepen kerntaken weergegeven die karakteristiek zijn voor de functies in de betreffende functiegroep.

Naast de genoemde functiegroepen met karakteristieke functies en kerntaken, zijn er functies die zich richten op een beperkt deel van informatierisicomanagement of ICT-beveiliging. Hierbij valt te denken aan functies zoals informatiebeveiligingsarchitect, digitaal forensisch onderzoeker en cryptoloog. Dergelijke specialistische functies hebben eigen beroepsprofielen, waar we hier niet verder op in zullen gaan.

Functieniveau	IRM	ICT-beveiligers
Strategisch (WO-niveau)	– Inrichten en integreren van informatierisicomanagement in organisatie – Leiding geven aan informatiebeveiligers – Managen van informatiebeveiligingsprojecten – Opdrachten geven aan en aansturen van externe partijen – Adviseren over informatiebeveiliging – Opstellen van informatiebeveiligingsbeleid – Opstellen van informatiebeveiligingsarchitectuur op hoofdlijnen – Opstellen van bewustwordingscampagnes – Ondersteunen van cultuurverandering – Uitvoeren van informatiebeveiligingsonderzoeken – Audits van informatiebeveiliging	– Leiding geven aan ICT-specialisten – Managen van ICT-beveiligingsprojecten – Opdrachten geven aan en aansturen van externe partijen – Adviseren over ICT-beveiliging – Specificeren van technische maatregelen – Opstellen van ICT-beveiligingsarchitectuur op hoofdlijnen – Adviseren van lijnmanagement over ICT-beveiliging – Uitvoeren van ICT-beveiligingsonderzoeken – Audits van ICT-beveiliging
Tactisch (hbo-niveau)	– Leiding geven aan informatiebeveiligers – Managen van informatiebeveiligingsprojecten – Adviseren over informatiebeveiliging – Opstellen informatiebeveiligingsplan – Ondersteunen bij het opstellen van informatiebeveiligingsarchitectuur – Uitvoeren van risicoanalyses – Uitvoeren van bewustwordingscampagnes – Adviseren van lijnmanagement over informatiebeveiliging – Uitvoeren van informatiebeveiligingsonderzoeken – Audits van informatiebeveiliging	– Adviseren over ICT-beveiliging – Specificeren van technische beveiligingsmaatregelen – Ondersteunen bij het opstellen van ICT-beveiligingsarchitectuur – Implementeren van technische beveiligingsmaatregelen – Uitvoeren van beveiligingstesten – Uitvoeren van ICT-beveiligingsonderzoeken – Audits van ICT-beveiliging
Operationeel (mbo-niveau)		– Implementeren van technische beveiligingsmaatregelen – Uitvoeren van beveiligingstesten – Uitvoeren van ICT-beveiligingsonderzoeken

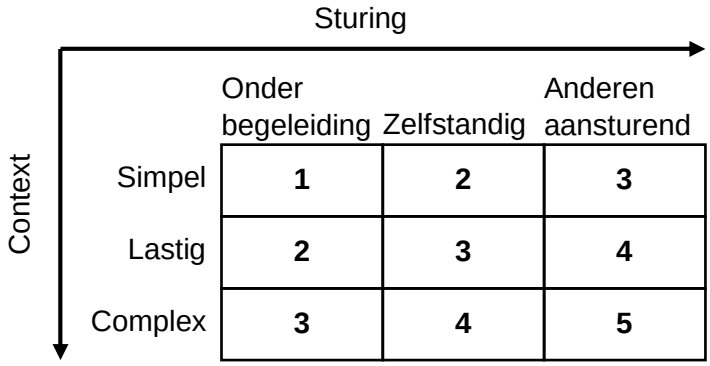
Tabel 3: Kerntaken van de informatierisicomanager en de ICT-beveiliger.

5. Opleidingsprofielen

In het vorige hoofdstuk is een aanzet gegeven voor de beroepsprofielen voor informatiebeveiligers. In dit hoofdstuk wordt een aanzet gegeven voor de daarop gebaseerde opleidingsprofielen. In een later stadium dienen deze opleidingsprofielen verder uitgewerkt en getoetst te worden. De beroeps- en opleidingsprofielen zijn noodzakelijke input voor een kwalificatie- en certificatiestelsel voor informatiebeveiligers.

5.1 Competentieniveaus

Opleidingen richten zich op het verbeteren van competenties, oftewel kennis, inzicht, vaardigheden en houding. De verschillende onderwerpen die in een opleiding aan bod komen hoeven niet allemaal in dezelfde omvang en diepgang te worden behandeld. Op de kernonderwerpen van de opleiding moeten de studenten verder komen dan op de ondersteunende onderwerpen. Om de competenties voor de verschillende onderwerpen goed te kunnen benoemen wordt onderscheid gemaakt in vijf competentieniveaus. Deze hangen af van enerzijds de context waarbinnen de competenties ingezet worden en anderzijds de wijze van sturing die daarbij van toepassing is. Dit wordt toegelicht in Figuur 1.



Figuur 1: Vijf competentieniveaus.

Een mbo-opleiding beoogt een gemiddeld competentieniveau 2 te halen, een hbo-opleiding een gemiddeld competentieniveau 2.5 – 3 en een WO-opleiding een gemiddeld competentieniveau 3 – 3.5.

Op basis van de beroepsprofielen beschreven in hoofdstuk 4, kunnen we de belangrijkste competenties en de bijbehorende competentieniveaus formuleren, de zogenaamde opleidingsprofielen. Deze zijn uitgewerkt in de paragrafen 5.2 en 5.3.

5.2 Informatierisicomanager

5.2.1 Strategisch (WO-niveau)

Uit de kerntaken voor informatierisicomanagers op strategisch niveau, oftewel WO denk- en/of opleidingsniveau (zie Tabel 3) volgen de benodigde competenties. Voor iedere competentie is een schatting gemaakt van het benodigde competentieniveau en is aangegeven wat de belangrijkste onderwerpen zijn die voor het behalen van de betreffende competentie in de opleiding aan bod moeten komen.

Competentie	Niveau	Belangrijkste onderwerpen
Inrichten en integreren van informatierisicomanagement in organisatie	3	Organisatiekunde, risico- en security management, wet- en regelgeving en compliance
Leiding geven aan informatiebeveiligers	3	Leiding geven, organisatiekunde, risico- en security management
Managen van informatiebeveiligingsprojecten	3	Leiding geven, projectmanagement, risico- en security management
Opdrachten geven aan en aansturen van externe partijen	3	Communicatie, samenwerken, financieel management
Adviseren over informatiebeveiliging	4	Presenteren, adviseren, risico- en security management, beveiligingsstandaarden, business continuity management, financieel management, basiskennis ICT
Opstellen van informatiebeveiligingsbeleid	4	Organisatiekunde, wet- en regelgeving en compliance, beveiligingsstandaarden
Opstellen van informatiebeveiligingsarchitectuur op hoofdlijnen	3	Beveiligingsarchitectuur
Opstellen van bewustwordingscampagnes	3	Psychologie, menselijk falen, communicatie
Ondersteunen van cultuurverandering	3	Psychologie, veranderkunde
Uitvoeren van informatiebeveiligingsonderzoeken	4	Analyseren, presenteren, samenwerken, beveiligingsstandaarden, risicoanalyse, wet- en regelgeving en compliance
Audits van informatiebeveiliging	3	Auditen, presenteren, samenwerken, beveiligingsstandaarden

Tabel 4: Belangrijkste onderwerpen in de opleiding voor informatierisicomanagers op strategisch niveau.

5.2.2 Tactisch (hbo-niveau)

Uit de kerntaken voor informatierisicomanagers op tactisch niveau, oftewel hbo denk- en/of opleidingsniveau (zie Tabel 3) volgen de benodigde competenties. Voor iedere competentie is een schatting gemaakt van het benodigde competentieniveau en is aangegeven wat de belangrijk-

ste onderwerpen zijn die voor het behalen van de betreffende competentie in de opleiding aan bod moeten komen.

Competentie	Niveau	Belangrijkste onderwerpen
Leiding geven aan informatiebeveiligers	2.5	Leiding geven, organisatiekunde, risico- en security management
Managen van informatiebeveiligingsprojecten	2.5	Leiding geven, projectmanagement, risico- en security management
Adviseren over informatiebeveiliging	3	Presenteren, adviseren, risico- en security management, beveiligingsstandaarden, basiskennis ICT
Opstellen van informatiebeveiligingsplan	3	Presenteren, beveiligingsstandaarden
Ondersteunen bij het opstellen van informatiebeveiligingsarchitectuur	2.5	Beveiligingsarchitectuur
Uitvoeren van risicoanalyses	3	Risicomanagement, risicoanalyse, analyseren
Uitvoeren van bewustwordingscampagnes	2.5	Psychologie, menselijk falen, communicatie
Adviseren van lijnmanagement over informatiebeveiliging	3	Mondeling presenteren, communicatie, beveiligingsstandaarden
Uitvoeren van informatiebeveiligingsonderzoeken	3	Analyseren, presenteren, samenwerken, beveiligingsstandaarden, risicoanalyse, wet- en regelgeving en compliance
Audits van informatiebeveiliging	2	Auditen, presenteren, samenwerken, beveiligingsstandaarden

Tabel 5: Belangrijkste onderwerpen in de opleiding voor informatierisicomanagers op tactisch niveau.

5.3 ICT-beveiliger

5.3.1 Strategisch (WO-niveau)

Uit de kerntaken voor ICT-beveiligers op strategisch niveau, oftewel WO denk- en/of opleidingsniveau (zie Tabel 3) volgen de benodigde competenties. Voor iedere competentie is een schatting gemaakt van het benodigde competentieniveau en is aangegeven wat de belangrijkste onderwerpen zijn die voor het behalen van de betreffende competentie in de opleiding aan bod moeten komen.

Competentie	Niveau	Belangrijkste onderwerpen
Leiding geven aan ICT-specialisten	2.5	Leiding geven
Managen van ICT-beveiligingsprojecten	3	Leiding geven, projectmanagement, ICT-beveiliging*
Opdrachten geven aan en aansturen van externe partijen	3	Communicatie, samenwerken, financieel management
Adviseren over ICT-beveiliging	4	Presenteren, adviseren, ICT-beveiliging*, financieel management
Specificeren van technische maatregelen	4	ICT-beveiliging*
Opstellen van ICT-beveiligingsarchitectuur op hoofdlijnen	2.5	Beveiligingsarchitectuur
Uitvoeren van ICT-beveiligingsonderzoeken	3	Analyseren, presenteren, samenwerken, ICT-beveiliging*, risicoanalyse, wet- en regelgeving en compliance
Opdrachten geven aan en aansturen van externe partijen	3	Communicatie, samenwerken, financieel management
Audits van ICT-beveiliging	3	Auditen, presenteren, samenwerken, ICT-beveiliging*

* ICT-beveiliging omvat de volgende onderwerpen: ICT, malware- en fraudetechnieken, cryptografie, computer- en netwerkbeveiliging, technische beveiligingsstandaarden.

Tabel 6: Belangrijkste onderwerpen in de opleiding voor ICT-beveiligers op strategisch niveau.

5.3.2 Tactisch (hbo-niveau)

Uit de kerntaken voor ICT-beveiligers op tactisch niveau, oftewel hbo denk- en/of opleidingsniveau (zie Tabel 3) volgen de benodigde competenties. Voor iedere competentie is een schatting gemaakt van het benodigde competentieniveau en is aangegeven wat de belangrijkste onderwerpen zijn die voor het behalen van de betreffende competentie in de opleiding aan bod moeten komen.

Competentie	Niveau	Belangrijkste onderwerpen
Adviseren over ICT-beveiliging	3	Presenteren, adviseren, ICT-beveiliging*
Specificeren van technische beveiligingsmaatregelen	3	ICT-beveiliging*
Ondersteunen bij het opstellen van ICT-beveiligingsarchitectuur	2	Beveiligingsarchitectuur
Implementeren van technische beveiligingsmaatregelen	3	ICT-beveiliging*
Uitvoeren van beveiligingstesten	3	Analyseren, presenteren, samenwerken, ICT-beveiliging*
Uitvoeren van ICT-beveiligingsonderzoeken	2.5	Analyseren, presenteren, samenwerken, ICT-beveiliging*, risicoanalyse
Audits van ICT-beveiliging	2.5	Auditen, presenteren, samenwerken, ICT-beveiliging*

* ICT-beveiliging omvat de volgende onderwerpen: ICT, malware- en fraudetechnieken, cryptografie, computer- en netwerkbeveiliging, technische beveiligingsstandaarden.

Tabel 7: Belangrijkste onderwerpen in de opleiding voor ICT-beveiligers op tactisch niveau.

5.3.3 Operationeel (mbo-niveau)

Uit de kerntaken voor ICT-beveiligers op operationeel niveau, oftewel mbo denk- en/of opleidingsniveau (zie Tabel 3) volgen de benodigde competenties. Voor iedere competentie is een schatting gemaakt van het benodigde competentieniveau en is aangegeven wat de belangrijkste onderwerpen zijn die voor het behalen van de betreffende competentie in de opleiding aan bod moeten komen.

Competentie	Niveau	Belangrijkste onderwerpen
Implementeren van technische beveiligingsmaatregelen	2.5	ICT-beveiliging*
Uitvoeren van beveiligingstesten	2.5	Analyseren, presenteren, samenwerken, ICT-beveiliging*
Uitvoeren van ICT-beveiligingsonderzoeken	2	Analyseren, presenteren, samenwerken, ICT-beveiliging*, risicoanalyse

* ICT-beveiliging omvat de volgende onderwerpen: ICT, malware- en fraudetechnieken, cryptografie, computer- en netwerkbeveiliging, technische beveiligingsstandaarden.

Tabel 8: Belangrijkste onderwerpen in de opleiding voor ICT-beveiligers op operationeel niveau.

5.4 Opleidingsprofielen en opleidingen

De opleidingsprofielen die in de paragrafen 5.2 en 5.3 zijn bepaald, zijn samengevat in Tabel 9. Voor iedere functiegroep is aangegeven wat de belangrijkste onderwerpen zijn die in de opleiding aan bod moeten komen.

Onderwerp \ Opleiding	IRM Strat.	IRM Tact.	ICT-bev. Strat.	ICT-bev. Tact.	ICT-bev. Oper.
Organisatie					
Organisatiekunde	X	X			
Veranderkunde	X				
Projectmanagement	X	X	X		
Beveiligingsarchitectuur	X	X	X	X	
Risico- en security management	X	X			
Risicoanalyse	X	X	X	X	X
Business continuity management	X				
Wet- en regelgeving en compliance	X	X	X		
Financieel management	X		X		
Beveiligingsstandaarden	X	X			
Mens en gedrag					
Psychologie	X	X			
Menselijk falen	X	X			
Communicatie	X	X	X		
Techniek					
Informatietechnologie	X	X	X	X	X
Malware- en fraudetechnieken			X	X	X
Cryptografie			X	X	X
Computer- en netwerkbeveiliging			X	X	X
Softwarebeveiliging			X	X	X
SCADA-beveiliging			X	X	X
Technische beveiligingsstandaarden			X	X	X
Vaardigheden					
Leiding geven	X	X	X		
Samenwerken	X	X	X	X	X
Analyseren	X	X	X	X	X
Presenteren (mondeling, schriftelijk)	X	X	X	X	X
Adviseren	X	X	X	X	
Auditen	X	X	X	X	

Tabel 9: Opleidingsprofielen voor de informatierisicomanager en de ICT-beveiliger.

6. Voorstel voor kwalificatie- en certificatiestelsel

Dit hoofdstuk gaat verder in op de tweede onderzoeksvraag, namelijk hoe een kwalificatie- en certificatiestelsel in Nederland met voldoende relevantie en draagvlak gerealiseerd kan worden, en gaat tevens in op de derde onderzoeksvraag, namelijk hoe het beheer en de bekostiging ervan gerealiseerd kunnen worden.

Een kwalificatie- en certificatiestelsel voor informatiebeveiligers bestaat uit een kwalificatiedeel en een certificatiedeel. Eerst gaan we in paragraaf 6.1 in op kwalificatie van informatiebeveiligers, waarna we in paragraaf 6.2 ingaan op certificatie van informatiebeveiligers. In paragraaf 6.3 wordt een scenario voor invoering van een kwalificatie- en certificatiestelsel geschetst. Ten slotte geven we in paragraaf 6.4 de conclusies uit dit hoofdstuk.

6.1 Kwalificatie van informatiebeveiligers

Informatiebeveiliging wordt steeds meer beschouwd als een relevant en afgebakend vakgebied waarvoor gekwalificeerde professionals nodig zijn. Om voor de professionals binnen het vakgebied te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de samenleving, is het nodig om uniforme kwalificatie in te voeren. Dit is vooral van belang voor de beroepen binnen het vakgebied die door een relatief groot aantal professionals uitgevoerd zullen worden.

De grootste groep professionals binnen het vakgebied informatiebeveiliging zal terechtkomen in de volgende beroepen:

- Informatierisicomanager op strategisch en tactisch niveau.
- ICT-beveiliger op strategisch, tactisch en operationeel niveau.
- Relatief grootschalige specialistische beroepen op het gebied van informatierisicomanagement en ICT-beveiliging.

Voor deze beroepen is het zinvol en wellicht zelfs noodzakelijk om uniforme kwalificatie in te voeren. De voordelen hiervan zijn:

- Organisaties kunnen op basis van behaalde kwalificaties beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties.
- De aanbieders van onderwijs kunnen de gedefinieerde kwalificatieniveaus gebruiken om hun opleidingen op af te stemmen.
- Professionals kunnen met erkende kwalificaties en certificaten eenvoudiger aantonen welke specifieke competenties ze met betrekking tot informatiebeveiliging hebben.

Voor uniforme kwalificatie in de informatiebeveiliging zijn voor de te kwalificeren beroepen uniforme kwalificatieschema's nodig. Ieder uniform kwalificatieschema geeft voor een gegeven beroep aan welke startkwalificatie daarvoor nodig is, bijvoorbeeld een bepaalde opleiding, en

welke eisen gesteld worden aan het continueren van de kwalificatie, bijvoorbeeld aantoonbare werkervaring en het volgen van seminars of cursussen. Ieder uniform kwalificatieschema is gebaseerd op een beroeps- en opleidingsprofiel waarvoor binnen de betreffende beroepsgroep een breed draagvlak is.

De uniforme kwalificatieschema's voor informatierisicomanagers en ICT-beveiligers kunnen gebaseerd worden op de aanzet voor beroeps- en opleidingsprofielen uit hoofdstuk 4 en 5. Verdere uitwerking van deze profielen en de daarop gebaseerde kwalificatieschema's kan het beste gebeuren door, of in opdracht van, één of meer van de beroepsorganisaties. Het meest voor de hand ligt de PvIB, al dan niet met één of meer van de andere beroepsorganisaties (zie bijlage E). Aanbieders van onderwijs kunnen de opleidingsprofielen uit de kwalificatieschema's gebruiken voor het inrichten van opleidingen.

Voor de relatief grootschalige specialistische beroepen binnen het vakgebied informatiebeveiliging kunnen beroeps- en opleidingsprofielen gedefinieerd worden door, of in samenwerking met, de betreffende beroepsgroepen en de andere stakeholders (werkgevers, opleidingsinstellingen en betrokken ministeries). Op basis hiervan kunnen uniforme kwalificatieschema's voor de betreffende beroepen opgesteld worden. Voor bijvoorbeeld digitaal forensisch onderzoeker (operationeel niveau) is reeds een beroeps- en opleidingsprofiel en een daarop gebaseerd kwalificatieschema opgesteld.
De aanbieders van onderwijs kunnen ook hier de opleidingsprofielen uit de kwalificatieschema's gebruiken voor het inrichten van opleidingen. Voor het profiel digitaal forensisch onderzoeker is dit gedaan door verscheidene mbo-instellingen.

Daarnaast zijn er kleinschalige specialistische beroepen, zoals cryptoloog. Deze beroepen worden in Nederland slechts door een relatief klein aantal professionals uitgevoerd. Voor deze kleine aantallen is het niet zinvol om te investeren in uniforme kwalificatieschema's. Voor de kleinschalige specialistische beroepen kan beter gericht geworven worden met individuele kwalificatie en maatwerk voor het opbouwen en bijhouden van kennis en ervaring. Voor onderwijs kan men putten uit cursussen bij specialistische organisaties en onderwijsmodules uit het initiële en post-initiële onderwijs.

6.2 Certificatie van informatiebeveiligers

Certificatie, oftewel formele registratie in een certificatieregister op basis van een certificatieschema, is een logisch vervolg op kwalificatie en kan op een behoorlijk groot draagvlak rekenen. Toch waren nog niet alle geraadpleegde personen helemaal overtuigd van het nut en de haalbaarheid van certificatie. Daarom ligt het voor de hand om de beslissing over het al dan niet invoeren van certificatie pas te nemen als de kwalificatie van informatiebeveiligers geregeld is.

Als kwalificatie op basis van één of meer beroepsprofielen en kwalificatieschema's geregeld is en de daarvoor benodigde opleidingen ook geregeld zijn, moet nog een aantal punten gerealiseerd worden om met certificatie te kunnen werken:

- Een certificatie-instantie.

- Een certificatieregister.
- Gedrag- en beroepsregels.
- Eisen voor bij- en nascholing.
- Een Raad van Tucht.

De centrale vraag hierbij is welke partij of partijen de certificatie-instantie(s) worden. De andere punten moeten dan door, of in samenwerking met, de certificatie-instantie(s) gerealiseerd worden.

Voor de certificatie-instantie(s) kan een keuze gemaakt worden uit de volgende opties:

- Opleidingsinstellingen.
- Een niet-geaccrediteerde certificatie-instantie.
- Een geaccrediteerde certificatie-instantie.

Ieder van deze opties heeft voor- en nadelen. Deze worden in de volgende subparagrafen besproken.

6.2.1 Opleidingsinstellingen

In deze optie richten opleidingsinstellingen opleidingen in op basis van de kwalificatieschema's. Dit betekent dat een opleidingsinstelling voor een gegeven beroep een opleiding inricht en aanbiedt waarmee iemand zich kan kwalificeren voor het betreffende beroep. De opleidingsinstelling gebruikt hiervoor het opleidingsprofiel uit het kwalificatieschema voor het betreffende beroep. Iemand die de gegeven opleiding met succes afrondt, krijgt een diploma.

De afgestudeerde heeft met het behaalde diploma weliswaar de startkwalificatie binnen, maar zal zich nog verder dienen te bekwamen. Dit betekent dat de afgestudeerde op regelmatige basis kennis en ervaring moet verbreden, bijvoorbeeld door middel van cursussen of aantoonbare werkervaring. De opleidingsinstelling toetst periodiek, bijvoorbeeld elke twee jaar, of de afgestudeerde voldoende gedaan heeft aan het verbreden van kennis en ervaring. De opleidingsinstelling houdt een register bij met de resultaten van de toetsing. Zo lang de afgestudeerde voldoet aan de verplichtingen is hij of zij een gekwalificeerde en certificeerde professional voor het betreffende beroep.

In het algemeen zal de opleidingsinstelling voor de periodieke toetsing kosten in rekening brengen. De beroepsorganisatie(s) beoordelen periodiek de conformiteit van de opleidingsinstellingen ten aanzien van het kwalificatie- en certificatiestelsel.

De kosten van deze optie zitten vooral in het opstellen en beheren van een certificatieschema voor ieder beroep, of groep van beroepen. Met een kostendekkende eigen bijdrage voor de toetsing worden alle verdere kosten gedekt. De kwaliteit, transparantie en continuïteit van deze optie zijn relatief moeilijk te borgen.

6.2.2 Niet-geaccrediteerde certificatie-instantie

Analoog aan de vorige optie richten de opleidingsinstellingen opleidingen in op basis van de kwalificatieschema's en geven diploma's af waarmee de afgestudeerden hun startkwalificatie behalen.

In deze optie kan iedere afgestudeerde zich met de behaalde startkwalificatie echter laten registreren in het certificatieregister van de daarvoor aangewezen certificatie-instantie. Vervolgens wordt door deze instantie periodiek getoetst of de betreffende persoon voldaan heeft aan de eisen die aan de certificering verbonden zijn, bijvoorbeeld het bij blijven op het vakgebied. Zo lang de persoon in het register opgenomen blijft, is hij of zij een gekwalificeerde en certificeerde professional voor het betreffende beroep.

Voor het certificatieproces stelt de certificatie-instantie een certificatieschema op. Desgewenst kan daarin onderscheid gemaakt worden tussen meerdere te certificeren niveaus, bijvoorbeeld junior, medior en senior. Dit onderscheid kan gebaseerd zijn op de ervaring, zoals in het schema van de Britse IISP, of op basis van opleiding- en/of denkniveau. Als ervaring een rol speelt dan moet deze wel op een valide wijze gemeten worden, dus niet het tellen van gevolgde seminars.

Naast het certificatieschema zijn gedrag- en beroepsregels en een Raad van Tucht nodig. Daarmee ontstaat de mogelijkheid om gecertificeerden in bepaalde gevallen, bijvoorbeeld bij wanprestatie, te schrappen uit het certificatieregister.

In het algemeen zal de certificatie-instantie voor de registratie jaarlijks kosten in rekening brengen. De beroepsorganisatie(s) beoordelen periodiek de conformiteit van de opleidingsinstellingen en de certificatie-instantie ten aanzien van het kwalificatie- en certificatiestelsel.

Om relatief snel een bepaalde kritische massa aan gecertificeerden te krijgen, wordt niet gekozen voor grandfathering, maar voor de mogelijkheid dat de huidige beroepsbeoefenaren zich kunnen kwalificeren op basis van erkenning van eerder verworven competenties (EVC). Dit kan getoetst worden door bijvoorbeeld een examen, of het beoordelen van een ervaringsportfolio. De daarvoor benodigde examen- c.q. beoordelingscommissie dient door, of namens, de certificatie-instantie ingericht en gemonitoord te worden.

De kosten van deze optie liggen hoger dan die van de vorige optie, omdat er een aparte administratieve organisatie opgetuigd moet worden. Daar staat tegenover dat er in dit geval sprake is van een centrale organisatie, centrale toetsing en een centraal register. Dit komt de kwaliteit en de transparantie ten goede.

6.2.3 Geaccrediteerde certificatie-instantie

Deze optie is grotendeels hetzelfde als de vorige optie, maar de certificatie-instantie is geaccrediteerd door een accreditatieorganisatie, bijvoorbeeld de Raad van Accreditatie (RvA). De ac-

creditatieorganisatie kan eisen dat de certificatie-instantie(s) zich conformeren aan de standaard ISO/IEC 17024.

Voor informatiebeveiligers kan een beroepseigen geaccrediteerde certificatie-instantie worden opgezet, of het certificeren kan ondergebracht worden bij een daarin gespecialiseerde instantie die geaccrediteerd is, bijvoorbeeld DNV, DEKRA, LRQA, of Certiked. Het opzetten van een beroepseigen geaccrediteerde certificatie-instantie is duurder dan het gebruik maken van een gespecialiseerde instantie. Daarom ligt het voor de hand om binnen deze optie te kiezen voor het laatste.

De kosten van deze optie liggen hoger dan die van de andere twee opties. Dit wordt vooral veroorzaakt door de extra administratieve last, de professionele opzet en de commerciële tarieven. Daar staat tegenover dat de kwaliteit en continuïteit van deze optie beter scoren dan bij de andere twee opties.

6.2.4 Voorkeuroptie

Hoewel ieder van de hierboven genoemde opties voor- en nadelen heeft, is er wel iets meer over aan te geven. De eerste optie, certificeren door opleidingsinstellingen, is onaantrekkelijk omdat goede kwaliteit, transparantie en continuïteit relatief moeilijk te borgen zijn. De kostenvoordelen wegen in dit geval minder zwaar. De tweede en derde optie, beide met een aparte certificatie-instantie, zijn allebei reële mogelijkheden. Optie drie, met een geaccrediteerde certificatie-instantie, is echter minder aantrekkelijk, omdat deze optie relatief duur is. Daarmee heeft optie twee, met een niet-geaccrediteerde certificatie-instantie, vooralsnog de voorkeur.

6.3 Scenario voor invoering

Het traject van invoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers doorloopt een aantal stappen die in Tabel 10 zijn weergegeven. Om een goede afstemming met de beroepspraktijk te krijgen ligt de trekkersrol voor dit scenario bij voorkeur bij één of meer van de beroepsorganisaties. Het meest voor de hand ligt de PvIB (Platform voor Informatiebeveiliging), al dan niet met één of meer van de andere beroepsorganisaties (zie bijlage E).

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 opleidingsinstellingen betrokken.	Beroepsorganisatie(s), zie bijlage E
2	Het opstellen van beroeps- en opleidingsprofielen voor informatiebeveiligingsberoepen. Voor informatierisicomanager (strategisch en tactisch) en ICT-beveiliger (strategisch, tactisch en operationeel) kan gebruik gemaakt worden van de aanzet in hoofdstuk 4 en 5.	Beroepsorganisatie(s) en andere stakeholders

Stap	Omschrijving	Uitvoerende partij
3	Het opstellen van kwalificatieschema's. Per informatiebeveiligingsberoep wordt een schema opgesteld op basis van het betreffende beroeps- en opleidingsprofiel. Bijzondere aandacht is nodig voor de mate waarin aanvullend ervaring nodig is voor kwalificatie. Desgewenst kunnen verschillende niveaus worden onderscheiden, bijvoorbeeld junior, medior en senior.	Beroepsorganisatie(s) en opleidingsinstellingen
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. Per beroep met een kwalificatieprofiel worden één of meer opleidingen gedefinieerd op basis van het betreffende opleidingsprofiel. Per opleiding moet een marktonderzoek uitgevoerd worden om aan te kunnen geven of er voldoende vraag is naar de betreffende opleiding.	Beroepsorganisatie(s) en opleidingsinstellingen
7	Het inrichten van erkende opleidingen.	Opleidingsinstellingen
8	Het nagaan in hoeverre certificatie door de beroepsorganisaties en andere stakeholders (werkgevers, opleidingsinstellingen en betrokken ministeries) nog steeds gewenst en haalbaar gevonden wordt. 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. Bij deze instantie hoort ook een Raad van Tucht.	Beroepsorganisatie(s)
10	Het opstellen van certificatieschema's. Per informatiebeveiligingsberoep wordt een schema opgesteld op basis van het betreffende kwalificatieprofiel. Er dient aandacht besteed te worden aan het certificeren van de huidige professionals.	Certificatie-instantie
11	Het inrichten van één of meer registers. 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)

Tabel 10: Invoering van kwalificatie- en certificatiestelsel voor informatiebeveiligers.

6.4 Conclusies

Binnen het vakgebied informatiebeveiliging is uniforme kwalificatie zinvol en wellicht zelfs noodzakelijk voor de volgende beroepen:

- Informatierisicomanager op strategisch en tactisch niveau.
- ICT-beveiliger op strategisch, tactisch en operationeel niveau.
- Relatief grootschalige specialistische beroepen op het gebied van informatierisicomanagement en ICT-beveiliging.

Kwalificatie gebeurt op basis van een kwalificatieschema dat gebaseerd is op een beroeps- en opleidingsprofiel. Aanbieders van onderwijs kunnen een opleidingsprofiel gebruiken voor het inrichten van een opleiding.
Voor kleinschalige specialistische beroepen is het niet zinvol om te investeren in een uniform kwalificatieschema en kan beter gericht geworven worden met individuele kwalificatie en maatwerk voor het opbouwen en bijhouden van kennis en ervaring.

Certificatie, oftewel formele registratie in een certificatieregister op basis van een certificatieschema, is een logisch vervolg op kwalificatie. Om tegemoet te komen aan degenen die nog niet helemaal overtuigd zijn van het nut en de haalbaarheid van certificatie, is de beslissing daarover in het scenario voorzien nadat de kwalificatie van informatiebeveiligers geregeld is.

Voor certificatie is de primaire vraag welke partij de certificatie-instantie is. Hiervoor zijn de volgende opties:

- Opleidingsinstellingen.
- Een niet-geaccrediteerde certificatie-instantie.
- Een geaccrediteerde certificatie-instantie.

Hoewel ieder van deze opties voor- en nadelen heeft, is duidelijk dat alleen de tweede en derde optie reëel zijn vanwege kwaliteit, transparantie en continuïteit. De tweede optie, met een niet-geaccrediteerde certificatie-instantie, scoort qua kosten beter en heeft daarom vooralsnog de voorkeur.

In paragraaf 6.3 is een scenario geschetst voor de invoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. De trekkersrol voor dit scenario ligt bij één of meer van de beroepsorganisaties. Het meest voor de hand ligt de PvIB, al dan niet met één of meer van de andere beroepsorganisaties (zie bijlage E).

Daarmee hebben we de tweede onderzoeksvraag beantwoord, namelijk hoe een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland met voldoende relevantie en draagvlak gerealiseerd kan worden.

De derde onderzoeksvraag, waarin gevraagd wordt naar het beheer en de bekostiging van het kwalificatie- en certificatiestelsel voor informatiebeveiligers, is slechts gedeeltelijk beantwoord. Er zijn partijen genoemd die het beheer op zich zouden kunnen nemen, maar er is nog geen

uitsluitsel of dat ook gerealiseerd kan worden. Bovendien is er nog geen goed financieel plaatje voor het kwalificatie- en certificatiestelsel beschikbaar.

7. Conclusies en aanbevelingen

7.1 Conclusies

Is het nuttig en haalbaar om een kwalificatie- en certificatiestelsel voor informatiebeveiligers in Nederland in te voeren?

Binnen het vakgebied informatiebeveiliging bestaat een chaotische situatie met betrekking tot kwalificatie en certificatie van professionals. Om binnen het vakgebied te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de samenleving, is het nuttig om in Nederland een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers op te zetten op basis van opleiding en ervaring. De voordelen hiervan zijn:

- Organisaties kunnen op basis van behaalde kwalificaties en certificaten beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties.
- De aanbieders van onderwijs kunnen de gedefinieerde kwalificatie- en certificatieniveaus gebruiken om hun opleidingen op af te stemmen.
- Professionals kunnen met erkende kwalificaties en certificaten eenvoudiger aantonen welke specifieke competenties ze met betrekking tot informatiebeveiliging hebben.

Uniforme kwalificatie en certificatie is vooral zinvol en wellicht zelfs noodzakelijk voor de volgende beroepen:

- Informatierisicomanager op strategisch en tactisch niveau.
- ICT-beveiliger op strategisch, tactisch en operationeel niveau.
- Relatief grootschalige specialistische beroepen op het gebied van informatierisicomanagement en ICT-beveiliging. Sommige van deze beroepen, zoals IT-auditor en digitaal forensisch onderzoeker, werken al met kwalificatie en certificatie.

Een kwalificatie- en certificatiestelsel voor informatiebeveiligers is niet alleen nuttig en nodig, maar wordt ook haalbaar gevonden, mits duidelijk wordt dat te kleine aantallen kandidaten en te hoge kosten geen belemmerende factoren zullen zijn.
Een aantal geraadpleegde personen ziet bij voorkeur dat de beslissing om certificatie al dan niet in te voeren pas wordt genomen nadat kwalificatie van informatiebeveiligers geregeld is.

Desgewenst kunnen in een kwalificatie- en certificatiestelsel voor informatiebeveiligers meerdere niveaus onderscheiden worden, bijvoorbeeld junior, medior en senior. Daarnaast moet de reële mogelijkheid bestaan om geschrapt te worden uit het certificatieregister, bijvoorbeeld na wanprestatie.

Het is nodig dat de relevante bestaande kwalificaties en certificaten, ook uit het buitenland, in een nieuw kwalificatie- en certificatiestelsel voor informatiebeveiliging meegenomen worden.

Ook is het van belang om nationale kwalificaties en certificaten internationaal te (laten) erkennen.

Hoe kan een kwalificatie- en certificatiestelsel in Nederland met voldoende relevantie en draagvlak gerealiseerd worden?

In paragraaf 6.3 is een scenario beschreven voor de invoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Om een goede afstemming met de beroepspraktijk te krijgen ligt de trekkersrol voor dit scenario bij voorkeur bij één of meer van de beroepsorganisaties. Het meest voor de hand ligt de PvIB (Platform voor Informatiebeveiliging), al dan niet met één of meer van de andere beroepsorganisaties (zie bijlage E).

De certificatie-instantie is bij voorkeur een onafhankelijke organisatie die daarvoor door de beroepsorganisaties is opgezet, of aangewezen. De certificatie-instantie kan al dan niet geaccrediteerd zijn. De niet-geaccrediteerde instantie scoort qua kosten beter en heeft daarom vooralsnog de voorkeur.

Hoe zijn het beheer en de bekostiging van een kwalificatie- en certificatiestelsel voor informatiebeveiligers te realiseren?

De ontwikkeling van een kwalificatie- en certificatiestelsel voor informatiebeveiligers zal vooral getrokken moeten worden door één of meer van de beroepsorganisaties. Wie het beheer ervan op zich kan nemen is nog geen uitgemaakte zaak. Er zijn weliswaar partijen genoemd die het beheer op zich zouden kunnen nemen, maar er is nog geen uitsluitsel of dat ook gerealiseerd kan worden. Bovendien is er nog geen goed financieel plaatje voor het kwalificatie- en certificatiestelsel beschikbaar.

7.2 Aanbevelingen

Ten behoeve van het binnen afzienbare termijn realiseren van een kwalificatie- en certificatiestelsel voor informatiebeveiligers zijn de volgende aanbevelingen geformuleerd:

- Het mobiliseren van de beroepsorganisatie PvIB om gezamenlijk met de andere beroepsorganisaties (zie bijlage E) de taakverdeling te bepalen voor het ontwikkelen van een kwalificatie- en certificatiestelsel voor informatiebeveiligers.
- Het opstellen van een financieel overzicht voor een kwalificatie- en certificatiestelsel voor informatiebeveiligers. Hierin wordt ook aangegeven wat de eenmalige en jaarlijkse kosten zijn voor degenen die van de kwalificatie- en certificatiediensten gebruik gaan maken. Hierbij valt te denken aan een jaarlijkse bijdrage van € 50 tot € 150, plus de kosten van eventuele examens. Bovendien maakt het financieel overzicht duidelijk in hoeverre formele accreditatie van de certificatie-instantie qua kosten wellicht toch haalbaar is.
- Het onderzoeken of subsidie verkregen kan worden voor het opzetten van een kwalificatie- en certificatiestelsel voor informatiebeveiligers en de daarvoor benodigde onderzoeksstappen.

- Het onderzoeken welke partij(en) het beheer en de uitvoering van een kwalificatie- en certificatiestelsel voor informatiebeveiligers op zich kunnen nemen. De te selecteren partij(en) moeten voldoende garanties kunnen bieden met betrekking tot de continuïteit van het kwalificatie- en certificatiestelsel.
- Het uitwerken van een kwalificatie- en certificatiestelsel voor informatiebeveiligers volgens het scenario dat beschreven is in paragraaf 6.3. Onderdeel hiervan is het door de beroepsorganisaties en andere stakeholders (werkgevers, opleidingsinstellingen en betrokken ministeries) uitwerken van de benodigde beroeps- en opleidingsprofielen en de toelatingseisen voor de huidige professionals. Tevens dienen de relevante bestaande kwalificaties en certificaten, ook uit het buitenland, te worden geïnventariseerd en 'gemapt' op de kwalificatie- en certificatieschema's.
- Het inventariseren van relevante kwalificatie- en certificatiestelsels in het buitenland, om daar zo goed mogelijk op aan te kunnen sluiten en in een later stadium wederzijdse erkenning van kwalificaties en certificaten mogelijk te maken.

Bijlage A: Interviewvragen

1. Is in Nederland en/of het buitenland behoefte aan (aanvullende) certificering van IB-functies?
2. Welke relevante (inter)nationale certificaten zijn reeds in gebruik en wat houden ze in?
3. Welke IB-functies en -niveaus komen voor certificering in aanmerking?
4. Welke inhoudelijke criteria zouden aan deze IB-functies gesteld moeten worden voor certificering?
5. Is een ‘stapeling’ van certificaten nuttig/nodig?
6. Moeten aanvullende inspanningen gepleegd worden om een verkregen certificaat geldend te laten blijven?
7. Welke procedure zou hiervoor moeten gelden en wie zou dat moeten bewaken?
8. Wie is de certificatie-instantie?
9. Wie beheert de voor certificering geldende procedures, inclusief de certificatiecriteria en de nascholingsverplichting?
10. Wie beheert het register van certificaten?
11. Mag een certificaat eenmalig of jaarlijks kosten met zich meebrengen?
12. Wie draagt de kosten voor het certificatiestelsel?

Bijlage B: Geraadpleegde personen

De hieronder genoemde personen zijn geïnterviewd voor het onderzoek.

Naam	Functie	Organisatie
Werkgevers Privaat		
Mark Buiting	CISO	UVIT (Unive-VGZ-IZA-Trias)
Geo Aldershof	Secretaris Commissie Infobeveiliging	VNO-NCW
Ton Diemont	CISO, Hoofd Information Risk Management	ING, Corporate Operational Risk Management
Jan Willem Schoemaker	Security Officer/ Business Continuity Manager	Erasmus Medisch Centrum
Groepsinterview	Info.bev.specialisten	Airport-ISAC
Groepsinterview	Info.bev.specialisten	Energie en Water-ISAC
Groepsinterview	Info.bev.specialisten	Multinationals-ISAC
Werkgevers Publiek		
Henk Gomis	Info.bev.functionaris	Centr.Just.Incassobureau
Frank Heijligers	Senior beleidsmedewerker	Ministerie van BZK
Carl Adamse	Senior beleidsmedewerker	Ministerie van BZK
Wilbert Vrouwenvelder	Info.bev.functionaris, Privacyfunctionaris	Ministerie van Verkeer & Waterstaat
Werkgevers Specialisten		
Lex Dunn	Security Officer	Capgemini Outsourcing
Jaap Halfweeg	Customer Security Compliance Officer	Getronics
Floris van den Dool	Security Lead EALA	Accenture
Informatiebeveiligingsspecialisten		
Paul Overbeek	Zelfstandig adviseur	Overbeek Information Security
Opleidingsinstellingen		
Hans Blankendaal	Teammanager	ECABO
Ad van Dijk	Coördinator opleiding PDO	ID College Gouda
Leo van Koppen	Coördinator opleiding ISM	Haagse Hogeschool

Naam	Functie	Organisatie
Gert de Ruiter	Directeur Academie ICT&M	Haagse Hogeschool
Wouter Stol	Hoogleraar, Lector, Lector	Open Universiteit, Noord.Hogesch.Leeuwarden, Politieacademie
Certificatie-instanties		
Jan Sauer	Zelfstandig adviseur	Sauer Quality Consulting
Wilfried Olthof	Executive Director	NOREA
Prof. Paul Dorey	Voorzitter	IISP

Bijlage C: Geraadpleegde documentatie

De hieronder genoemde documentatie is geraadpleegd voor het onderzoek.

Titel	Auteur	Uitgever	Datum
Accreditor Role Definitions	CESG		16 maart 2010
Bachelor of ICT	HBO-I	HBO-I	2009
Beoordeling van Schema's voor Conformiteitsbeoordeling	Raad van Accreditatie	Raad van Accreditatie	Juli 2008
Digital Agenda	N. Kroes	Europese Unie	19 mei 2010
Functies in de informatiebeveiliging	B. Bokhorst en anderen	PvIB	December 2006
Human Resource Management	CIO Platform Nederland	CIO Platform Nederland	Juni 2007
Informatiebeveiliging onder controle	P. Overbeek en anderen	Pearson Education	Juli 2006
Information Security Certifications	C. Casper en A. Esterle	ENISA	December 2007
ISO/IEC 17024:2003 Conformity assessment – General requirements for bodies operating certification of persons	ISO	ISO	2003
IT Specialist Certification (ITSC), Certification Policy, version2.0	The Open Group	The Open Group	Februari 2010
Landelijke kwalificaties MBO: Particulier digitaal onderzoeker	ECABO	ECABO	2009-2010
Leidraad Functieprofiel Informatiebeveiliger in het Hoger Onderwijs	SURF-IBO	SURF	December 2005
Kwalificatie van Professionals informatiebeveiliging (position paper)	Commissie Informatiebeveiliging	VNO-NCW	September 2010
Nationale Cyber Security Strategie (NCSS)	Verscheidene partijen		2011
RE-Gids 2010/2011	NOREA	NOREA	2010
Taken, functies, rollen en competenties in de informatica	J.C. op de Coul	Ngi	2002
Trust and Security in the Digital Agenda	N. Kroes	Informatiebeveiliging 8, PvIB	December 2010

Bijlage D: Leden klankbordgroep

De volgende personen maakten deel uit van de klankbordgroep voor het onderzoek:

- Dhr. Dick Brandt – TNT Post, Information Security Officer.
- Dhr. Pieter van Dijken – VNO-NCW, Voorzitter Commissie Informatiebeveiliging.
- Dhr. Wim Hafkamp – Rabobank, Linking pin voor Nederlandse Vereniging van Banken.
- Dhr. Auke Huistra – CPNI.NL, Project Manager.
- Dhr. Eelco Stofbergen – GOVCERT.NL, Hoofd Kennismanagement.

Bijlage E: Beroepsorganisaties informatiebeveiliging

PvIB (www.pvib.nl)
Het Platform voor Informatiebeveiliging (PvIB) is een onafhankelijke beroepsvereniging met ca. 1200 professionals en verenigt zowel aanbieders/leveranciers als gebruikers/beheerders van producten en diensten op het gebied van informatiebeveiliging.

Het PvIB is het kenniscentrum op het gebied van informatiebeveiliging in Nederland. Het PvIB is het platform waar informatie, kennis en ervaring over informatiebeveiliging wordt verzameld, verbeterd, verrijkt en weer wordt uitgedragen. Het PvIB verenigt alle betrokkenen en geïnteresseerden in het vakgebied informatiebeveiliging. Het PvIB levert een bijdrage aan vraagstukken met maatschappelijke relevantie.

Het PvIB is het door en voor vrijwilligers georganiseerde ontmoetingspunt van professionals, inclusief verantwoordelijken voor informatiebeveiliging en andere geïnteresseerden, die elkaar willen steunen met hun deskundigheid door op basis van vrijwilligheid en collegialiteit kennis en ervaring uit te wisselen. Daarnaast wil de vereniging de deskundigheid op het gebied van en de bekendheid met informatiebeveiliging bevorderen.

Ngi (www.ngi.nl)
Het Ngi is een beroepsvereniging van en voor ICT-professionals en -managers. Het is een onafhankelijk platform waar ruim 2.500 leden hun kennis verdiepen en hun netwerk onderhouden. De afdeling Informatiebeveiliging heeft 165 leden.
De beroepsvereniging richt zich op thema's die in Nederland en internationaal van belang zijn voor de ontwikkeling en positionering van het vakgebied. De Ngi werkt onder meer op basis van de thema's vanuit de Digitale Agenda van de Europese Unie.

NGN (www.ngn.nl)
De NGN is een beroepsvereniging van en voor ICT-professionals. NGN brengt ICT- en netwerkprofessionals met elkaar in contact, en vormt een onafhankelijk en onpartijdig platform waar ongeveer 2.500 leden kennis opdoen en ervaringen met elkaar uitwisselen.
De beroepsvereniging richt zich op thema's die in Nederland en internationaal van belang zijn voor de ontwikkeling en positionering van het vakgebied. De NGN kijkt nadrukkelijk naar ontwikkelingen rond (nieuwe) technologieën die aan de basis staan van de uitvoering van het ICT vak.

NOREA: zie bijlage I

ISACA: zie bijlage G.

EEMA (www.eema.org)

EEMA is an independent association of IT professionals, businesses and governments, providing business and technical networking opportunities at both local and regional levels in the broad areas associated with digital identity and its applications, including security.
EEMA is Europe's leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.
EEMA's remit is to educate and inform around 160 Member organisations (and over 1,500 Member contacts) on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas.

GvRM (www.genootschapvoorrisicomanagement.nl)

Het Genootschap voor Risicomanagement is een vereniging van en voor mensen die zich bezighouden met risicomanagement in de breedste zin van het woord. Het genootschap biedt een platform voor kennisuitwisseling, is een netwerk voor geïnteresseerden en professionals en stelt zich ten doel het vakgebied verder te ontwikkelen. Het genootschap ondersteunt diverse opleidingen en organiseert elk jaar een congres waar opleidingsinstituten worden uitgenodigd om de laatste ontwikkelingen rond risicomanagement met elkaar te delen.

Bijlage F: Kwalificatie- en certificatie-instanties in Nederland

SVPB (www.svpb.nl)
De Stichting Vakexamens voor de Particuliere Beveiligingsorganisaties (SVPB), is een onafhankelijke stichting die de examens ontwikkelt en afneemt voor de Nederlandse beveiligingsopleidingen. SVPB-diploma's en -certificaten zijn verankerd in justitiële regelgeving en opgenomen in de CAO voor de beveiligingssector.

ECABO (www.ecabo.nl)
Kenniscentrum ECABO zorgt dat het bedrijfsleven goed gekwalificeerde mensen op mbo-nivo kan krijgen die het nodig heeft. Het werkterrein beslaat een groot deel van de zakelijke dienstverlening met beroepen als beveiliger en ICT-beheerder. Een essentieel element van ECABO's werk is afstemming van het beroepsonderwijs op de arbeidsmarkt. Voor medewerkers van bedrijven is erkenning van eerder verworven competenties (EVC) de kortste weg naar een diploma: wat je in de praktijk geleerd hebt. ECABO heeft het beroepscompetentieprofiel voor de Particulier Digitaal Onderzoeker ontwikkeld.

EXIN
EXIN is een exameninstituut voor ICT'ers en zorgt wereldwijd voor de ontwikkeling en afname van onafhankelijke ICT-examens. EXIN's missie is de bevordering van de kwaliteit van het ICT-vakgebied en de daarin werkzame ICT-professionals en ICT-gebruikers door onafhankelijke toetsing en certificering.
EXIN ontwikkelt ICT-examens maar geeft geen (ICT-)opleidingen. Daardoor blijft EXIN onafhankelijk en worden examenresultaten objectief beoordeeld. EXIN examineert ICT'ers in meer dan 125 landen van zes continenten, en in 15 talen. Meer dan een miljoen ICT-professionals hebben inmiddels een EXIN-examen afgelegd.

Informatiebeveiliging
De module Information Security Management Expert based on ISO/IEC 27002 maakt samen met de Foundation en de Advanced module deel uit van het EXIN-kwalificatieprogramma voor Information Security based on ISO/IEC 27002. De internationale norm, de Code voor Informatiebeveiliging NEN-ISO/IEC 27002:2005 geeft structuur bij het inrichten van informatiebeveiliging en is daarom een belangrijk uitgangspunt van de module.
De kandidaat dient aantoonbare praktijkervaring op managementniveau te hebben, minimaal 2 jaar, op ten minste twee van de hoofdonderwerpen (exameneisen) van deze module.

Register voor Post HBO opleidingen (www.cpion.nl)
Het Centrum voor Post-Initieel Onderwijs Nederland (CPION) vormt het aanspreekpunt voor aanbieders die hun post-initiële opleidingen willen laten registreren als officiële Registeropleiding. CPION zorgt voor inhoudelijke toetsingen. Alleen opleidingen die voldoen aan de kwali-

teitscriteria, komen in aanmerking voor het predicaat ‘Registeropleiding’ en worden opgenomen in het Register.
Deelnemers die met goed gevolg deelnemen aan deze Registeropleidingen, worden opgenomen in het Abituriëntenregister en ontvangen een officieel, erkend diploma of certificaat.

Bijlage G: Internationale certificatie-instanties

IISP (www.instisp.org)
The Institute of Information Security Professionals (London) is setting the standard for professionalism in information security, speaking with an independent and authoritative voice. Full Membership of the Institute is becoming the internationally recognised professional standard qualification for information security professionals.

The Institute aims to provide a universally accepted focal point for the information security profession. The Institute is an independent not-for-profit body governed by its members, ensuring standards of professionalism - for training, qualifications, operating practices and individuals. One of its main activities is to act as an accreditation authority for the industry. Full Membership of the Institute is Information Security's "professional standard" and endorses the knowledge, experience and professionalism of an individual in this field. The Award is competency based which sets it apart from purely knowledge based qualifications and is awarded to those professionals who demonstrate breadth and depth of knowledge, and substantial practical experience.

There are currently four levels of Individual Membership:
Full Membership of the IISP is Information Security's 'professional standard' and endorses the knowledge, experience and professionalism of an individual in this field. Individuals who can demonstrate breadth and depth of knowledge, and substantial practical experience should apply at this level. Applicants will be asked to complete a detailed application form which is assessed for a standard of competency. Successful candidates are then invited to attend a face to face interview with suitably skilled Members. Recommendations from these interviews are made to the Institute's Accreditation Committee which makes the final decision.
Individuals who can demonstrate breadth of knowledge, and some practical experience should apply **Associate membership**. Applicants will be asked to complete a detailed application form which is assessed for a standard of competency. Recommendations from this assessment are made to the Institute's Accreditation Committee. You are likely to be successful at this level if you have 2+ years experience in an Information Security Role.
Affiliate membership is open to any individual with an interest in the information security industry, or someone who does not have the required qualification or experience to become an Associate Member. The **Student membership** is open to all those studying for an information security related degree from a university.

(ISC)² (www.isc2.org)
De non-profit organisatie (ISC)² (International Information Systems Security Certification Consortium) heeft zijn hoofdkwartier in de Verenigde Staten. In 135 landen zijn meer dan 60.000 gecertificeerden. (ISC)² is door American National Standards Institute (ANSI) conform ISO/IEC 17024 geaccrediteerd voor zijn SSCP® (Systems Security Certified Practitioner). Het behalen

van het certificaat geeft recht op het dragen van de CISSP-titel achter de naam. In 2010 droegen ruim 1000 security-professionals in Nederland de CISSP-titel.
De CISSP titel mag gevoerd worden als aan de volgende voorwaarden is voldaan:

- Slagen voor een zes uur durend examen.
- Minimaal 5 jaar relevante werkervaring in minimaal twee van de onderscheiden 10 domeinen.
- Ondertekenen van de (ISC)² Code of Ethics.
- Bevestiging door een CISSP gecertificeerde of vergelijkbare professional over de goede naam van de kandidaat.

Om de titel te kunnen verlengen dient een deelnemer in een periode van 3 jaar 120 zogenaamde CPE credits te verzamelen. CPE credits kunnen behaald worden door het volgen van opleidingen, het bezoeken van relevante seminars, het verzorgen van onderwijs, het schrijven van artikelen et cetera.
De certificaten van (ISC)² zijn georiënteerd op de Verenigde Staten. Er zijn aanbieders in Nederland die daarom een 'Europees blok' aanbieden.

(ISC)² kent de volgende certificaten:

- CISSP - Certified Information Systems Security Professional.
- ISSAP - Information Systems Security Architecture Professional.
- ISSEP – Information Systems Security Engineering Professional.
- ISSMP - Information Systems Security Management Professional.
- CSSLP - Certified Secure Software Lifecycle Professional.

ISACA (www.isaca.nl)
ISACA is in 1967 opgericht door een groep gelijkgestemden, werkzaam in de computerbranche, met specifieke aandacht voor audit en beheersingsvraagstukken. Vanuit ISACA werd in 1976 het IT Governance Instituut opgericht, dat onderzoek uitvoert naar de gecontroleerde inrichting van ICT binnen organisaties en de manier waarop met ICT waarde aan een organisatie kan worden toegevoegd. Op basis van dit onderzoek worden internationale standaarden ontwikkeld, zoals Cobit.

ISACA telt meer dan 86.000 leden verspreid over meer dan 160 landen. De leden van ISACA vervullen een veelheid aan ICT-gerelateerde functies, zoals IT security specialist, IT auditor, IT consultant en Chief Information Officer. De leden vindt men terug op verschillende niveaus in hun organisaties en in bijna alle sectoren, waaronder banken en verzekeringen, pensioenfondsen, industrie en overheden. ISACA heeft een uitgebreid netwerk van meer dan 185 chapters in meer dan 75 landen.

Het certificaat Certified Information System Auditor (**CISA**) wordt gevoerd door meer dan 75.000 professionals. De CISA-certificering is geaccrediteerd door American National Standards Institute (ANSI) onder nummer ISO/IEC 17024:2003. Het voeren van de kwalificatie CISA is niet beschermd door specifieke Nederlandse wetgeving; ISACA heeft civielrechtelijk de titulatuur beschermd.

De op het management gerichte opleiding van Certified Information Security Manager (**CISM**) is door meer dan 12.500 personen succesvol afgerond. De titel van **CGEIT** (Certified in the Governance of Enterprise Information Technology) die aangeeft dat een professional kennis en ervaring heeft op het gebied van IT Governance, is inmiddels 4.000 keer verleend. Deze certificering richt zich specifiek op het risicobeheer en Information Systems' Control en wordt verleend aan professionals die ICT-risico's kunnen identificeren en managen.

Het certificaat Certified in Risk and Information Systems Control™ (**CRISC**) is ontwikkeld voor ICT-professionals met hands-on ervaring met onder meer risico-identificatie, -beoordeling, -evaluatie en -monitoring en het ontwerpen, implementeren en onderhouden van informatiesysteembeveiliging.

Bijlage H: Huidige kwalificatie van informatiebeveiligers in Nederland

In onderstaande paragraaf staan enkele voorbeelden van opleidingen voor informatierisicomanagement en ICT-beveiliging in Nederland.

Informatierisicomanagement	Toelichting
MISM (Tias-Nimbas)	De opleiding Executive Master of Information Security Management (MISM) is een professional Master's opleiding op het gebied van informatiebeveiliging. De opleiding bestrijkt het gebied van de informatiebeveiliging voor zover niet-technisch van aard, en levert een inleiding in de technische aspecten die het mogelijk maakt om inhoudelijk contact te onderhouden met de betrokken ICT'ers. In de opleiding worden bovendien communicatieve aspecten die wenselijk zijn voor liaisondoeleinden op beveiligingsgebied behandeld, in het bijzonder in relatie tot het leiden en managen van informatiebeveiligingsactiviteiten in organisaties.
ISM (HHS)	Het studieprogramma van de Hbo-opleiding Information Security Management duurt vier jaar en leidt op tot information security manager. De opleiding Information Security Management bestaat uit een propedeuse van één jaar en een hoofdfase van drie jaar. Information Security Management leidt op tot een informatiebeveiliger die van verschillende markten thuis is (zowel technisch als bestuurskundig én gericht op menselijk gedrag). In het derde en vierde jaar is de voertaal Engels. Bij Information Security Management van de HHS wordt de student voorbereid op een internationale toekomst.
ICT beveiliging	
Hogeschool Utrecht	Voltijd 4-jarige Hbo-opleiding. Een combinatie van technisch, sociaal én maatschappelijk vlak. Vakken: sensor- en detectietechnologie, data-encryptie, ethiek, digitale opsporingssystemen en politie- en forensische technologie, biometrie, recht, privacy, ethiek en innovatie. Als Security Technoloog kun je terecht als projectontwikkelaar of consultant in je eigen bedrijf. Of je kunt werken bij een beveiligingspecialist of een ict-bedrijf. Ook de (internationale) overheid is een optie. Denk hierbij aan de AIVD, politie, justitie of bij een ministerie.

Particulier Digitaal Onderzoeker	Een digitaal onderzoeker onderzoekt misbruik op digitale apparaten (vormen van criminaliteit op het internet), bijvoorbeeld computers, laptops, pda's et cetera. Een Particulier Digitaal onderzoeker moet in bezit zijn van een Particulier Onderzoeker diploma, dit vereist de basiskennis van rechercheren en de wettelijke kaders van rechercheren, evenals het correct rapporteren zodat het als bewijsmateriaal gebruikt mag en kan worden. Mbo Niveau: Particulier Digitaal Onderzoeker . Hbo Niveau: Network Forensic Research (Heerlen), Forensisch ICT (Leiden). Universitair: Digitaal Onderzoeker, Computer Forensics (Universiteit van Amsterdam).

Bijlage I: Kwalificatie voor andere beroepen

Deze bijlage geeft een beknopte beschrijving van de kwalificatie voor een aantal beroepen, te weten:

a. Accountant.
b. IT-auditor.
c. Beroepen in de beveiligingsbranche.
d. Beroepen in de gezondheidszorg.
e. Tandarts.
f. Advocaat.
g. Ingenieur.
h. Technisch personeel luchtvaart.

De beschrijvingen zijn afkomstig van de websites dan wel de statuten van de genoemde organisaties. Waar mogelijk is de relatie met kwalificatie op Europees niveau aangegeven.

a. Accountant (NBA)

Accountant is een beschermde titel. In Nederland mogen alleen registeraccountants (RA's) en Accountants-administratieconsulenten (AA's) zich accountant noemen. Registeraccountants staan ingeschreven in het register van hun beroepsorganisatie, het Koninklijk NIVRA. Accountants-administratieconsulenten staan ingeschreven bij hun beroepsorganisatie, de NOvAA. De NIVRA en de NOvAA gaan fuseren tot de Nederlandse Beroepsorganisatie van Accountants (NBA).

De geregistreerde accountants zijn conform artikel 55 van de Wet op de Registeraccountants opgenomen in het accountantsregister. Registeraccountants kunnen een tuchtrechtelijke maatregel opgelegd krijgen. Dit wordt aangetekend in het accountantsregister. Het register kan kosteloos ingezien worden bij het bestuur van de NBA. Tegen betaling van een vergoeding kan een ieder schriftelijk meegedeeld krijgen of iemand in het register is opgenomen en of diegene een tuchtrechtelijke maatregel opgelegd heeft gekregen.

b. IT-auditor (NOREA)

NOREA (Nederlandse Orde van Register EDP-Auditors) is de beroepsorganisatie van IT-auditors in Nederland met 1450 registerleden (RE's), 320 aspirantleden en ruim 200 geassocieerde leden. NOREA heeft haar regelgeving aangesloten bij internationaal erkende regelgeving zoals die is opgesteld door de International Federation of Accountants (IFAC). Het voeren van de kwalificatie RE is niet beschermd door specifieke Nederlandse wetgeving; NOREA heeft civielrechtelijk de titulatuur beschermd.

Doelstelling van NOREA is het bevorderen van de kwaliteit van de beroepsuitoefening door IT-auditors en het behartigen van hun gemeenschappelijk belang.

De Gedragscode vormt de basis van de gehele set aan regelgeving van de beroepsorganisatie en is van toepassing op alle Register IT-auditors (RE's).

Om voor toelating als student van een erkende opleiding in aanmerking te komen, dient hij/zij met succes een hbo- of WO-opleiding te hebben gevolgd, dan wel een aan te tonen vergelijkbaar niveau te bezitten. Het opleidingsprogramma heeft een studiebelasting van ten minste 900 uur. Erkende opleidingen zijn opleidingen die kwalificeren voor inschrijving in het RE-register. Ze voldoen daarmee aan de eindtermen die door NOREA in overleg met de opleidingen zijn vastgesteld.

Als gewoon lid van NOREA kunnen worden toegelaten natuurlijke personen die zijn afgestudeerd aan een erkende universitaire opleiding en voldoen aan de gestelde ervarings- en gedragsvereisten.

Op de ledenlijst staan alle gekwalificeerde IT-auditors (RE's). Dit register is openbaar en actueel. NOREA kent drie soorten lidmaatschap:
Registerleden zijn ingeschreven in het register van IT-auditors, d.w.z. dat ze op grond van hun formele kwalificatie ten aanzien van de informatietechnologie in een bedrijf of organisatie een oordeel of advies mogen geven. Ze zijn in dat verband gebonden aan de gedrags- en beroepsregels en onderworpen aan tuchtrecht.
Aspirant-leden zijn nog in opleiding of beschikken nog over onvoldoende werkervaring in de IT-auditpraktijk. **Geassocieerde** leden zijn leden die wel betrokkenheid of belangstelling hebben voor het vakgebied maar geen erkende opleiding hebben gevolgd en niet in het register worden ingeschreven.

c. Beroepen in de beveiligingsbranche (NEROB)

Doel van stichting NEROB is het bevorderen en instandhouden van de deskundigheid en vakbekwaamheid van natuurlijke personen die werkzaam zijn in de beveiligingsbranche. Om dit doel te bereiken zijn registers ingesteld voor onderzoekers, voor adviseurs in de beveiligingsbranche, forensisch ICT-onderzoekers, chauffeurs met een toegevoegde beveiligingstaak en voor persoonsbeveiligers. Om voor inschrijving in de registers in aanmerking te komen moeten kandidaten aan een aantal eisen ten aanzien van opleiding en ervaring voldoen. Ook zijn kandidaten verplicht een gedragscode te ondertekenen. Door deze eisen te stellen wil stichting NEROB de deskundigheid en vakbekwaamheid van de ingeschrevenen waarborgen.

De registers zijn openbaar en dus door derden te raadplegen. Ingeschrevenen mogen achter hun naam RAN en/of RON en/of RPN en/of RCN en/of RFIN vermelden waaruit blijkt dat zij ingeschreven zijn in een van de registers van de stichting NEROB.

d. Beroepen in de gezondheidszorg (CIBG)

De Wet op de beroepen in de individuele gezondheidszorg (BIG) stelt eisen aan werknemers in de individuele gezondheidszorg. In de wet staan regels over opleidingseisen, registratie, deskundigheidsgebied en het voeren van een titel.

Het CIBG, een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport, beheert zorgregisters, zorgt voor veilige gegevensoverdracht, verstrekt vergunningen en ondersteunt toetsingscommissies. Het CIBG registreert zorgverleners in het BIG-register.
Het BIG-register is een taak die voortkomt uit de Wet-BIG (Wet op de Beroepen in de Individuele Gezondheidszorg) en verleent duidelijkheid over de bevoegdheid van een zorgverlener. Er staan meer dan 400.000 zorgverleners geregistreerd in het BIG-register. Iedereen kan het register raadplegen. Het BIG-register is er voor vele soorten zorgverleners, zoals apothekers, artsen, fysiotherapeuten, gezondheidszorgpsychologen, psychotherapeuten, tandartsen, verloskundigen en verpleegkundigen.
In het BIG-register kan men zien of een sollicitant bevoegd is. Ook kan men zien of er misschien een beperking van kracht is. Of een sollicitant bekwaam is moet een werkgever zelf vaststellen. Met een BIG-registratie:

- mag men de wettelijk beschermde beroepstitel voeren;
- mag men het beroep zelfstandig uitoefenen;
- mogen artsen, tandartsen en verloskundigen zelfstandig de voorbehouden handelingen uitvoeren;
- valt men onder het tuchtrecht;
- kan men starten met een opleiding tot specialist.

e. Tandarts (KRT register)

Het Kwaliteitsregister Tandartsen (KRT) wil dat het beroep tandarts op professionele wijze wordt uitgeoefend. Het KRT stimuleert de deskundigheid (vakkennis en vakbekwaamheid) van praktiserende tandartsen in Nederland en bevordert de patiëntveiligheid in de tandartspraktijk. Het KRT is hét onafhankelijke, openbare kwaliteitsregister van praktiserende tandartsen in Nederland. Sinds de start in 2007 is meer dan de helft van de praktiserende tandartsen in Nederland (eind 2010: 3.521 tandartsen) aangesloten.
Tandartsen die staan ingeschreven in het KRT committeren zich aan vijf normen die horen bij een professionele uitoefening van het beroep tandarts. Dit betekent dat ingeschreven tandartsen:

- officieel staan (onvoorwaardelijk) geregistreerd bij de overheid (BIG-registratie) en gemiddeld minimaal 14 uur per week tandheelkundige zorg aan patiënten verlenen;
- gedragsregels en (praktijk)richtlijnen naleven;
- minimaal 240 uur in vijf jaar besteden aan het bestuderen van (wetenschappelijke) vakliteratuur;
- geaccrediteerde bij- en nascholing volgen en regelmatig vakinhoudelijk overleg met collega's voeren;
- een klachtenregeling hebben die voldoet aan de Wet Klachtrecht Cliënten in de Zorgsector.

f. Advocaat (Nederlandse Orde van Advocaten)

Een advocaat wordt beëdigd als hij/zij voldoet aan de opleidingseisen die worden gesteld in de Advocatenwet en als men beschikt over een verklaring omtrent gedrag (VOG). De beëdiging leidt tot opname op het Landelijk Advocaten Tableau (LAT) van de Nederlandse Orde van Ad-

vocaten. De eerste 3 jaar na de inschrijving is men verplicht als stagiair te werken onder toezicht van een ervaren advocaat (een patroon). Het patronaat moet goedgekeurd zijn door de Raad van Toezicht.
Door een tuchtrechter kan beslist worden dat een advocaat wordt geschrapt of geschorst. De uitspraken van tuchtrechters zijn voor iedereen beschikbaar op de website www.tuchtrecht.nl. De Geschillencommissie behandelt geschillen volgens de regels zoals die zijn vermeld in het Reglement Geschillencommissie Advocatuur. De commissie is bevoegd te oordelen over klachten betreffende de kwaliteit van de dienstverlening van de advocaat, de hoogte van de declaratie in alle soorten zaken en schadeclaims met een maximum van € 10.000.

g. Ingenieur (KIVI NIRIA)

Het Koninklijk Instituut Van Ingenieurs KIVI NIRIA is de beroepsvereniging van ingenieurs en techniekstudenten. Het netwerk behartigt de belangen van ingenieurs en ondersteunt haar leden in hun beroepsuitoefening. KIVI NIRIA telt momenteel 25.000 leden en 500 netwerkactiviteiten per jaar.

KIVI NIRIA zet zich in voor de kwaliteit van het hoger technisch onderwijs in Nederland. De Europese Unie wordt als vestigingsgebied steeds belangrijker, KIVI NIRIA is actief in verschillende nationale, Europese en internationale netwerken.

Lid worden van KIVI NIRIA kunnen afgestudeerden en studenten van een technische universiteit in Nederland of de Rijksuniversiteit Groningen, de landbouwuniversiteit in Wageningen of aan een Nederlandse hogeschool in een technische of agrarische richting. Tevens afgestudeerden van een niet-technische HBO/WO met aantoonbare affiniteit voor techniek.

h. Technisch personeel luchtvaart (Kiwa Register)

Onderhoudstechnici spelen een centrale rol in de veiligheid van de luchtvaart. Daarom is er een Europese standaard waaraan zij moeten voldoen. Het Aircraft Maintenance Licence wordt uitgegeven door Kiwa Register. Er bestaan verschillende bevoegdverklaringen voor onderhoud en vrijgave van verschillende luchtvaartuigen. Welke hangt af van het soort toestel. Er zijn specifieke type ratings, opleidingen en examens.
Afhankelijk van de (sub)categorie die wordt aangevraagd, moet door de aanvrager een vastgesteld kennisniveau worden aangetoond van gerelateerde onderwerpen. Deze onderwerpen en het bijbehorende kennisniveau zijn per (sub)categorie nader gespecificeerd.
Afhankelijk van de categorie die wordt aangevraagd, moet door de aanvrager een vastgesteld aantal jaren ervaring worden aangetoond in de civiele luchtvaart. De hoeveelheid aan te tonen ervaring varieert niet alleen per categorie, maar is mede afhankelijk van de gevolgde opleiding. Daarnaast dient de verkregen ervaring recent en relevant te zijn.

Bijlage J: Interview mw. Neelie Kroes

Deze bijlage bevat de vragen over kwalificatie die zijn gesteld aan mw. Neelie Kroes, de Europese Commissaris voor ICT en Telecom, in het PvIB-interview over Trust and Security in de Digitale Agenda.

Questions:

- Does the EU have any plans on having to meet any international recognized qualification for information security professionals?
- What are the advantages in meeting international recognized qualification for information security professionals in the opinion of Ms. Kroes?
- Does the EU want a publicly available registry for information security professionals which public consultation is possible, similar to healthcare workers in the Netherlands (BIG registry, a registry for professionals working in healthcare), and if so, what are the main reasons in the opinion of Ms. Kroes for (not) wanting such a registry?
- Does EUROPASS provide in qualifications for information security professionals on a wider area then a pure technical area?

Answer:

> "In order to attract good people to working with ICT, in both the private and public sectors, it is very important to have skills frameworks and well-known career ladders. Through such tools ICT professionals can plan better and make smart choices.
> The European Commission is committed to developing tools to identify and recognise the competences of ICT practitioners and users by 2012. These should be developed in connection with the European Qualifications Framework (EQF) and EUROPASS, so as to make national qualifications more mutually recognised across Europe and to promote the mobility of information security professionals.
> As to a publicly available registry, I wonder whether this would not be better organised at the level of PvIB and your sister organisations?"

Europass

Europass geeft op een Europees uniforme manier gegevens over scholing, werkervaring, talenkennis en competenties weer. Dit levert een eenduidige beschrijving van kwalificaties en competenties op. Werkgevers kunnen zo eenvoudig matchen en kandidaten met elkaar vergelijken. Europass is een initiatief van de Europese Commissie om mobiliteit bij werken en leren binnen Europa te vergemakkelijken. Europass maakt het voor bedrijven eenvoudiger om personeel te selecteren en bevordert de mobiliteit van werknemers.

European Qualifications Framework (EQF)

Het European Qualifications Framework (EQF) beoogt de verschillende nationale kwalificatiesystemen te relateren aan een gemeenschappelijk Europees referentiekader. Individuen en

werkgevers zijn met het EQF in staat om de kwalificatieniveaus van verschillende landen en de verschillende opleiding- en trainingssystemen beter te begrijpen en te vergelijken.

EQF wordt in Europa sinds 2008 in praktijk gebracht en moedigt landen aan om hun nationale kwalificatiesystemen te relateren aan het EQF. Het streven is dat alle nieuwe kwalificaties vanaf 2012 aan het juiste EQF-niveau worden gerefereerd. EQF is toepasbaar voor alle soorten opleidingen, trainingen en kwalificaties.

Europees internationaliseringsbeleid

De Europese Commissie is een bron van allerlei initiatieven die te maken hebben met internationalisering. Voorbeelden hiervan zijn mobiliteitsprogramma's die streven naar transparantie van kwalificaties die in verschillende landen gebruikt worden. Deze benadering vanuit de Europese Unie vergemakkelijkt de vergelijkbaarheid van opleidingen.

Bijlage K: Enquêteresultaten

De vragenlijst in deze bijlage is ingevuld door personen die in hun dagelijkse werk met informatiebeveiliging te maken hebben. De 35 respondenten waren afkomstig van overheid, bedrijfsleven en onderwijs:

De vragen en de percentages waarmee het eens was zijn in onderstaande tabel weergegeven. De vragen zijn gesteld als ja/nee-vragen, maar met de mogelijkheid om het antwoord toe te lichten.

Vraag	Mee eens (%)
Wordt binnen uw organisatie informatiebeveiliging als een separate business professie gezien?	89
Vindt u het huidige aanbod van opleidingen (WO, HBO, MBO) voldoende?	50
Vindt u het zinvol dat professionals in de informatiebeveiliging een formele certificatie hebben waarvoor continue nascholing en uitbouw van ervaring verplicht is?	89
Vindt u dat de bestaande certificatieschema's voor professionals in de informatiebeveiliging voldoen aan de behoefte van uw organisatie?	46
Vindt u dat Nederland ervoor moet kiezen om kwalificatie- en certificatiesystemen op het gebied van informatiebeveiliging uit het buitenland over te nemen?	66
Vindt u dat een in Nederland gebruikt kwalificatie- en certificatiesysteem voor informatiebeveiliging (mede) beheerd moet worden door een Nederlandse instantie?	65
Vindt u dat een in Nederland uitgereikte kwalificatie of certificatie op het gebied van informatiebeveiliging in het buitenland erkend moet zijn?	81
Vindt u dat de Nederlandse overheid zich in voldoende mate bewust is van het belang van informatiebeveiliging voor de Nederlandse maatschappij en economie?	50
Vindt u dat de Nederlandse overheid een rol moet spelen in de professionalisering van informatiebeveiliging in Nederland?	50
Vindt u dat de Nederlandse overheid een rol moet spelen in de professionalisering van informatiebeveiliging in Europa?	54
Vindt u dat de Nederlandse overheid meer moet doen richting bedrijven om het belang van informatiebeveiliging te benadrukken?	65

De functies die genoemd zijn waarvoor momenteel onvoldoende reguliere opleidingen beschikbaar zijn als startkwalificatie: CERT-functionaris; Security Officer; CISO; ISO; Adviseur Informatiebeveiliging; Security Architect; Secure Programmer; alle ICT-gebruikers (awareness); ICT-forensisch onderzoeker; Integrale Beveiligingsambtenaar; Onderzoeker; Risicoanalist; Senior Security Consultant; Operational Security Officer.

Bijlage L: Afkortingen

Onderstaande tabel geeft de afkortingen weer die in het rapport voorkomen. De afkortingen van certificeringen in de informatiebeveiliging zijn opgenomen in bijlage M.

Afkorting	Betekenis
ANSI	American National Standards Institute
BIG	Beroepen in de individuele gezondheidszorg
BZK	Binnenlandse Zaken & Koninkrijksrelaties
CIBG	Centraal Informatiepunt Beroepen Gezondheidszorg
CISO	Chief/Corporate Information Security Officer
CPE	Continuing Professional Education Credits'
CPION	Centrum voor Post-Initieel Onderwijs Nederland
CPNI.NL	Centre for the Protection of National Infastructure Netherlands
CV	Curriculum Vitae
DNV	Det Norske Veritas
EA	European co-operation for Accreditation
ECABO	kenniscentrum beroepsonderwijs bedrijfsleven
EEMA	European association for e-identity and security
ENISA	European Network and Information Security Agency
EQF	European Qualifications Framework
EU	Europese Unie
EVC	Erkenning van eerder verworven competenties
EXIN	Exameninstituut Informatica
GvRM	Genootschap voor Risicomanagement
Hbo	Hoger beroepsonderwijs
HEC	Het Expertise Centrum
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants
IISP	Institute of Information Security Professionals
IRM	Informatierisicomanagement
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
(ISC)²	International Information Systems Security Certification Consortium
ISO	International Organization for Standardization
IT / ICT	Informatietechnologie / informatie- en communicatietechnologie
KRT	Kwaliteitsregister Tandartsen
LAT	Landelijk Advocaten Tableau
LRQA	Lloyd's Register Quality Assurance
Mbo	Middelbaar beroepsonderwijs

Afkorting	Betekenis
NBA	Nederlandse Beroepsorganisatie van Accountants
NCSS	Nationale Cyber Security Strategie
NEROB	Stichting Registers Risicomanagement
NICC	Nationale Infrastructuur tegen Cybercrime
NOREA	Nederlandse Orde van Register Edp Auditors
NVAO	Nederlands-Vlaamse Acceditatieorganisatie
PDO	Particulier Digitaal Onderzoeker
PvIB	Platform voor Informatiebeveiliging
RvA	Raad van Accreditatie
SCADA	Supervisory Control And Data Acquisition
SVPB	Stichting Vakexamens voor de Particuliere Beveiligingsorganisaties
VKA	Verdonck, Klooster & Associates
VOG	Verklaring omtrent gedrag
V&W	Verkeer & Waterstaat
WO	Wetenschappelijk onderwijs

Bijlage M: Afkortingen van certificeringen informatiebeveiliging

Deze tabel bevat een niet uitputtende lijst namen van certificeringen en de daarvoor gehanteerde afkortingen die door professionals in het vakgebied informatiebeveiliging worden gebruikt.

Afkorting	Betekenis
ABCP	Associate Business Continuity Professional
CAP	Certified Authorization Professional
CBCP	Certified Business Continuity Professional
CEH	Certified Ethical Hacker
CGEIT	Certified in the Governance of Enterprise Information Technology
CIA	Certified Internal Auditor
CIPP	Certified Information Privacy Professional
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CITP	Certified Information Technology Professional
CRISC	Certified in Risk and Information Systems Control
CSSLP	Certified Secure Software Lifecycle Professional
FBCI	Fellow of the Business Continuity Institute
FBCS	Fellow of the British Computer Society
ISMAS	Information Security Management Advanced
ISMES	Information Security Management Expert
ISSAP	Information Systems Security Architecture Professional
ISSEP	Information Systems Security Engineering Professional
ISSMP	Information Systems Security Management Professional
MBCP	Master Business Continuity Professional
MISM	Master of Information Security Management
MSIT	Master of Security in Information Technology
OPSA	OSSTMM Professional Security Analyst
OPST	OSSTMM Professional Security Tester
QiCA	Qualification in Computer Auditing
RE	Register EDP auditor
RIB	Register Informatie Beveiliger
RO	Register Operational auditor
RSE	Register Security Expert
SSCP	Systems Security Certified Practitioner

Bijlage N: Terminologie en definities

Deze tabel bevat de betekenis van een aantal belangrijke termen en begrippen die in dit document worden gebruikt.

Term	Beschrijving
Accreditatie	Procedure waarbij een autoriteit bezittende organisatie (de accreditatieorganisatie) een formele erkenning uitspreekt dat een entiteit (de certificatie-instantie) bekwaam is specifieke taken uit te voeren [ISO/IEC Guide 2].
Beroepsprofiel	Een beschrijving van een beroep, waarin ook de eisen beschreven zijn die aan de beroepsbeoefenaar gesteld worden.
Certificaat	Een schriftelijke document waarin een daartoe bevoegde instantie verklaart dat een product, dienst, of persoon aan specifieke eisen voldoet. Toelichting: Een persoonscertificaat is een certificaat betreffende de vakbekwaamheid van een bepaalde persoon. Een diploma van een met goed gevolg afgelegd examen van een opleiding is een certificaat. Het bewijs van toelating tot een beroepsregister is ook een certificaat.
Certificatie	Een procedure waarbij een onpartijdige, competente en daartoe bevoegde organisatie een document (certificaat) afgeeft als officiële verklaring dat een product, dienst, of persoon aan specifieke eisen voldoet [ISO/IEC Guide 2].
Certificatie-instantie	Een onpartijdige, competente en daartoe bevoegde organisatie die certificaten afgeeft.
Certificatieregister	Een centraal register waarin aangegeven is welke personen een bij het register behorend certificaat behaald hebben.
Certificatieschema	Een verzameling criteria en procedures volgens welke een certificatie-instantie beoordeelt of een product, dienst, of persoon voldoet aan een gegeven norm.
Competentie	Een geschikheidsbepalende component, bestaande uit kennis, inzicht, vaardigheden en/of houding. Toelichting: Beroepscompetenties zijn de competenties, oftewel de kennis, inzicht, vaardigheden en houding die nodig zijn voor de uitoefening van een bepaald beroep.
Competentieniveau	Een bepaald niveau van een competentie, oftewel kennis, inzicht, vaardigheden en/of houding. Toelichting: Competentieniveaus worden gedifferentieerd naar de context waarbinnen een competentie ingezet wordt en de wijze van sturing die daarbij van toepassing is.

Term	Beschrijving
Conformiteitsbeoordeling	Een procedure waarin wordt beoordeeld of een product, dienst, of persoon aan specifieke eisen voldoet.
Conformiteitsverklaring	Een schriftelijk document waarin een daartoe bevoegde instantie verklaart dat een product, dienst, of persoon aan specifieke eisen voldoet. Toelichting: Een conformiteitsverklaring is een certificaat.
Grandfathering	Het voor bepaalde tijd en/of bepaalde groep laten gelden van de oude regelgeving, terwijl voor alle andere gevallen de nieuwe regelgeving van toepassing is.
Informatiebeveiliging	Het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening te waarborgen.
Informatierisicomanagement	Het proces of het vakgebied dat beoogt de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening te waarborgen. Toelichting: Informatierisicomanagement is een onderdeel van (corporate) risicomanagement.
Informatierisicomanager	Een persoon of een functie die invulling geeft aan informatierisicomanagement.
ICT-beveiliger	Een persoon of een functie die invulling geeft aan ICT-beveiliging.
ICT-beveiliging (IT security)	Het proces of het vakgebied dat beoogt de ICT (de geautomatiseerde informatievoorziening) te beveiligen. Toelichting: ICT-beveiliging omvat het plannen, realiseren, beheren en evalueren van ICT-beveiligingsmaatregelen.
Kwalificatie	Een formeel resultaat van een beoordelings- en validatieproces, dat wordt verworven wanneer een bevoegde instantie bepaalt dat de capaciteiten van een product, dienst, of persoon aan bepaalde eisen beantwoorden.
Norm	Een eisenstellend document. Toelichting: De eisen in een norm zijn zodanig verwoord dat in een gegeven situatie beoordeeld kan worden of aan de eisen voldaan wordt.
Opleidingsprofiel	Een beschrijving van de opleiding die voor de uitoefening van een bepaald beroep nodig is.