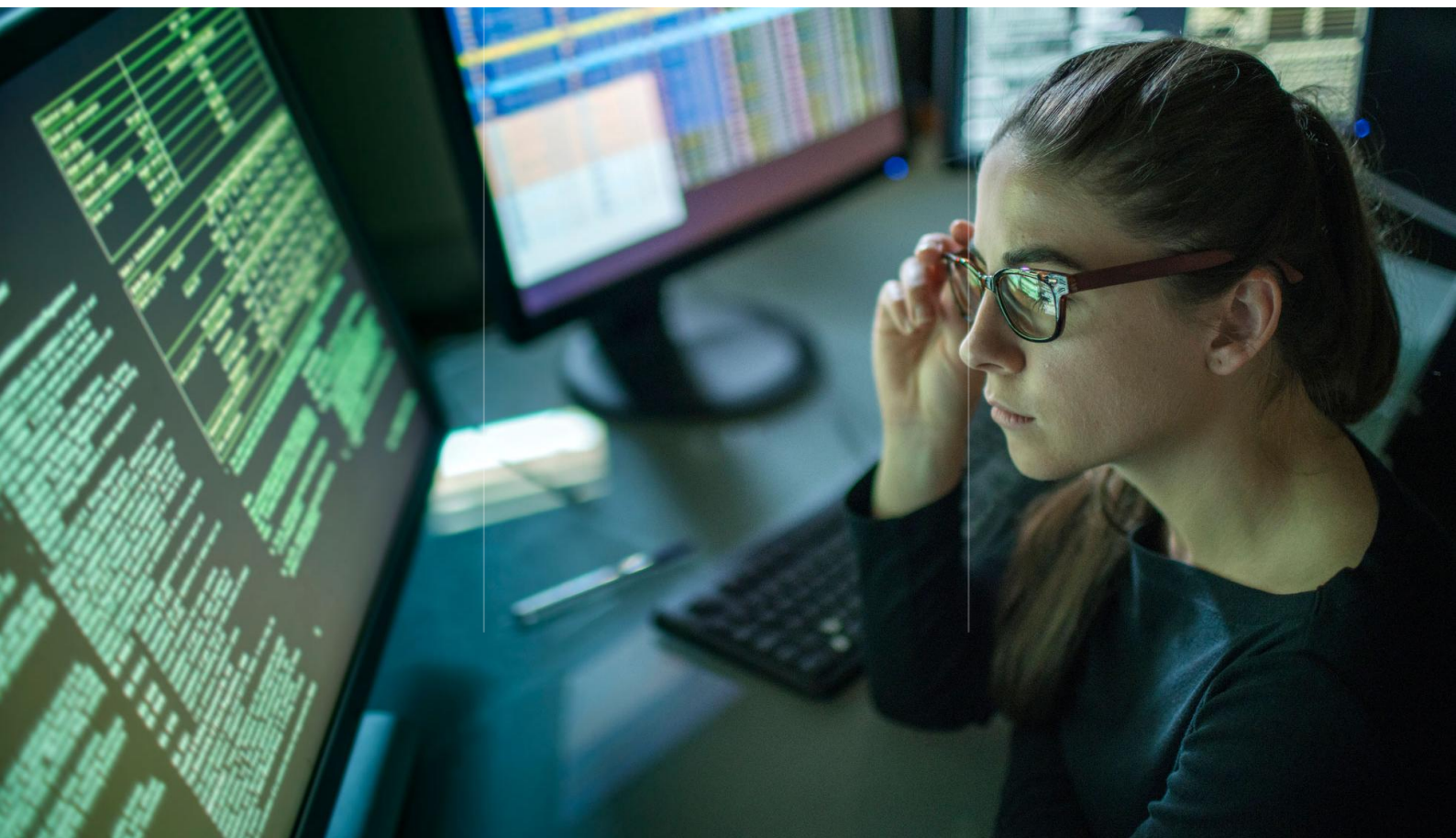




RAPPORT

Certificering van cyberprofessionals in Nederland

Een verkenning naar passende
vormen van persoonsgebonden
kwaliteitsborging

14 september 2026

I.S. Sloover, L. Stadhouders, A. Schrijver en K. Schaafstra

Berenschot



Inhoudsopgave

Managementsamenvatting	3
Hoofdstuk 1.....	5
Inleiding.....	5
1.1 Context, vraag- en doelstelling van het verkennende onderzoek.....	5
1.2 Onderzoeksaanpak	6
1.3 Leeswijzer	7
Hoofdstuk 2.....	8
Bevindingen en analyse.....	8
2.1 Feitelijke bevindingen.....	8
2.2 Beelden en meningen uit de (groeps-)interviews	12
2.3 Analyse	16
Hoofdstuk 3.....	20
Mogelijke vormen van certificering	20
3.1 Ontwerpprincipes	20
3.2 Van principes naar ontwerp: mogelijke vormen.....	23
3.3 Beslisboom persoonscertificering cyberprofessionals.....	25
Hoofdstuk 4 Conclusies en Aanbevelingen.....	30
Conclusies en aanbevelingen.....	30
4.1 Conclusies.....	30
4.2 Aanbevelingen	32
Bijlage 1. Overzicht gesprekspartners	35
Bijlage 2. Kader conformiteitsbeoordeling.....	36

Managementsamenvatting

Het doel van de verkenning is om inzicht te krijgen in mogelijke vormen van persoonscertificering van cyberprofessionals en geïnformeerd een mening te kunnen vormen over welke vormen van certificering passend en haalbaar kunnen zijn voor de cybersecuritysector om vervolgstappen op korte en/of langere termijn te kunnen zetten. De bevindingen in deze eerste verkenning berusten op een selectie van openbare bronnen, een globale vergelijking met twee landen en gesprekken met een beperkt aantal betrokkenen, die niet representatief zijn voor de breedte van de sector.

Nederland kent momenteel geen samenhangend stelsel voor persoonsgebonden kwaliteitsborging van cyberprofessionals. De bestaande kwaliteitsborging richt zich vooral op organisaties, producten en diensten, terwijl op persoonsniveau private, vaak internationale certificeringen dominant zijn. Deze certificeringen spelen een belangrijke rol in werving, selectie en opdrachtverlening, maar verschillen sterk in inhoud, toetsingsvorm, ervaringsvereisten, kosten en eisen voor hercertificering. Daardoor is voor opdrachtgevers niet altijd duidelijk welk certificaat relevant of voldoende is voor een specifieke opdracht. De RE-functie is in Nederland wel aantoonbaar geslaagd, omdat deze via een beschermde titel, praktijkervaring, gedragsregels, permanente ontwikkeling en tuchtrecht een duurzaam systeem voor persoonsgebonden kwaliteitsborging biedt.

De verkenning bevestigt dat cybersecurity een breed en heterogeen vakgebied is. Rollen zoals pentester, incident responder, security architect, IT-auditor, CISO en security consultant verschillen wezenlijk in werkzaamheden, benodigde kennis, praktijkvaardigheden en verantwoordelijkheden. Een generieke certificering kan daarom hooguit iets zeggen over een gemeenschappelijke basis, zoals integriteit, vertrouwelijkheid, risicobewustzijn, ethiek en permanente ontwikkeling. Zij biedt echter beperkt bewijs dat iemand een specifieke technische, auditmatige of bestuurlijke taak deskundig kan uitvoeren. Vooral waar rol, vaardigheden en praktijktoetsing sterk samenkomen, zoals bij pentesten, lijkt rolspecifieke certificering kansrijker.

Uit de interviews blijkt dat het onderliggende probleem niet eenduidig wordt ervaren. De beroepsgroep is nog relatief jong en de markt en technologie veranderen constant. Respondenten verschillen van mening over de vraag of onvoldoende individuele vakbekwaamheid daadwerkelijk een breed maatschappelijk probleem vormt. Wel is er een herkenbaar vraagzijdeprobleem: met name kleinere en minder cybervolwassen opdrachtgevers lijken moeite te hebben om de kwaliteit van aanbieders en professionals te beoordelen. Zij kunnen vaak niet goed inschatten of een certificaat, referentie of functietitel aansluit bij de aard en risico's van een opdracht. Persoonscertificering kan dit probleem gedeeltelijk verminderen, maar is geen vervanging voor goede inkoopvoorwaarden, referenties, organisatiekeurmerken, praktijkassessments en inhoudelijke gesprekken. Naarmate certificering specialistischer wordt, neemt de inhoudelijke waarde toe, maar wordt de betekenis ervan voor niet-specialistische opdrachtgevers juist minder eenvoudig te duiden.

Een belangrijk aandachtspunt is dat een certificaat altijd een momentopname is. De ontwikkeling van technologie, dreigingen, wetgeving en AI gaat sneller dan veel opleidingen, normenkaders en examens kunnen bijhouden. Zonder aantoonbare permanente ontwikkeling, actuele praktijkervaring en periodieke herbeoordeling ontstaat het risico van schijnzekerheid. Een toekomstig stelsel van persoonscertificering zou daarom niet uitsluitend op kennistoetsen moeten

berusten, maar afhankelijk van het specialisme gebruik moeten maken van bijvoorbeeld praktijkexamens, simulaties, portfolio's, referenties, peer review en ervaringsverificatie. Tegelijkertijd moet worden voorkomen dat herregistratie verwordt tot een administratieve puntentelling zonder aantoonbare relatie met actuele vakbekwaamheid.

De internationale vergelijking in dit verkennende onderzoek biedt relevante aanknopingspunten. Het Europese Cybersecurity Skills Framework (ECSF) biedt een bruikbaar ordenend kader voor rollen, taken, kennis, vaardigheden en competenties, maar is zelf geen certificeringsstelsel. Het Verenigd Koninkrijk laat zien hoe professionele registratie kan worden gecombineerd met niveaus van erkenning, specialismen, gedragsregels, permanente ontwikkeling en onafhankelijke beoordeling. Het Litouwse voorbeeld benadrukt dat certificering vooral betekenis krijgt als onderdeel van een bredere aanpak voor onderwijs, arbeidsmarktontwikkeling en vaardigheden. Voor Nederland lijkt aansluiting op Europese kaders en het zichtbaar maken van de relatie tussen bestaande certificaten en ECSF-rolprofielen meer voor de hand te liggen dan het ontwikkelen van een volledig losstaand nationaal stelsel.

De meest passende richting lijkt een gelaagd en gefaseerd model. Dit kan bestaan uit een lichte basisregistratie voor algemene professionaliteit, vrijwillige rolspecifieke certificering voor afgebakende specialismen en een expertstatus op basis van aantoonbare praktijkervaring en beoordeling door vakgenoten. Een dergelijke aanpak moet beginnen bij specialismen waar drie factoren samenkomen: een substantieel risico bij ondeugdelijke uitvoering, beperkte zichtbaarheid van kwaliteit voor opdrachtgevers en voldoende scherp te formuleren en te toetsen competenties. Een wettelijke verplichting tot certificering ligt op dit moment niet voor de hand. Zelfregulering en co-regulering met de overheid bieden meer ruimte voor actualisatie en aansluiting op de internationale markt. Wettelijke verankering lijkt hooguit op termijn te kunnen worden overwogen voor scherp afgebakende werkzaamheden met een hoog publiek risico, indien lichtere instrumenten aantoonbaar tekortschieten.

Een generiek cybersecurityregister lijkt op dit moment niet de meest logische route. Daarvoor is het onderliggende kwaliteitsprobleem nog onvoldoende scherp afgebakend en is de cybersecuritysector te divers. Eventuele vervolgstappen zouden kunnen zijn om inzichtelijk te maken wat het veronderstelde probleem is, welke categorisering er is van certificeringen, het ondersteunen van opdrachtgevers en het aansluiten bij Europese kaders. Onderzoek daarna - bijvoorbeeld in de vorm van een pilot - bij enkele afgebakende hoog-risicospecialismen of onafhankelijke en praktijkgerichte certificering aantoonbaar meerwaarde biedt ten opzichte van bestaande instrumenten.

HOOFDSTUK 1

Inleiding

1.1 Context, vraag- en doelstelling van het verkennende onderzoek

Context

Dit verkennende onderzoek is uitgevoerd als onderdeel van werktafel 2 (Vraag & Aanbod) van het Digitaal Talent Nederland – Cyber programma. Het Digitaal Talent Nederland – Cyber programma, in opdracht van het Ministerie van Economische Zaken en Klimaat, is gestart en wordt uitgevoerd door Platform Talent voor Technologie (PTvT) en het NCC-NL. De co-voorzitters van werktafel 2, Bibi van den Berg en Liesbeth Holtermann, hebben het verzoek voor een onderzoek en verkenning van een cyberregister besproken en voorbereid met Berenschot. Dit onderzoek en verkenning naar een cyberregister in Nederland komt voort uit de behoefte van Nederlandse stakeholders in cybersecurity.

De Nederlandse cybersecuritysector staat voor een professionaliseringsvraagstuk dat kenmerkend is voor relatief jonge, kennisintensieve beroepsgroepen. Het vakgebied van cybersecurity is in korte tijd gegroeid van een technische niche tot een discipline waarvan de continuïteit van vitale (bedrijfs)processen, bedrijfsvoering en publieke en private dienstverlening afhankelijk is. Tegelijkertijd neemt bijvoorbeeld de complexiteit van cyberdreigingen door uiteenlopende actoren toe, heeft AI een grote vlucht genomen en is er diverse wet- en regelgeving zoals de Cyberbeveiligingswet (NIS2), Wet weerbaarheid kritieke entiteiten, DORA (Digital Operational Resilience Act) en Cyber Resilience Act (CRA) en de AI Act.

In veel sectoren waarin beroepsgroepen met grote c.q. vitale belangen omgaat, bestaat in Nederland een vorm van persoonsgebonden kwaliteitsborging. Artsen staan bijvoorbeeld in het BIG-register, advocaten zijn geregistreerd in het Landelijk Advocaten Tableau (LAT) en notarissen in het Register Notariaat van de Koninklijke Notariële Beroepsorganisatie (KNB). Waar in de loop der tijd stelsels van persoonsgebonden kwaliteitsborging (persoonscertificering) zijn ontstaan, ontbreekt zo'n stelsel voor cyberprofessionals in Nederland vrijwel geheel. Nederland kent wel een certificeringslandschap voor cybersecurity, maar dit ziet met name op het niveau van organisaties, producten of diensten, maar niet direct op *personen*. Wie in Nederland bijvoorbeeld als pentester, security consultant of CISO aan de slag wil, hoeft daarvoor in principe geen enkele toets te maken en er is geen algemeen register of (centrale)instantie die bijvoorbeeld toezicht erop houdt. Bovendien is van belang om het probleem precies te formuleren. Het ontbreken van persoonscertificering en afwezigheid van een algemeen register betekent niet automatisch dat één generiek register de juiste oplossing is. De cybersecuritysector bestaat immers uit sterk verschillende beroepspraktijken. De kennis, vaardigheden en verantwoordelijkheden van bijvoorbeeld een CISO, pentester, SOC-analist, incident responder, auditor, security-architect of OT-securityspecialist zijn onderling moeilijk vergelijkbaar.

Vraagstelling en doelstellingen

Bovenstaande omschrijving roept de vraag op welke vorm van persoonscertificering passend zou kunnen zijn voor professionals in de cybersecuritysector in Nederland.

Opdrachtgever voor dit verkennende onderzoek zijn Prof. dr. Bibi van den Berg (Hoogleraar Cybersecurity Governance verbonden aan de Universiteit Leiden), Liesbeth Holtermann (Directeur bij Cyberveilig Nederland) en Pritti Rana (Programma coördinator bij NCC NL). De opdrachtgever wil verkennen welke wijze van certificering zou kunnen bijdragen aan een versteviging van de kwaliteitsborging in de cybersector in Nederland. De arbeidsmarkt heeft namelijk vooral behoefte aan professionals met hoogwaardige kennis en skills. Er is op dit moment geen voldoende sterke kwaliteitsborging met risico's voor de digitale veiligheid van organisaties en van Nederland. Een systeem van persoonscertificering kan de kwaliteitsborging verbeteren en daarmee de kennis en skills van professionals versterken en zo de risico's voor de digitale veiligheid terugbrengen. Deze verkenning heeft de volgende doelstellingen:

- Inzicht krijgen in de mogelijke vormen voor certificering van cyberprofessionals in algemene zin. Bijvoorbeeld: welke vormen bestaan er, hoe zijn zij opgebouwd, welke mechanismen maken dat zij wel of niet werken en welke randvoorwaarden vragen zij?
- Geïnformeerd een mening kunnen vormen over welke vormen van certificering passend en haalbaar kunnen zijn voor de cybersector om vervolgstappen op korte en/of langere termijn te kunnen zetten.

Bij de interpretatie van de onderzoeksbevindingen is terughoudendheid betracht ten aanzien van bevestigingsbias. In gesprekken, desk research en interne reflectie bestaat het risico dat de gekozen vraagstelling de richting van de analyse beïnvloedt. Dat geldt temeer bij een onderwerp als certificering, omdat het vertrekpunt al snel suggereert dat certificering ook de meest logische oplossingsrichting is. In deze verkenning is certificering daarom niet als doel op zichzelf beschouwd, maar als één mogelijk instrument binnen een breder stelsel van kwaliteitsborging. Alternatieven, beperkingen en ongewenste neveneffecten, zoals schijnzekerheid, toetredingsbarrières en verdere fragmentatie, zijn expliciet meegewogen.

1.2 Onderzoeksaanpak

Op hoofdlijnen bestaat het onderzoek uit de volgende stappen:

- Startgesprek
- Oriëntatie cybersecuritysector en certificering, vergelijken met andere persoonscertificering, documentenstudie
- (groeps)interviews op basis van een selectie van door opdrachtgever en onderzoekers aangedragen partijen (zie bijlage 1 voor een overzicht van organisaties)
- Tussentijdse afstemming en overleggen met opdrachtgever over inhoudelijke aspecten en reikwijdte van het onderzoek
- Conceptrapport opstellen, ter reactie aan opdrachtgever
- Verwerken reacties en eindrapport opleveren.

In ons werk maakt Berenschot waar passend gebruik van generatieve AI ter ondersteuning, bijvoorbeeld bij documentanalyse en het opstellen van conceptteksten. Wanneer vertrouwelijke, herleidbare of anderszins niet-openbare informatie wordt verwerkt, gebeurt dit uitsluitend binnen daarvoor goedgekeurde, beveiligde en afgeschermdde omgevingen, waaronder een beveiligde Microsoft Azure-omgeving binnen de EER, waarbij data niet wordt gebruikt voor trainingsdoeleinden. De verwerking van (persoons-)gegevens vindt plaats conform AVG-richtlijnen, de Europese AI act en het informatiebeveiligingsbeleid van Berenschot. AI ondersteunt de analyse, maar alle resultaten worden inhoudelijk beoordeeld door een adviseur, die eindverantwoordelijk blijft.

1.3 Leeswijzer

Dit rapport betreft een verkennend onderzoek naar de mogelijke vormen van certificering van cybersecurityprofessionals in Nederland. Het doel van deze verkenning is niet om definitieve conclusies te trekken of een uitputtend oordeel te geven over de wenselijkheid van specifieke oplossingsrichtingen, maar om relevante ontwikkelingen, perspectieven, kansen en aandachtspunten in kaart te brengen. De bevindingen uit deze verkenning dienen daarom te worden geïnterpreteerd als richtinggevende inzichten die kunnen bijdragen aan verdere beleidsvorming, discussie en eventueel vervolgonderzoek. Deze verkenning gaat over certificering van personen, niet van bedrijven, instellingen, producten of diensten. Certificering op organisatieniveau komt in deze verkenning alleen aan de orde indien dat samenhangt met persoonscertificering.

Het rapport bestaat uit vier hoofdstukken. In hoofdstuk 2 staan de bevindingen uit dit verkennende onderzoek en de analyse van de onderzoekers. In hoofdstuk 3 staan mogelijke vormen van certificering. De conclusies en aanbevelingen volgen in hoofdstuk 4. Het rapport heeft 2 bijlagen.

HOOFDSTUK 2

Bevindingen en analyse

In dit hoofdstuk komen eerst de feitelijke bevindingen aan bod. Daarna volgt een weergave van de beelden en meningen vanuit de interviews en daarna de analyse van de onderzoekers.

2.1 Feitelijke bevindingen

In een eerste verkenning van diverse openbare bronnen is op hoofdlijnen onderzocht of al eerder onderzoek is gedaan naar persoonscertificering van cyberprofessionals in Nederland. Daarnaast is op verzoek van opdrachtgevers op hoofdlijnen bekeken op welke wijze het Verenigd Koninkrijk en Litouwen de persoonscertificering van cyberprofessionals hebben georganiseerd. Verder is een korte beschrijving gegeven van het Nederlandse- en Europese landschap op het gebied van certificering van cyberprofessionals.

2.1.1 Het Europese landschap

ENISA

Op EU-niveau richt de Cybersecurity Act zich uitdrukkelijk op producten, diensten en processen, niet op personen.¹ Wel heeft ENISA het European Cybersecurity Skills Framework (ECSF)² ontwikkeld, dat twaalf rolprofielen onderscheidt met bijbehorende taken, vaardigheden en kennisgebieden. Het ECSF is echter geen certificeringsschema voor cyberprofessionals, maar een ordenend raamwerk. Het ECSF biedt een gemeenschappelijke Europese taal voor cybersecurityberoepen. De twaalf profielen vertalen functies naar missies, taken, kennis, vaardigheden en competenties en kunnen daarmee richting geven aan opleiding, loopbaanontwikkeling en eventuele persoonscertificering.

Op Europees niveau is het ECSF het belangrijkste referentiepunt. De Europese Commissie heeft deze lijn versterkt met de Cybersecurity Skills Academy. Deze academie is bedoeld om bestaande initiatieven voor cybervaardigheden beter te coördineren, de skills gap te verkleinen en scholing, *upskilling* en *reskilling* zichtbaarder te maken. De Commissie plaatst dit nadrukkelijk in de context van toenemende dreigingen en Europese verplichtingen. De Europese benadering richt zich daarmee op het versterken van competenties, opleidingsroutes en arbeidsmarktmobiliteit. Relevant is verder dat ENISA inmiddels een koppeling (*'mapping'*) faciliteert van bestaande certificeringen op het ECSF³. Certificerende partijen kunnen hun certificeringen koppelen aan ECSF-rolprofielen. Dat helpt professionals om te zien welke certificeringen passen bij hun loopbaanontwikkeling en helpt organisaties om upskilling- en reskillingpaden te structureren langs rollen en competenties.

Beknopte landenstudie

De context van dit verkennende onderzoek in vergelijking met het Verenigd Koninkrijk (VK) en Litouwen wijst op enkele relevante ontwikkelingen: het VK-model van professionele registratie en de Litouwse benadering van cybersecurityskills en workforceontwikkeling. Hieronder staat een korte toelichting van beide stelsels.

¹ Rijksinspectie Digitale Infrastructuur, Cybersecurity certificering (NCCA); Verordening (EU) 2019/881 (Cybersecurity Act).

² ENISA, European Cybersecurity Skills Framework (ECSF).

³ <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf>

Verenigd Koninkrijk

Het VK biedt een institutioneel uitgewerkt voorbeeld van persoonsgebonden kwaliteitsborging. De UK Cyber Security Council kent vier professionele titels⁴: Associate Cyber Security Professional, Practitioner Cyber Security Professional, Principal Cyber Security Professional en Chartered Cyber Security Professional. Deze titels benadrukken oplopende niveaus van expertise, zelfstandigheid, verantwoordelijkheid en professionele ontwikkeling. Kandidaten moeten aantonen dat hun kennis en ervaring aansluiten bij de Standard for Professional Competence and Commitment en zich verbinden aan een *code of ethics*.

Het VK-model is niet uitsluitend generiek. De UK Cyber Security Council heeft de professionele standaard in een kader geplaatst voor acht specialismen⁵: Cyber Security Audit & Assurance, Security Testing, Secure System Architecture and Design, Secure Operations, Incident Response, Cyber Security Governance and Risk Management, Secure Systems Development en Cyber Security Management.

Ook de governance van het VK-model is relevant. De UK Cyber Security Council stelt de professionele standaard vast, maar werkt met licensed bodies die aanvragen behandelen en aanbevelingen doen over toekenning van titels. De Standard for Professional Competence and Commitment bevat onder meer bepalingen over het registratieproces, een professioneel register, revalidatie, disciplinary and appeal process en continuïng professional development⁶. Het model combineert normstelling, beoordeling door erkende partijen, permanente ontwikkeling en herkenbare titelvoering.

Deze professionele standaard wordt bovendien als beleidsinstrument ingezet. In 2024 heeft de regering uitgesproken dat zij UK Cyber Security Council-standaarden wil inbedden in haar cyber workforce, onder meer door het Government Security Career Framework te mappen op de titels en specialismen van de UK Cyber Security Council⁷. De overheid ziet dit als manier om meer duidelijkheid te creëren voor werkgevers, loopbaanpaden te structureren en de complexe markt van kwalificaties overzichtelijker te maken.

Litouwen

Litouwen biedt een ander type voorbeeld. Daar ligt de nadruk meer op het ontwikkelen van een nationaal cybersecurityskills-ecosysteem. De Cybersecurity Skills Strategy Lithuania uit 2025, opgesteld binnen het Europese CyberHubs-project, richt zich op het ontwikkelen van een hooggekwalificeerde en adaptieve cybersecurity workforce⁸. De strategie benoemt twee herkenbare problemen: een tekort aan professionals en de behoefte aan veelzijdige specialisten die meerdere ENISA-rollen kunnen bestrijken.

De Litouwse strategie zet vooral in op modernisering van opleidingen, praktische ontwikkeling van vaardigheden, internationale certificeringsmogelijkheden, publiek-private samenwerking en bewustwording. Daarbij worden specifieke marktbehoeften benoemd, onder meer CISO's, security

⁴ <https://www.ukcybersecuritycouncil.org.uk/for-individuals/become-professionally-registered/professional-titles>

⁵ <https://www.ukcybersecuritycouncil.org.uk/for-individuals/become-professionally-registered/specialisms>

⁶ <https://www.ukcybersecuritycouncil.org.uk/for-individuals/become-professionally-registered/professional-standards> en <https://www.ukcybersecuritycouncil.org.uk/base/media/docs/the-uk-csc-spcc-4-2-final.pdf>

⁷ <https://www.gov.uk/government/publications/government-statement-on-the-adoption-of-uk-cyber-security-council-standards/statement-from-hm-government-on-the-adoption-of-uk-cyber-security-council-standards> en <https://www.ncsc.gov.uk/organisation/uk-cyber-security-council/about-uk-cyber-security-council>

⁸ <https://cyberhubs.eu/resource/cybersecurity-skills-strategy-lithuania/>

managers en incident respons-specialisten. Ook wordt in de strategie benadrukt dat naast technische expertise ook management-, juridische- en communicatieve vaardigheden nodig zijn.

Deze benadering sluit aan bij eerder Litouws werk aan een 'cybersecurity competence map'⁹. Dat onderzoek had tot doel om de vraag naar cybersecurityspecialisten in Litouwen en internationaal in beeld te brengen, loopbaanpaden te bepalen, werkrollen te onderscheiden en aanbevelingen te doen om specialisten aan te trekken en competenties verder te ontwikkelen.

2.1.2 Het Nederlandse landschap: kwaliteitsborging vooral georganiseerd op organisatieniveau, producten of diensten

Het Nederlandse certificeringslandschap voor cybersecurity is vooral gericht op het niveau van organisaties, producten of diensten. De Rijksinspectie Digitale Infrastructuur vervult als National Cybersecurity Certification Authority de rol die de Europese Cybersecurity Act voorschrijft en ziet toe op certificering van ICT-producten, -diensten en -processen. Het Centrum voor Criminaliteitspreventie en Veiligheid beheert, in samenwerking met onder meer Cyberveilig Nederland, een reeks keurmerken voor cybersecuritydiensten: pentesten, awarenessstraining, incident response en sinds 2026 ook monitoring.¹⁰ Het Nationaal Cyber Security Centrum liet onderzoek doen naar het certificeringslandschap na de intrede van de Cybersecurity Act waarbij persoonscertificering van cyberprofessionals niet expliciet een onderdeel was.¹¹ De Nederlandse Cybersecuritystrategie 2022-2028 benoemt verder onder andere de arbeidsmarkt als pijler, maar niet persoonscertificering als beleidsinstrument.¹² Het recente arbeidsmarktonderzoek van Platform Talent voor Technologie en Dialogic signaleert kwaliteitsverschillen tussen opleidingen en certificeringen als knelpunt, maar werkt geen stelsel uit van persoonscertificering voor cyberprofessionals.¹³

2.1.3 Veel private certificeringen van private (internationale) bedrijven

In Nederland is door het ontbreken van een algemeen beroepsregister of publiek certificeringsstelsel voor cyberprofessionals in de praktijk een markt ontstaan waarin private, vaak internationale certificeringen een belangrijke rol vervullen. De oorsprong daarvan ligt vooral in de behoefte van werkgevers, opdrachtgevers en professionals aan herkenbare validatie van kennis, ervaring of specialisatie in een snelgroeiend en internationaal vakgebied. Het eerdere Nederlandse onderzoek uit 2011 (zie volgende paragraaf 2.1.4) constateerde al dat er een grote verscheidenheid aan titels en certificaten bestond en ook dat de betekenis en onderlinge waarde daarvan lastig te duiden waren.

Bekende voorbeelden zijn onder andere CISSP van ISC2, CISM en CISA van ISACA, CEH van EC-Council, OSCP van OffSec en diverse GIAC/SANS- en cloudcertificeringen. Deze certificeringen verschillen sterk in aard en bewijskracht. Sommige richten zich vooral op brede kennis, governance of management, zoals CISSP en CISM. CISSP vereist bijvoorbeeld vijf jaar relevante werkervaring in ten minste twee securitydomeinen. CISM en CISA kennen daarnaast verplichtingen voor permanente educatie (PE) om de certificering te behouden. Andere certificeringen zijn sterker praktijkgericht. OSCP toetst bijvoorbeeld hands-on vaardigheden via een praktijkexamen waarin kandidaten systemen moeten compromitteren, privileges verhogen en hun bevindingen documenteren.

⁹ <https://scispace.com/papers/cybersecurity-competence-map-of-lithuania-252dxwrx>

¹⁰ Centrum voor Criminaliteitspreventie en Veiligheid, Keurmerken Cybersecurity; Cyberveilig Nederland, Activiteiten en Nieuw keurmerk monitoring (certificering mogelijk vanaf 1 mei 2026).

¹¹ Tilburg Institute for Law, Technology, and Society, Het Nederlandse cybersecurity certificeringslandschap na de intrede van de Cybersecurity Act, i.o.v. het Nationaal Cyber Security Centrum.

¹² Nationaal Coördinator Terrorismebestrijding en Veiligheid, Nederlandse Cybersecuritystrategie 2022-2028, pijler IV en het bijbehorende actieplan.

¹³ Platform Talent voor Technologie & Dialogic, Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity, i.o.v. het ministerie van Economische Zaken en Klimaat, 2024.

2.1.4 Eerder Nederlands onderzoek, maar geen implementatie

De vraag naar persoonscertificering van cyberprofessionals is in Nederland eerder onderzocht en tot in de ontwerpfasen uitgewerkt, maar heeft destijds niet tot een operationeel stelsel geleid. In april 2011 verscheen "*Onderzoek naar kwalificatie en certificatie van informatiebeveiligers*" van Marcel Spruit en Fred van Noord, uitgevoerd vanuit VKA/HEC in samenwerking met CPNI.NL. Het onderzoek betrof, in het kort gezegd, expliciet de wenselijkheid en haalbaarheid van een nationaal kwalificatie- en certificatiestelsel voor *informatiebeveiligers*, met de mogelijkheid om in een later stadium aansluiting te zoeken bij internationale gremia. Het rapport benoemt diverse bouwstenen van een persoonscertificeringsstelsel: een beroeps- en opleidingsprofiel, een onafhankelijke certificatie instantie, een openbaar certificatieregister, opleidingen, gedrags- en beroepsregels, eisen voor bij- en nascholing (permanente educatie) en tuchtrecht. Over de governance was de conclusie dat de trekkersrol bij voorkeur bij één of meer beroepsorganisaties zou liggen, waarbij het Platform voor Informatiebeveiliging het meest voor de hand lag. De later opgestelde profielschetsen waren vooral gericht op informatiebeveiligers, niet op het bredere spectrum van cyberprofessionals.

2.1.5 Het implementatieprogramma Qualification of Information Security (QIS)

Op het voorgaande onderzoek volgde een publiek-privaat programma: Qualification of Information Security. QIS startte in september 2013 met deelname van onder meer Rabobank, ING, ABN AMRO, AkzoNobel, Rijksoverheid, KPN, de Cyber Security Raad, EY, ECP en PvIB.¹⁴ De klankbordgroep omvatte onder meer het CIO Platform, CIP, VNO-NCW, MKB-Nederland, ECABO, HBO-i en vertegenwoordigers van het wetenschappelijk onderwijs. Het programma ontwikkelde een certificatiestelsel dat geschikt zou zijn voor publieke en private organisaties, waarbinnen eisen worden gesteld aan opleidingsinstituten en gecertificeerde professionals in een register worden opgenomen. Als onderligger verschenen de Beroepsprofielen Informatiebeveiliging, in 2014 in versie 1.0 en in januari 2017 in versie 2.0.¹⁵ Deze documenten beschrijven per beroep de taken, de benodigde kennis, vaardigheden en ervaring en de competentieniveaus. Deze zijn expliciet bedoeld als basis voor een uniform kwalificatiestelsel. Aanvullend zijn nog een reeks documenten opgesteld, waaronder Loopbaanperspectieven voor cybersecurity (2015, mede in relatie tot de Cyber Security Raad), Update Kwalificatiestelsel PvIB (2016) en Certificatiestelsel informatiebeveiligers: competenties van de professional (2016).¹⁶ Een operationeel Nederlands certificatiestelsel voor cyberprofessionals is er echter niet gekomen. Uit de openbare bronnen is niet vast te stellen waarom er niet tot implementatie is gekomen of dat QIS de landelijke standaard is geworden.

2.1.6 Voorbeeld van een Nederlandse vorm van persoonscertificering bestaat: IT-auditors.

NOREA, de beroepsorganisatie van IT-auditors, beheert sinds 1992 het register van Register EDP-Auditors. Na een erkende universitaire opleiding en minimaal drie jaar aantoonbare praktijkervaring kan men worden ingeschreven als RE met bijbehorende beschermde deskundigheidsaanduiding; met die inschrijving verbindt men zich aan gedrags- en beroepsregels en is men onderworpen aan tuchtrechtspraak. Volgens NOREA zelf is de organisatie geaccrediteerd door de NBA (Nederlandse Beroepsorganisatie van Accountants), waardoor RE's op vergelijkbare voet opereren als registeraccountants. NOREA stelt daarnaast op haar website dat de meerwaarde

¹⁴ Programma Qualification of Information Security (QIS); zie PvIB, Certificering.

¹⁵ Zie M. Spruit & F. van Noord, Beroepsprofielen Informatiebeveiliging, PvIB/QIS, versie 1.0, 15 mei 2014 en Beroepsprofielen Informatiebeveiliging 2.0, versie 2.0a, 1 januari 2017 (CC BY-ND 4.0). Het betrof: CISO, Information Security Officer (ISO), ICT Security Manager en ICT Security Specialist.

¹⁶ Onder meer: Kwalificatie en certificatie van informatiebeveiligers, Opleidingsmarkt, 24 mei 2011; Loopbaanperspectieven voor cybersecurity, NIOG, 23 april 2015; Update Kwalificatiestelsel PvIB, 19 april 2016; Certificatiestelsel informatiebeveiligers: competenties van de professional, QIS, 14 oktober 2016.

van de RE-titel wordt erkend door toezichthouders zoals De Nederlandsche Bank en de Autoriteit Financiële Markten.¹⁷

2.1.7 Beleidskader voor conformiteitsbeoordeling van de Nederlandse overheid

De Nederlandse overheid beschikt over een formeel afwegingskader over conformiteitsbeoordeling en accreditatie uit september 2016.¹⁸ Van belang is dat dit standpunt persoonscertificering uitdrukkelijk binnen de reikwijdte brengt: het spreekt over het beoordelen of "een product, dienst, *persoon*, ontwerp of een systeem" voldoet aan vooraf gestelde eisen. Het standpunt onderscheidt drie¹⁹ vormen waarop de overheid conformiteitsbeoordeling kan inzetten.

De eerste is bevordering zonder relatie met regelgeving: de sector zet certificering vrijwillig in om zich te onderscheiden, de overheid stimuleert: dit betreft zelfregulering. De tweede is toezichtsondersteuning: het gaat hier om een vorm van co-regulering waarbij een publieke toezichthouder houdt en in zijn toezicht rekening houdt met vrijwillig behaalde certificaten. De derde vorm is opname in regelgeving, waarbij certificering wettelijk verplicht wordt. Deze volgorde is overigens niet vrijblijvend. Het kabinet stelt dat conform staand beleid eerst wordt bekeken of het beleidsdoel bereikbaar is zonder regelgeving. Daarbij speelt de aard van het te beschermen publieke belang een rol: het ligt volgens het kabinet niet voor de hand ernstige veiligheidsrisico's volledig over te laten aan een vrijwillig privaat initiatief. Het standpunt stelt twee voorwaarden: 1. de keuze mag niet uitsluitend zijn ingegeven door de wens te besparen op de kosten van overheidstoezicht en 2. de sector moet voldoende organisatiegraad, structuur en draagkracht hebben om de regeling vorm en inhoud te geven. Verder worden twee grenzen expliciet getrokken: conformiteitsbeoordeling kan het overheidstoezicht niet vervangen en geen enkel systeem geeft volledige garantie op het voorkomen van incidenten.

2.2 Beelden en meningen uit de (groeps-)interviews

In deze paragraaf worden beelden en meningen van enkele voor het onderzoek relevante centrale thema's uit de gesprekken toegelicht. De bevindingen uit deze interviews dienen te worden beschouwd in het licht van het verkennende karakter van het onderzoek. De bevindingen zijn namelijk gebaseerd op een beperkt aantal gesprekken en zijn primair bedoeld om relevante perspectieven, aandachtspunten en mogelijke richtingen voor deze verkenning in kaart te brengen.

2.2.1 Ontwikkelingen in het veld

Snelheid wordt door respondenten genoemd als de meest bepalende ontwikkeling: techniek, dreigingslandschap en in het bijzonder AI veranderen sneller dan opleidingen, normkaders en wetgeving kunnen bijhouden. Respondenten koppelen daaraan de toenemende digitalisering en het structurele tekort aan professionals. Daarnaast wordt erop gewezen dat een puur technische opleiding niet langer volstaat en dat nieuwe opleidingsvormen – onder meer rond AI – nodig zijn; daaraan wordt de vraag verbonden wat op dit moment precies gecertificeerd zou worden als het blijkaar allemaal zo snel gaat.

2.2.2 Probleemperceptie en urgentie

Het beeld van het onderliggende probleem loopt sterk uiteen. Het merendeel van de respondenten stelt de vraag welk probleem met persoonscertificering precies wordt opgelost en bepleit een expliciete kosten-batenafweging. Daarbij geven zij aan slecht of niet in te kunnen schatten hoeveel "personen met nihil kennis, kunde of vaardigheden" binnen de cybersecurity actief zijn en welke schade zij aanrichten. Enkele respondenten herkennen de behoefte in het geheel niet en wijzen op

¹⁷ Zie website NOREA.

¹⁸ Vanuit het Nederlandse kabinetsbeleid is conformiteitsbeoordeling *het proces* waarmee wordt aangetoond dat een product, proces, dienst, systeem, *persoon* of instantie voldoet aan vooraf vastgestelde eisen. Die eisen kunnen bijvoorbeeld voortkomen uit wetgeving, normen of andere formele afspraken; zie *Kabinetsstandpunt over conformiteitsbeoordeling en accreditatie*, brief van de minister van Economische Zaken, Kamerstukken II 2015/16, 29 304, nr. 6, 19 september 2016, met bijlage *Het gebruik van conformiteitsbeoordeling en accreditatie in het overheidsbeleid*.

¹⁹ Zie Kamerstukken II 2015/16, 29 304, nr. 6, onderdeel 'Kabinetsstandpunt over het gebruik van conformiteitsbeoordeling', manieren 1 tot en met 3. In de bijlage 2 is een nadere toelichting opgenomen.

de volwassenheid van de sector en op de aard van de incidenten: bij een recent grootschalig incident bij een Nederlands bedrijf gaat het naar het oordeel van enkele respondenten om gestapelde risico's in een keten, niet om een individuele (cyber)professional die een fout maakt. Tegenover deze relativering staat een breed gedeeld signaal over de vraagzijde: respondenten constateren dat het MKB en opdrachtgevers zonder eigen cybersecuritykennis de kwaliteit van aanbieders vrijwel niet zelfstandig kunnen beoordelen. Vanuit diverse respondenten wordt opgemerkt dat de markt zich eerst bewust moet worden van de meerwaarde van certificering. Ook geven diverse respondenten aan dat het vakgebied enorm (snel) in beweging is, nog niet alle cyberberoepen een bepaalde mate van volwassenheid hebben en dat kwaliteit niet eenduidig c.q. gemakkelijk te onderscheiden is. Vanuit dit laatste perspectief zou volgens diverse respondenten persoonscertificering wel nuttig zijn.

2.2.3 Het object van certificering: rollen, functies en skills

Alle respondenten benadrukken de heterogeniteit van het vakgebied. Er bestaan veel verschillende profielen en binnen de gehele cybersecuritysector slaagt men er niet in eenduidige functieomschrijvingen te hanteren; zo kent de rolinvulling van CISO uiteenlopende verschijningsvormen. Cybersecurity omvat uiteenlopende specialismen, zoals governance, risicomanagement, compliance, technische beveiliging, auditing, pentesten, incident response en security operations, die onderling verschillen in kennisbasis, vaardigheden, risicoprofiel, praktijkgerichtheid en maatschappelijke impact. Een generieke certificering voor "de cyberprofessional" blijft daardoor noodzakelijkerwijs breed en abstract volgens diverse respondenten: het zegt iets over basiskennis, beroepshouding of risicobewustzijn, maar beperkt iets over de vraag of iemand een specifieke taak verantwoord kan uitvoeren. Bij pentesten vallen volgens diverse respondenten de rol, vaardigheidsprofiel en toetsbare praktijk relatief sterk samen; bij CISO of security consultant is dat minder het geval, omdat de inhoud van die functie sterk afhangt van de omvang, volwassenheid, sector en rolinvulling van de eigen organisatie. Over het aangrijpingspunt van certificering lopen de opvattingen uiteen. Vanuit de meeste respondenten wordt certificering van generalisten als lastig beschouwd. Men benoemt het risico dat men "van alles een beetje" toetst en een meerderheid van de deelnemers heeft een uitgesproken voorkeur voor specialistische certificering. Enkele respondenten zien de oplossing in de gelaagdheid binnen abstractieniveaus: certificeren binnen de domeinen strategisch, tactisch en operationeel, waarbij op strategisch niveau algemener wordt getoetst dan bij bijvoorbeeld pentesting. Enkele achten certificering op het niveau van functiegroepen en basisvaardigheden het meest werkbaar, omdat dan niet jaarlijks opnieuw hoeft te worden gemeten en zij zien het ENISA-framework (ECSF), met de twaalf onderscheiden rolprofielen inclusief taken, kennis, vaardigheden en competenties per profiel, als bruikbaar startpunt voor de rolindeling. Men geeft echter ook aan dat het ENISA-framework in de praktijk nog beperkt wordt toegepast en dat het pas de facto norm kan worden bij breed gebruik binnen de EU. Diverse respondenten zijn voor een modulaire, op vaardigheden gebaseerde opzet van certificering, uitdrukkelijk niet vormgegeven als harde poortwachter voor de markt.

2.2.4 Wat een certificaat wel en ook niet aantoont

Over de beperkingen van certificering bestaat brede overeenstemming. Kwaliteiten die zich moeilijk laten toetsen – nieuwsgierigheid, creativiteit, durven doordenken en het vermogen complexe materie begrijpelijk uit te leggen – worden door vrijwel iedereen genoemd. Andere aspecten die werden genoemd zijn affiniteit met cyber, IT-vaardigheden, materie kennis, ervaring, crisisvaardigheden en een onafhankelijke, kritische houding richting de directie, bij voorkeur getoetst in een assessment. Praktijkervaring wordt vrijwel door iedereen als doorslaggevend gezien: basistheorie zonder toepassing heeft volgens hen beperkte waarde. Een keurmerk/certificering vormt hooguit een basis, maar vervangt niet het gesprek van de werkgever met kandidaat of leverancier van cybersecuritydiensten. Bij het beoordelen van buitenlandse partijen stellen enkele deelnemers het beheersen van de Nederlandse taal als randvoorwaarde. Diverse deelnemers wijzen op het risico van een vals gevoel van veiligheid bij persoonscertificering, vergelijkbaar met bijvoorbeeld ISO 27001 bij bedrijfscertificering: persoonscertificering is een aanduiding van een basisniveau en het gaat niet om het certificaat als doel maar om beheersing van de onderliggende principes, die zelf niet veranderen.

2.2.5 Bestaande certificaten, actualiteit en leven lang ontwikkelen

Over de waarde van het bestaande, overwegend private aanbod lopen de meningen uiteen. Deze certificeringen zijn weliswaar sterk ingebed in werving, selectie en opdrachtverlening, maar zijn ook versnipperd en onderling moeilijk vergelijkbaar en worden vastgesteld door private, vaak buitenlandse / Angelsaksische partijen. Daardoor heeft de Nederlandse sector beperkte invloed op de normstelling, toetsingsvormen, kosten en mogelijke hercertificeringseisen. Voor opdrachtgevers blijft volgens vrijwel alle respondenten daarbij vaak onduidelijk welk certificaat relevant is voor welk type opdracht: een generiek certificaat zegt iets anders dan een praktijkgericht specialismecertificaat. Een lange lijst titels is ook geen garantie voor actuele vakbekwaamheid. Trainingen van enkele gevestigde internationale aanbieders worden door vrijwel alle deelnemers genoemd als opleidingen met aanzien en aantoonbare kwaliteit. Tegelijkertijd wordt vanuit enkele respondenten gesteld dat de waarde van een privaat certificaat van buitenaf moeilijk is in te schatten, omdat het onderscheid tussen een deelname- ("alleen vinkje zetten dat men aanwezig is geweest") en een kenniscertificaat (daadwerkelijke toetsing) niet zichtbaar is. Enkele deelnemers constateren dat cybersecurity vrijwel geen equivalent kent van de zwaardere, streng gescreende beroepstitels in bijvoorbeeld het audit- en accountancydomein en wijzen op de kosten en PE-verplichtingen van diverse cybersecuritycertificaten als CISM en CRISC. Het houdbaarheidsvraagstuk van certificaten wordt breed benoemd: een certificaat van enkele jaren oud zegt weinig als de cyberprofessional het vak niet actief bijhoudt en toont competentie aan op het moment van examinering, niet noodzakelijk daarna. Dit levert een risico van schijnzekerheid op. Anders dan bij advocaten of artsen ontbreekt in de cybersecuritysector een vorm van *tucht van de markt* of regulering die bij disfunctioneren tot verlies van een 'license to operate' leidt: een cyberprofessional kan, in tegenstelling tot een arts of advocaat, in principe zonder consequenties als zodanig doorgaan als cyberprofessional. Oplossingsrichtingen die werden aangedragen door deelnemers zijn bijvoorbeeld het certificeren van skills in het kader van leven lang ontwikkelen (LLO), een periodiek assessment en een puntensysteem om ingeschreven te blijven.

2.2.6 Opleiding, instroom en toegankelijkheid

Het opleidingsstelsel komt in vrijwel elk gesprek terug en het aanbod wordt mager genoemd. Het beeld is dat het op mbo-niveau in de kinderschoenen staat, terwijl mbo-opgeleiden voor de markt juist nuttig kunnen zijn. Ook wordt aangegeven dat op hbo-niveau het aanbod ook beperkt is. Door diverse deelnemers wordt geconstateerd dat onderwijsinstellingen verschillende benamingen hanteren voor hun opleidingen en inhoudelijk uiteenlopende aspecten laten aanleren, waardoor certificering niet zonder meer op het diploma kan worden gebaseerd. Relevante suggesties die genoemd zijn door respondenten zijn aandacht voor cybersecurity in het basisonderwijs, aandacht voor stages en opleidingskader en het breed meegeven van basisvaardigheden in het onderwijs met (later) specialisatie daarbovenop. Over de instroom lopen de opvattingen uiteen. Een deel van de deelnemers is van mening dat certificering die drempelverhogend werkt onwenselijk is zolang het tekort aan cyberprofessionals niet is opgelost. De vrees is dat het probleem daarmee groter wordt. Daarnaast wijzen enkele respondenten op het risico dat alleen de 'happy few' het certificaat kan behalen omdat zij dat kunnen betalen. Enkele respondenten vragen aandacht voor mensen zonder diploma maar met veel praktijkkennis en ook wordt ook het omgekeerde effect genoemd: een certificaat kan de toegang tot de markt juist verbreden (het behalen van de license to operate) voor wie niet over langjarige of voldoende specifieke ervaring beschikt.

2.2.7 Vergelijking met andere beroepsgroepen

De vergelijking met gereguleerde beroepen is expliciet voorgelegd en de meningen van respondenten hierover lopen uiteen. Diverse deelnemers achten een stelsel naar het model van het BIG-register denkbaar, mits daarin – net als in de medische wereld – praktijkervaring is verankerd; bij het model van de advocatuur plaatst men de kanttekening dat opdrachtgevers dan kunnen vervallen in de aanname dat inhuren van een ingeschreven professional volstaat. Enkele zien geen toegevoegde waarde in zo'n register: de Nederlandse markt is klein en men kent elkaar, en de verantwoordelijkheid van een arts voor leven en dood is van een andere orde dan die in de cybersecuritysector. Diverse deelnemers herkennen overigens wel de logica van andere assurance-instrumenten, zoals het verplichten van een Verklaring Omtrent het Gedrag (VOG).

2.2.8 Reguleringsvarianten en tempo

Zelfregulering (vorm 1) en co-regulering (vorm 2) uit het eerder genoemde Beleidskader van de Nederlandse overheid (zie paragraaf 2.1.7) hebben de voorkeur van de meerderheid van de respondenten en hun onderbouwing hiervoor komt sterk overeen. Bij zelfregulering wijst men vooral op de snelheid van de markt om te kunnen reageren (adaptiviteit) en dat volwassen organisaties hun eigen, hogere eisen stellen, terwijl minder volwassen organisaties een certificering als minimum kunnen hanteren. Bij vorm 2 stelt de overheid het referentiekader en het gewenste niveau vast, terwijl private partijen de invulling en uitvoering verzorgen vanwege hun kennis en hun vermogen het tempo van het vakgebied bij te houden. Als randvoorwaarden worden genoemd: toezicht op de uitvoerende partijen, transparantie over de eisen, certificering van de partij die het assessment ontwikkelt of afneemt en een certificaat dat niet gratis maar wel vrijwillig is. Een respondent noemt vorm 1 als gelijkwaardig alternatief voor vorm 2 en merkt men op dat er in de praktijk al een vorm van zelfregulering bestaat: een cyberprofessional of diens bedrijf dat niet presteert, verlaat de markt vanwege de tucht van de markt. Bij vorm 1 wordt gewaarschuwd voor de ervaringen met bestaande private certificeringen. Bij vorm 2 worden door diverse deelnemers vraagtekens geplaatst bij de afdwingbaarheid en borging om partijen te laten meedoen (mate van draagvlak). Publiekrechtelijke regulering (fase 3) roept bij de meeste deelnemers terughoudendheid op. Genoemde bezwaren zijn de uitvoerbaarheid door de overheid, het tempo van technologische ontwikkeling die de overheid als regulerende entiteit niet kan bijbenen, het risico van marktafscherming en de vraag hoe internationaal opererende cybersecuritybedrijven aan Nederlandse regelgeving kunnen worden gehouden. Enkele deelnemers bepleiten een gefaseerde invoering in de tijd: certificering kan pas worden ingebouwd als dat waarde toevoegt, bijvoorbeeld over drie of vier jaar na de inwerkingtreding van NIS2/de Cyberbeveiligingswet; dan is er een beeld of deze wetgeving een afdwingmechanisme voor de markt is geworden voor kwaliteitsborging van professionals. Het nader te bepalen omslagpunt zou dan moeten zijn dat, als deze wetgeving onvoldoende effect heeft gehad, sterker op kwaliteit wordt gestuurd met als consequentie dat de kwantiteit op de arbeidsmarkt (tijdelijk) kan afnemen.

2.2.9 Europese inbedding en cyberwetgeving

Deelnemers plaatsen het vraagstuk vrijwel allemaal nadrukkelijk buiten de Nederlandse context: het onderwerp wordt te groot geacht voor Nederland alleen en de verwachting is dat op EU-niveau hoe dan ook iets wordt georganiseerd, waarbij NIS2 kan helpen certificering – mogelijk op termijn verplichtend – op de kaart te zetten (zie ook hierboven). Een internationaal keurmerk heeft vanuit diverse respondenten toch de voorkeur, omdat een aanzienlijk deel van de professionals niet uit Nederland afkomstig is en breed draagvlak nodig is; ook is een groot deel van het opleidingsaanbod internationaal georiënteerd, wat afstemming op EU-niveau vergt en niet alleen op Nederlandse schaal of context. Een terugkerend aandachtspunt in de gesprekken is de samenloop: aansluiten bij de ontwikkeling van wet- en regelgeving om dubbeling en een “administratief circus” te voorkomen.

2.2.10 Internationale vergelijking: Verenigd Koninkrijk en Litouwen

Het Verenigd Koninkrijk en Litouwen verschillen in hun instrumentkeuze: het Verenigd Koninkrijk focust op professionele registratie en titelvoering, terwijl Litouwen vooral investeert in de ontwikkeling van vaardigheden en de versterking van de arbeidsmarktcapaciteit. Voor Nederland volgen hieruit enkele lessen. Aansluiting bij het ECSF lijkt voor de hand te liggen, omdat mapping van bestaande certificeringen de voorkeur heeft boven duplicatie van private of internationale certificaten. Het VK-model laat bovendien zien dat een gelaagde aanpak mogelijk is: een generieke professionele standaard, oplopende niveaus van erkenning, rolspecifieke specialismen, praktijkbewijs, permanente ontwikkeling en een register. Het voorbeeld van Litouwen laat overigens zien dat certificering pas betekenis krijgt als onderdeel van een bredere strategie waarin onder meer (praktisch) onderwijs en training, aandacht voor arbeidsmarktcapaciteit en internationale certificeringsmogelijkheden samenkomen.

2.2.11 Borging in de inkoop- en aannamepraktijk

Deelnemers beschrijven ook de mechanismen die zij nu al gebruiken om kwaliteit te borgen; het meest uitgewerkt gebeurt dat volgens hen vanuit de (semi)overheid. Onderliggend hieraan speelt

informatie-asymmetrie tussen aanbieder en afnemer: voor veel opdrachtgevers is moeilijk vast te stellen of een pentest diepgaand genoeg is uitgevoerd, of een incident response-aanpak adequaat was, of een strategisch advies werkelijk past bij het risicoprofiel van de organisatie. Voor ingewijde organisaties is dit probleem kleiner, omdat zij het veld kennen en certificaten, ervaring en reputatie kunnen wegen. Minder volwassen organisaties, waaronder delen van het MKB, lijken op basis van de interviews vaker te varen op reputatie, bestaande ICT-leveranciers en contractuele afspraken, waardoor kwaliteit deels wordt afgeleid van de eigen organisatie-eisen of bedrijfsvoering en niet van de aantoonbare vakbekwaamheid van de persoon. Persoonscertificering lost daarmee naar het oordeel van deelnemers slechts een deel van dit probleem op en levert een *wicked problem* op; naarmate certificering specialistischer wordt, neemt de inhoudelijke waarde ervan toe, maar wordt de uitkomst voor de gemiddelde opdrachtgever minder goed leesbaar. In aanbestedingen van een (semi)publieke organisatie is kwaliteit vrijwel altijd al onderdeel van de inkoop/aanbestedingseisen, naast bijvoorbeeld leveringsgaranties, referenties bij inschrijvers, organisatiekeurmerken als ISO en SOC. Persoonsgebonden certificering wordt in de praktijk van inkoop uitgevraagd, maar ook bij eigen vacatures: naast het bedrijfsniveau wordt gekeken naar opleiding, referenties en certificering van de individuele professionals, afhankelijk van het type werk, bijvoorbeeld bij pentesting. Respondenten noemen vrijwel allemaal reputatie en het eigen netwerk als dominante afwegingsfactoren, met als gedeelde kanttekening dat dit niet werkt voor opdrachtgevers die de markt van cybersecurity niet of onvoldoende kennen.

2.3 Analyse

In de vorige paragraaf zijn de rode draden uit het onderzoek weergegeven en in deze paragraaf geven we onze analyse over deze hoofdbevindingen weer. Ook voor deze analyse geldt dat deze vanuit het perspectief van een verkenning moeten worden gelezen.

- Private certificeringen zijn inmiddels sterk ingebed in werving, selectie en opdrachtverlening. Tegelijkertijd zijn ze versnipperd, onderling moeilijk vergelijkbaar en worden vastgesteld door private, vaak buitenlandse partijen. Daardoor heeft de Nederlandse sector beperkte invloed op de inhoudelijke normstelling, toetsingsvormen, kosten en (her-)certificeringseisen. Voor opdrachtgevers blijft bovendien vaak onduidelijk welk certificaat relevant is voor welk type opdracht. Een generiek certificaat zegt iets anders dan een praktijkgericht specialismecertificaat; een lange lijst titels is geen garantie voor actuele vakbekwaamheid. Zeker in cybersecurity, waar technieken en dreigingen snel veranderen, blijft aantoonbare praktijkervaring en permanente ontwikkeling noodzakelijk.
- Dit versnipperde certificeringslandschap ontstaat en verandert bovendien in een snel bewegend speelveld: uit de interviews komt naar voren dat techniek, dreigingslandschap en met name AI sneller veranderen dan opleidingen, normkaders en wetgeving kunnen bijhouden en dat de sector daarnaast te maken heeft met een structureel tekort aan professionals. Dat plaatst het certificeringsvraagstuk in een kritisch daglicht: elk stelsel dat wordt ontwikkeld, loopt het risico bij invoering al achter de feiten aan te lopen en een certificeringseis die de instroom verder beperkt, kan het bestaande arbeidsmarkttekort onbedoeld verscherpen. Een certificeringsstelsel is daarom alleen houdbaar als het is ingericht op periodieke actualisatie en niet als eenmalige normstelling.
- Cybersecurity is geen homogeen beroep, maar een verzamelbegrip voor uiteenlopende specialismen. Het omvat onder meer governance, risicomanagement, compliance, technische beveiliging, auditing, pentesten, incident response, security operations. Deze specialismen verschillen in kennisbasis, benodigde vaardigheden, risicoprofiel, mate van praktijkgerichtheid en maatschappelijke impact. Dat maakt een generieke benadering kwetsbaar. Een algemene certificering voor 'de cyberprofessional' zal noodzakelijkerwijs breed en abstract blijven. Daardoor kan zij wel iets zeggen over basiskennis, beroepshouding of risicobewustzijn, maar waarschijnlijk beperkt over de vraag of iemand een specifieke taak verantwoord kan uitvoeren (lees: competenties en vaardigheden heeft). Omgekeerd kan een te zwaar generiek certificaat juist eisen stellen die voor sommige rollen overbodig zijn en voor andere rollen onvoldoende diepgaand. Het ECSF onderkent deze heterogeniteit door twaalf rolprofielen te onderscheiden, met per profiel een uitwerking van taken, kennis, vaardigheden en competenties.

- Deze heterogeniteit komt ook terug in de opvattingen van de respondenten zelf: zij zijn verdeeld over het juiste *aangrijpingspunt* van certificering. Een deel pleit voor specialistische certificering per rol, juist omdat certificering van generalisten het risico heeft 'van alles een beetje' te toetsen. Anderen zoeken de oplossing in certificering op het niveau van abstractere domeinen (strategisch, tactisch, operationeel) of op het niveau van specifieke functiegroepen en basisvaardigheden. Kritisch beschouwd wijst dit gebrek aan consensus over het schaalniveau van certificering op een onderliggend probleem: zolang niet is vastgesteld *op welk niveau* certificering de meeste waarde kan toevoegen, lijkt de keuze voor een stelsel van certificering voorbarig. Het pleidooi voor een modulaire, vaardigheidsgebaseerde opzet – nadrukkelijk niet als harde poortwachter – biedt hiervoor een middenweg/tussenweg, omdat modulariteit toelaat dat verschillende rollen op hun eigen niveau worden getoetst zonder dat er één uniform, generiek certificaat ontstaat.
- Generieke certificaten hebben wel waarde als gemeenschappelijke taal en als indicatie van basiskennis, maar de voorspellende waarde ervan voor concrete vakbekwaamheid is beperkt. Veel bestaande certificaten toetsen vooral brede kennis. Daarmee beantwoorden zij niet automatisch de vraag of iemand in een specifieke context veilig, zorgvuldig en effectief kan handelen. Het onderscheid tussen functietitel en competentie is hierbij cruciaal. Een functietitel beschrijft een positie of verantwoordelijkheid binnen een organisatie; een competentieprofiel beschrijft wat iemand aantoonbaar kan. Bij enkele disciplines, zoals pentesten, vallen rol, vaardigheidsprofiel en toetsbare praktijk relatief sterk samen. Bij andere rollen, zoals CISO of security consultant, is dat minder het geval: de inhoud van de functie hangt daar sterk af van de omvang, volwassenheid van de sector en van de organisatie en de rolinvulling per organisatie. Kwaliteitsborging moet daarom primair aangrijpen op toetsbare competenties en aantoonbare ervaring.
- Dit sluit aan bij wat de meeste respondenten zelf als doorslaggevend voor kwaliteit benoemen: niet de titel, maar eigenschappen als praktijkervaring, creativiteit, kritisch vermogen en het kunnen handelen onder druk (samengevat: skills). Een kritische lezing hiervan is dat dit precies de eigenschappen zijn die zich waarschijnlijk het moeilijkst laten certificeren. De formele kennistoetsen – die zich wél goed laten certificeren volgens respondenten – zeggen daarover echter het minste. Een certificeringsstelsel dat zich beperkt tot toetsbare kennis, sluit niet per se aan bij de praktijk en loopt daardoor mogelijk het risico de verkeerde dingen te meten: het bewijst wat aantoonbaar is, maar niet noodzakelijk wat het meest bepalend is voor kwaliteit. Dat zou ervoor pleiten certificering te positioneren als aanvulling op – en niet als vervanging van – assessments, praktijkbeoordeling en het persoonlijke gesprek tussen opdrachtgever en professional, zoals door meerdere respondenten ook wordt bepleit.
- Toetsbare standaarden ontbreken en het tempo is hoog. De sector beschikt nog niet over breed gedragen, (goed) toetsbare standaarden voor specifieke rollen en verantwoordelijkheden. Titelvoering is versnipperd en de bestaande Europese kaders (ENISA) worden in de praktijk beperkt toegepast. Belangrijk aandachtspunt is dat technologische ontwikkelingen sneller gaan dan certificeringsstelsels kunnen bijhouden, wat het risico van schijnzekerheid introduceert: een certificaat toont competentie aan op het moment van examinering, niet daarna. Hercertificering is dan vereist, maar de vraag is wie dat dan verlangt want er is niet per se de tucht van de markt of regulering zoals bijvoorbeeld bij advocaten en artsen: het verliezen van de license to operate. In de cybersecurity sector kan je in principe gewoon doorgaan als cyberprofessional.
- Deze afwezigheid van een license to operate-mechanisme is ook het scharnierpunt van de vergelijking die respondenten zelf maken met andere gereguleerde beroepen. Een deel van de respondenten ziet een BIG-achtig register voor zich, mits daarin – net als in de medische wereld – praktijkervaring is verankerd; anderen zien juist geen toegevoegde waarde, omdat de Nederlandse markt klein is en men elkaar kent en omdat de aard van het risico in cybersecurity (materiële schade, reputatieschade) van een andere orde is dan bij een arts ('leven en dood'). Kritisch beschouwd is deze vergelijking op zichzelf interessant, maar niet zonder meer overdraagbaar: de kracht van het BIG-register en ook het advocatentableau ligt niet per se in de registratie zelf, maar in het onderliggende tuchtrecht en het reële risico op verlies van de titel en daarmee het verlies van de *license to operate*. Zonder een vergelijkbaar

handhavingsmechanisme – en de interviews laten zien dat dit voor cybersecurity vrijwel ontbreekt – riskeert een Nederlands register voor cyberprofessionals vooral symbolische waarde te krijgen, in plaats van daadwerkelijke kwaliteitsborging van een persoon. Ditzelfde geldt overigens voor lichtere instrumenten zoals een verplichting voor een Verklaring Omtrent Gedrag (VOG) of een puntensysteem: zij zijn behulpzaam als aanvullende waarborg, maar vervangen niet de kern van het probleem, namelijk het ontbreken van consequenties bij disfunctioneren.

- Het kwaliteitsvraagstuk wordt versterkt door informatie-asymmetrie tussen aanbieder en afnemer. Cybersecuritydiensten, -titels en -producten zijn voor veel opdrachtgevers moeilijk te beoordelen. Een gemiddelde opdrachtgever, zo blijkt uit de beelden van respondenten, kan vaak niet goed vaststellen of een incident respons-aanpak adequaat was, of een strategisch advies werkelijk past bij het risicoprofiel van de organisatie. Juist omdat cyberprofessionals vanwege de aard van hun werk toegang krijgen tot gevoelige systemen, data en kwetsbaarheden, is vertrouwen in hun deskundigheid en integriteit essentieel – net als bij artsen en advocaten. Voor ingewijde organisaties is dit probleem veel kleiner: zij kennen het veld, weten welke partijen en professionals gezaghebbend zijn en kunnen certificaten, ervaring en reputatie wegen. Voor minder volwassen organisaties, waaronder delen van het MKB en niet-specialistische opdrachtgevers, is dat veel lastiger. Zij varen vaak op reputatie, bestaande ICT-leveranciers en/of contractuele afspraken. Het gevolg kan zijn dat kwaliteit deels wordt afgeleid van de organisatie waarvoor iemand werkt en niet van aantoonbare persoonlijke vakbekwaamheid. Dit betekent dat persoonscertificering slechts een deel van het probleem oplost. Naarmate certificering specialistischer wordt, neemt de inhoudelijke/ specialistische kennis en waarde toe, maar wordt de uitkomst voor de gemiddelde opdrachtgever minder goed leesbaar.
- De interviews laten zien dat bovenstaande probleem in de praktijk al deels wordt opgevangen, met name door (semi)publieke opdrachtgevers: in aanbestedingen wordt kwaliteit uitgevraagd via referenties, organisatiekeurmerken als ISO en SOC en persoonsgebonden certificering per type opdracht, bijvoorbeeld bij pentesting. Dat is een positief signaal – het toont dat instrumenten voor kwaliteitsborging al bestaan en werken voor partijen die ze weten te benutten – maar het geeft ook een ongelijkheid aan: deze mechanismen werken vooral goed voor opdrachtgevers die de markt al kennen en zelf voldoende inkoopkracht en expertise hebben. Dit lijkt op basis van de interviews aanzienlijk minder goed voor het MKB en andere minder ervaren opdrachtgevers te werken, die juist het meest gebaat zouden kunnen zijn bij een objectief kwaliteitskenmerk. Dat relativeert het idee van persoonscertificering als generieke oplossing: als het probleem vooral aan de onderkant van de markt zit, zou een certificeringsinstrument primair op die doelgroep gericht moeten zijn in plaats van als uniforme eis voor de gehele sector te worden ingevoerd.
- Uit de gesprekken komt een duidelijke voorkeur voor zelfregulering en co-regulering naar voren. Zelfregulering is nu al de facto de norm en op deze wijze kan snel geschakeld worden als de praktijk vraagt om specialisten die kennis van zaken hebben. Bij co-regulering stelt de overheid een referentiekader en gewenst niveau vast, terwijl private partijen – vanwege hun kennis en tempo – bijvoorbeeld de uitvoering verzorgen, onder voorwaarden als toezicht op uitvoerende partijen, transparantie en een vrijwillig maar niet gratis certificaat. Kritisch beschouwd is deze voorkeur goed te verklaren, maar niet zonder risico: co-regulering vraagt om een overheid die zowel voldoende kennis als voldoende doorzettingsmacht heeft om private uitvoerders te blijven normeren en die balans lijkt in een snel veranderend vakgebied niet vanzelfsprekend. Zelfregulering biedt meer wendbaarheid, maar mist een onafhankelijke waarborg en leunt sterk op de 'tucht van de markt', die zoals eerder genoemd in cybersecurity minder hard werkt dan in andere gereguleerde beroepen. Publiekrechtelijke regulering wordt door de meeste respondenten als voorbarig en risicovol gezien, vanwege het gevaar van marktafscherming en de moeilijke handhaafbaarheid richting internationaal opererende bedrijven, soms met private certificering. Een gefaseerde invoering, waarbij pas op een later, aan de effectiviteit van NIS2/Cyberbeveiligingswet gekoppeld moment naar zwaardere regulering wordt bewogen, lijkt daarom een verstandiger uitgangspunt dan vooraf een keuze voor één vaste variant.

- Daarnaast plaatsen de meeste respondenten het vraagstuk nadrukkelijk in een Europese context: het onderwerp wordt als te groot voor Nederland alleen beschouwd en de verwachting is dat ontwikkelingen op EU-niveau – mede via NIS2 – hoe dan ook gaan volgen. Een kritisch punt is dat een zuiver nationale aanpak dubbel werk riskeert als de EU op hetzelfde vraagstuk beweegt: respondenten staan niet achter een ‘dubbeling’ en een ‘administratief circus’. Dit zou ervoor pleiten ervoor dat Nederland zich primair richt op aansluiting bij en actieve inbreng in Europese kaders zoals het ECSF, in plaats van vooruit te lopen met een zelfstandig nationaal²⁰ certificeringsstelsel dat later alsnog moet worden aangepast aan Europese normen.
- Het VK en Litouwen verschillen in hun instrumentkeuze: het VK focust op professionele registratie en titelvoering, terwijl Litouwen vooral investeert in ontwikkeling van vaardigheden en versterking van de arbeidsmarktcapaciteit. Voor Nederland volgen hieruit enkele lessen. Zo ligt aansluiting bij het ECSF voor de hand, omdat mapping van bestaande certificeringen de voorkeur heeft boven duplicatie van private of internationale certificaten. Het VK model laat bovendien zien dat een gelaagde aanpak mogelijk is: een generieke professionele standaard, oplopende niveaus van erkenning, rolspecifieke specialismen, praktijkbewijs, ethiek, permanente ontwikkeling en een register. Het voorbeeld van Litouwen laat volgens ons zien dat certificering pas betekenis krijgt als onderdeel van een bredere strategie waarin onder meer (praktisch) onderwijs en training, aandacht voor arbeidsmarktcapaciteit en internationale certificeringsmogelijkheden samenkomen.
- Dit landenperspectief resoneert met een thema dat in de interviews los van de VK/Litouwen-vergelijking naar voren komt: certificering wordt door respondenten niet gezien als doel op zich, maar krijgt pas betekenis in samenhang met het opleidingsstelsel en praktijkervaring. Uit de gesprekken blijkt dat het opleidingsaanbod in Nederland – met name op mbo-niveau, maar ook op hbo-niveau – als onvoldoende ontwikkeld wordt ervaren en dat onderwijsinstellingen onderling uiteenlopende namen en inhoud hanteren, waardoor certificering niet zomaar op het bezit van een diploma kan worden gebaseerd. Dit is een kritisch aandachtspunt voor de haalbaarheid van zowel het VK-model als het Litouwse model in de Nederlandse context: beide lijken een zekere mate van consistentie en volwassenheid te veronderstellen in het onderliggende opleidingslandschap. Daarnaast wijzen respondenten op het risico dat certificering, zonder aandacht voor toegankelijkheid, een onnodige toetredingsbarrière wordt in een sector die juist kampt met een tekort aan professionals: het risico dat alleen een ‘happy few’ het certificaat kan behalen en de wens om ook mensen zonder formeel diploma maar met aantoonbare praktijkkennis een plek te geven, verdienen mogelijk evenveel aandacht als de institutionele vormgeving van een stelsel zelf.

²⁰ Vanuit Nederland zou overwogen kunnen worden om een initiatief te starten om afspraken te maken, zie enkele voorbeelden op de website van de NEN: Verschillende typen afspraken.

HOOFDSTUK 3

Mogelijke vormen van certificering

In deze paragraaf gaan we in op de mogelijke vormen voor certificering van cyberprofessionals in Nederland in algemene zin.

3.1 Ontwerpprincipes

Uit de analyse volgen ontwerpprincipes voor mogelijk passende vormen van persoonsgebonden kwaliteitsborging van cyberprofessionals in Nederland. Deze principes zijn bedoeld als eerste toetsstenen voor mogelijke vormen van certificering. Belangrijk daarbij is om te voorkomen dat certificering als doel op zichzelf wordt benaderd. De focus dient te liggen op de vraag welke vorm van kwaliteitsborging daadwerkelijk kan bijdragen aan vakbekwaamheid, vertrouwen en transparantie in de cybersecuritysector.

- 1. Specialisatie staat centraal.** Cybersecurity is geen homogeen beroep, maar een verzamelnaam voor uiteenlopende specialismen. De verschillende rollen van cyberprofessionals verschillen sterk in kennisbasis, benodigde vaardigheden, toetsbaarheid, risicoprofiel en mate van praktijkgerichtheid. Een generiek certificaat voor *de cyberprofessional* loopt daardoor het risico te breed en te abstract te worden. Het kan hooguit een gemeenschappelijke professionele basis borgen, zoals ethiek, integriteit, betrouwbaarheid, risicobewustzijn, governance en permanente ontwikkeling. Een dergelijk certificaat kan echter niet aantonen dat iemand specifieke werkzaamheden deskundig kan uitvoeren. Verschillende functies en rollen kennen immers verschillende vaardigheden. Specialisatie moet derhalve het vertrekpunt zijn voor inhoudelijke kwaliteitsborging. Generieke borging heeft waarde als basis en vakbekwaamheid moet per rol of specialisme worden vastgesteld hetgeen aansluit bij het ECSF.
- 2. Competenties gaan boven functietitels.** Kwaliteitsborging moet voornamelijk toetsen wat iemand aantoonbaar kan in plaats van welke functietitel iemand draagt. Functietitels in cybersecurity zijn immers weinig uniform. Dezelfde titel kan in verschillende organisaties iets anders betekenen. Een CISO bij een multinational heeft bijvoorbeeld vaak een strategische en bestuurlijke rol, terwijl een CISO bij een kleinere organisatie ook (meer) operationele taken kan uitvoeren. Ook termen als security consultant, security officer, security specialist of security architect worden in de praktijk verschillend gebruikt. Een functietitel zegt dus vooral iets over iemands positie, zijn of haar verantwoordelijkheid en/of de organisatorische context. Competenties zeggen iets over bijvoorbeeld kennis, vaardigheden, houding en ervaring. Voor kwaliteitsborging is dat tweede element doorslaggevend. De vraag is of iemand aantoonbaar beschikt over de competenties die nodig zijn voor een specifieke taak of verantwoordelijkheid. Certificering moet dan ook niet te snel worden gekoppeld aan functies. Waar functie en competentieprofiel grotendeels samenvallen, zoals bij bepaalde vormen van pentesten of IT-auditing, kan die combinatie wel zinvol zijn. In andere gevallen ligt competentiegerichte certificering meer voor de hand.
- 3. Bewijs uit de praktijk is noodzakelijk.** Een certificeringsstelsel dat uitsluitend of hoofdzakelijk op theoretische kennis steunt, is onvoldoende voor een vakgebied waarin adequaat handelen in concrete situaties centraal staat. Opleiding en examinering tonen aan dat iemand begrippen, methodieken en kaders – op een bepaald moment in de tijd – kent, maar

daarmee is nog niet vastgesteld of iemand die kennis kan toepassen in praktijksituaties. Deze bewijslast is echter essentieel. Dat kan verschillende vormen aannemen: technische praktijkexamens, casuïstiek, portfolio's en/of referentieopdrachten, reviews van vakgenoten of aantoonbare werkervaring. De juiste vorm verschilt per specialisme. Voor bijvoorbeeld pentesten ligt een praktijkgericht assessment voor de hand, conform al bestaande certificaten. Voor incident respons kan casuïstiek of een technische simulatie passend zijn. Voor de meer strategische aspecten kan een portfolio met bestuurlijke adviezen of ervaring met implementatie en transformatie relevanter zijn. Dit geldt ook voor de mate van senioriteit. Naarmate het niveau hoger wordt, neemt het belang toe van aantoonbare ervaring, professionele oordeelsvorming en bestuurlijke- en organisatiesensitiviteit. Een expertstatus vraagt daarom om beoordeling door vakgenoten, relevante praktijkervaring en bewijs van blijvende bijdrage aan het vakgebied. Dit sluit aan bij bestaande beroepspraktijken waarin permanente educatie (PE), ervaring en gedragsnormen onderdeel zijn van de professionele status, zoals bij IT-auditors in het NOREA-register.

4. **Permanente ontwikkeling en herregistratie zijn randvoorwaardelijk.** Het vakgebied van cybersecurity verandert sneller dan veel meer klassieke gereguleerde beroepen als die van een arts of advocaat. Aanvalsmethoden, kwetsbaarheden, tooling, IT-/OT-omgevingen, (AI-) toepassingen, regelgeving en verdedigingsstrategieën ontwikkelen zich voortdurend. Een certificaat is daarom per definitie een momentopname en de waarde neemt, zonder actualisatie van kennis, af naarmate de tijd vordert. Hierdoor ontstaat, zo werd ook in de interviews genoemd, het risico van schijnzekerheid. Iemand beschikt weliswaar over een titel, maar mogelijk niet meer over actuele kennis of vaardigheden. Een passend certificeringstelsel moet daarom eisen stellen aan het onderhoud van vakbekwaamheid in de vorm van bijvoorbeeld permanente educatie, aantoonbare praktijken, deelname aan oefeningen, hercertificering of periodieke beoordeling van een portfolio. Let wel dat daarbij moet worden voorkomen dat permanente educatie verwordt tot het administratief verzamelen van punten zonder inhoudelijke betekenis. Het is een vereiste dat de cyberprofessional aantoonbaar blijft op de voor zijn of haar rol relevante ontwikkelingen. Dit principe is belangrijk omdat het (grotendeels) geen gesloten beroepsgroep is, hetgeen betekent dat iemand kan blijven werken - ook wanneer certificaten verlopen of kennis veroudert.
5. **Aansluiten waar de markt al werkende standaarden kent.** Nederland opereert in een internationale arbeidsmarkt waarin bestaande private certificeringen al sterk zijn ingebed in werving, selectie, opdrachtverlening en professionele ontwikkeling. Het eerdere Nederlandse onderzoek uit 2011 constateerde al dat hun onderlinge betekenis lastig te duiden is. Een Nederlands stelsel moet daarom niet overwegen ernaast iets te beginnen. Waar bestaande certificeringen aantoonbaar competenties toetsen die relevant zijn voor een rol of specialisme, ligt erkenning meer voor de hand. Bovendien vergroot het anders het risico op verwarring en extra kosten. Tegelijk mag aansluiting bij bestaande certificeringen niet betekenen dat hun (door de private instellingen zelf toegekende) waarde zonder meer moet worden overgenomen. Private certificeringen verschillen namelijk sterk qua inhoud, toetsvorm, ervaringsvereisten, hercertificering en praktijkgerichtheid. Een Nederlands model zou daarom transparant moeten maken welke bestaande certificeringen welke competenties dekken, voor welke rollen zij relevant zijn en waar lacunes bestaan.
6. **Begin selectief bij specifieke specialismen.** Het is waarschijnlijk onrealistisch en onwenselijk om in één keer een certificeringstelsel voor het volledige cybersecurityvakgebied te ontwikkelen. Daarvoor is het veld te breed, te dynamisch en te heterogeen. Een te brede start leidt waarschijnlijk tot abstracte normen, beperkte toetsbaarheid en weinig draagvlak. Een passende aanpak begint selectief bij rollen of specialismen waar drie factoren samenkomen: het risico van ondeugdelijke beroepsuitoefening is groot, de kwaliteit is voor opdrachtgevers moeilijk zichtbaar en de benodigde competenties zijn voldoende scherp te formuleren en te toetsen. De precieze selectie van persoonscertificering vraagt nadere uitwerking met de sector, opdrachtgevers en mogelijk de toezichthouders en bestaande certificerende partijen. Voor

enkele specifieke specialismes is al het nodige beschikbaar en start men derhalve niet op nul. Op deze manier starten kent twee voordelen. Ten eerste kan de sector ervaring opdoen met toetsbare rolstandaarden zonder direct het hele vakgebied te reguleren. Ten tweede wordt certificering daar ingezet waar de maatschappelijke meerwaarde het grootst is. Dit past ook bij het kabinetsstandpunt over conformiteitsbeoordeling, waarin een stapsgewijze benadering wordt gehanteerd en de aard van het publieke belang en de organisatiegraad van de sector bepalend zijn voor de mate van overheidsbemoeienis.

7. **Los ook het vraagzijdeprobleem op.** Certificering van personen richt zich met name op de aanbodzijde, de professional. Hij of zij toont aan over bepaalde kennis, vaardigheden of ervaring te beschikken. Het veronderstelde probleem zit echter ook aan de vraagzijde. Veel opdrachtgevers kunnen waarschijnlijk niet goed (genoeg) beoordelen welke expertise zij nodig hebben, welke certificeringen relevant zijn en of een aanbieder daadwerkelijk kwaliteit levert. Dat geldt met name voor organisaties die zelf beperkt volwassen zijn op het gebied van cybersecurity. Naarmate certificering specialistischer wordt, neemt de inhoudelijke waarde ervan toe, maar wordt zij voor niet-ingewijde opdrachtgevers/werkgevers minder goed interpreteerbaar. Een opdrachtgever die bijvoorbeeld niet weet wat het verschil is tussen verschillende meer technische, bestuurlijke en/of auditgerichte certificeringen, wordt niet automatisch geholpen door meer specialistische titels. Een certificeringsstelsel dat het aanbod preciezer ordent, versterkt potentieel het beoordelingsprobleem aan de vraagzijde. Daarom moet persoonscertificering worden verbonden met instrumenten die voor opdrachtgevers begrijpelijk zijn. Er kan gedacht worden aan registers met duidelijke rolomschrijvingen, toelichting op certificeringsniveaus of voorbeeldprofielen voor opdrachten.
8. **Certificering mag instroom en innovatie niet onnodig belemmeren.** De cybersecuritysector kent een structurele behoefte aan nieuwe professionals. Een stelsel moet daarom kwaliteit verhogend werken zonder onnodige barrières op te werpen. Te zware of kostbare certificering kan nadelig uitpakken voor zelfstandigen, kleinere dienstverleners, jonge professionals en zij-instromers. Dit betekent niet dat de meetlat moet worden afgezwakt. Wel betekent het dat meer en andersoortig bewijs nodig is. Ook aantoonbare praktijkervaring, portfolio's en eerder verworven competenties zouden moeten meetellen. Zo ontstaat een stelsel dat ruimte biedt aan verschillende loopbaanpaden, zonder dat de norm vrijblijvend wordt. Een goed stelsel maakt zichtbaar welke competenties iemand al bezit en welke nog ontbreken. Daarmee kan certificering bijdragen aan gerichte scholing, zij-instroom en doorgroei. Certificering wordt dan naast een selectiemechanisme ook een ontwikkelinstrument.
9. **Governance moet onafhankelijk, legitiem en adaptief zijn.** Een certificeringsstelsel staat of valt met de governance. De partij die normen opstelt, examens of beoordelingen laat uitvoeren, registers beheert en hercertificering bewaakt, moet voldoende onafhankelijk, deskundig en gelegitimeerd zijn. In de cybersecuritysector is dat niet gemakkelijk, omdat het veld bestaat uit (internationale) beroepsverenigingen, private opleiders, internationale certificerende instellingen, commerciële dienstverleners, zelfstandigen, opdrachtgevers, toezichthouders en (semi-) publieke organisaties. Een passend model vraagt daarom om brede betrokkenheid, draagvlak en duidelijke rolverdeling. De norm moet niet eenzijdig worden bepaald door één commerciële partij, één beroepsvereniging of één overheidsorganisatie. Tegelijk moet het stelsel niet zo breed worden georganiseerd dat niemand (eind-)verantwoordelijkheid draagt. Het moet gaan om een combinatie van een gezaghebbende entiteit in/voor de sector, die voldoende onafhankelijk is van directe commerciële belangen en tegelijk wendbaar genoeg blijft om normen tijdig te actualiseren. Adaptiviteit is daarbij cruciaal, want een statisch certificeringsschema veroudert snel. Het stelsel moet daarom voorzien in periodieke actualisatie van rolprofielen, competenties, toetsvormen en herregistratie-eisen. Aansluiting bij Europese kaders zoals het ECSF en bij bestaande private certificeringen lijkt voor de hand te liggen, maar de Nederlandse sector moet zelf kunnen beoordelen of dat afdoende zal zijn voor de Nederlandse context.

10. Wettelijke verplichting is sluitstuk, geen startpunt. Gegeven het huidige ontwikkelingsstadium van de sector ligt wettelijke verplichting van persoonscertificering niet voor de hand. Daarvoor is het vakgebied te divers, ontbreken nog breed gedragen toetsbare rolstandaarden en is niet duidelijk voor welke werkzaamheden een certificaat als noodzakelijke voorwaarde zou moeten gelden. Een stapsgewijze route zou dan beter passen. Eerst kan de sector bijvoorbeeld zelf standaarden (door)ontwikkelen en vrijwillige kwaliteitsborging organiseren. Vervolgens kunnen opdrachtgevers, waaronder de overheid, certificering gebruiken in inkoopvoorwaarden. Toezichthouders kunnen certificering eventueel risicogestuurd meewegen, zonder dat het certificaat overheidstoezicht vervangt. Pas als blijkt dat vrijwillige of semi-vrijwillige vormen onvoldoende werken bij scherp afgebakende hoog-risico werkzaamheden (zoals in de vitale sectoren op kritieke processen), kan wettelijke verplichting worden overwogen. Dit sluit aan bij het kabinetsstandpunt over conformiteitsbeoordeling, waarin wordt onderscheiden tussen vrijwillige bevordering, toezichtsondersteuning en wettelijke verplichting. Het standpunt benadrukt bovendien dat conformiteitsbeoordeling overheidstoezicht niet kan vervangen en dat geen enkel certificeringsstelsel volledige zekerheid biedt tegen incidenten.

Deze eerste ontwerpprincipes wijzen op een gelaagd en selectief model: een generieke professionele basis waar dat nuttig is, rolspecifieke competentietoetsing waar dat nodig is, bewijslast voor daadwerkelijke vakbekwaamheid en een begrijpelijke vertaalslag naar opdrachtgevers.

3.2 Van principes naar ontwerp: mogelijke vormen

De hiervoor genoemde uitgangspunten geven richting aan de inhoudelijke beoordeling van mogelijke vormen van persoonsgebonden kwaliteitsborging. De mogelijke vormen zijn in te delen langs verschillende assen en deze geven we hieronder als voorbeelden op hoofdlijnen weer.

Vorm 1: Van basislaag naar expert

Laag 1 — Professionele basisregistratie

Een lichte, breed toegankelijke registratie voor alle cyberprofessionals. Deze borgt niet de technische vakbekwaamheid maar het gemeenschappelijke fundament: bijvoorbeeld ethiek, integriteit, governance en risicobewustzijn, gekoppeld aan een gedragscode, een integriteitsverklaring en/of een verplichting tot permanente ontwikkeling/educatie/levenslang leren. Het is in de kern laagdrempelig (om instroom niet te belemmeren) en levert een herkenbaar basissignaal en de license-to-operate in deze cybersecuritysector. De basislaag is niet bedoeld als maatstaf voor vakbekwaamheid — dat zou namelijk niet passen als 'generiek stelsel'.

Laag 2 — Rolspecifieke certificering

Certificering gericht op concrete kennis en vaardigheden per specialisme, bijvoorbeeld geformuleerd langs de ECSF-rolprofielen en waar mogelijk praktijk getoetst.

Voor rolspecifieke certificering ligt het voor de hand om het ECSF als primaire ordering/kader te gebruiken. Het ECSF biedt Europese gemeenschappelijke taal voor cybersecurityrollen, taken, kennis, vaardigheden en competenties. Voor specialisten waar (private) internationale certificeringen het niveau al toetsen (bijvoorbeeld CREST en OSCP voor pentesten, ISO 27001 Lead Auditor voor audits) verdient erkenning mogelijk de voorkeur boven dupliceren.

Laag 3 — Expertstatus op basis van aantoonbare praktijk

Een erkenning die niet via examinering maar via aantoonbare praktijkervaring en peer review wordt verkregen: een minimum aantal jaren relevante ervaring in het specialisme, beoordeeld door vakgenoten.

Deze derde laag komt enerzijds tegemoet aan de constatering dat vakbekwaamheid niet volledig via toetsing te vangen is en anderzijds aan het probleem dat certificaten verouderen.

Vorm 2: Fasering passend conform het kabinetsstandpunt van de rijksoverheid inzake conformiteitsbeoordeling

1 – Stimuleren van een privaat sectorschema

De sector ontwikkelt zelf de standaarden en de lagen 1 en 2 van vorm 1 hierboven; de overheid stimuleert maar verplicht niets. De trekkersrol ligt niet vanzelfsprekend bij één partij. Gezien de diversiteit van het veld zou dat in de vorm van een consortium kunnen zijn. Aandacht voor scheiding tussen normontwikkeling, beoordeling en opleiding is hierbij het uitgangspunt. Een entiteit als bijvoorbeeld de NEN zou een neutrale rol kunnen vervullen als proces- en normbeheerder, terwijl partijen als bijvoorbeeld PvIB, Cyberveilig Nederland, NLdigital, NOREA, CIO Platform, NCSC/NCC, opleiders, opdrachtgevers en bestaande certificerende instellingen de inhoudelijke en praktische kennis en expertise kunnen inbrengen. Een alternatief zou kunnen zijn aansluiten bij bestaande structuren, zonder een nieuw apart certificeringsinstituut te bouwen.

1 – Toezichts- (co-regulering) en inkoopondersteuning

Zodra persoonscertificering volwassen is (lees: erkend door de markt, afnemers en cybersecurityprofessionals zelf), kan het bijvoorbeeld een rol krijgen in het risicogestuurd toezicht onder de Cyberbeveiligingswet: een onder toezicht staande organisatie die aantoonbaar met gekwalificeerde professionals werkt, kan als lager risico worden ingeschat. Het aangrijpingspunt is hier ook de overheid als inkoper; het kabinetsstandpunt merkt namelijk op dat inkoop en aanbesteding buiten de reikwijdte van het standpunt vallen, maar wel een route zijn waarlangs certificaten kunnen worden gebruikt om aan te tonen dat aan eisen wordt voldaan. Overheidsinkoop zorgt de facto dus voor een afdwingmechanisme, niet wet- of regelgeving. Hier geldt wel de opmerking dat persoonscertificering het overheidstoezicht niet vervangt; het persoonscertificaat is hulpmiddel en geen substituut voor toezicht.

3 – Wettelijke verplichting, selectief

Deze fase is alleen relevant als alleen de eerste twee fasen aantoonbaar tekortschieten en waarschijnlijk alleen voor een kleine categorie - te denken valt aan personen die bijvoorbeeld pentests of security audits uitvoeren bij aangewezen vitale infrastructuur (te vergelijken met de handelingsbevoegdheid/*voorbehouden handeling* van een arts, notaris of advocaat). Het kabinetsstandpunt biedt hiervoor de opening, omdat het stelt dat ernstige veiligheidsrisico's niet volledig aan vrijwillig privaat initiatief moeten worden overgelaten. Echter, de verschillen met de klassieke beroepen maken dat vorm 3 niet de voorkeursvariant is. Zonder een equivalent van een *voorbehouden handeling* is een wettelijke verplichting een heel zwaar middel en complex om toezicht op te houden. Daarbij wordt opgemerkt dat een wettelijke verankering op zichzelf geen garantie geeft: zonder vraag vanuit werkgevers, inkopers, opdrachtgevers en afnemers blijft een certificaat een keurmerk alleen relevant voor de ingewijden in de cybersecurity sector.

Alternatieve vormen die minder passend zijn

Volledigheidshalve zijn in het kader van deze verkenning drie andere alternatieven bekeken/overwogen.

Een generiek nationaal certificaat voor 'de cybersecurityprofessional'. Dit lijkt een voor de hand liggende, maar minst passende vorm. Het botst met de heterogeniteit van de groepen van cyberprofessionals en is ongewenst vanwege het dupliceren van bestaande internationale certificaten.

Een wettelijk stelsel naar het model van arts, advocaat of notaris. Dit lijkt ogenschijnlijk aantrekkelijk, vooral ook omdat het als een echt keurmerk bekend staat en direct daaraan vastgekoppeld het mogen uitvoeren van een *voorbehouden handeling*. Echter, in deze beroepsgroepen wijzigt het speelveld niet zo snel als in de cybersecuritysector en daarom is dit stelsel niet per se houdbaar als vorm van persoonscertificering voor cyberprofessionals.

Volledig vertrouwen op internationale, vooral private certificaten. Dit is feitelijk de huidige situatie en het levert geen Nederlandse zeggenschap op over bijvoorbeeld kwaliteitseisen, integriteitsborging en ervaringscomponenten. Het leidt evenmin tot een transparant register met persoonscertificering en de transparantie voor afnemers/opdrachtgevers neemt ook niet toe.

3.3 Beslisboom persoonscertificering cyberprofessionals

Beslisboom voor vervolgstappen

De keuze voor persoonsgebonden kwaliteitsborging begint bij de vraag welk probleem moet worden opgelost. Als het probleem vooral gaat om algemene professionaliteit, zoals integriteit, betrouwbaarheid, governance en risicobewustzijn, ligt hoogstens een lichte basisregistratie voor de hand. Als het probleem gaat om specialistische vakbekwaamheid, moet eerst worden bepaald voor welke rol of welk specialisme competenties aantoonbaar moeten zijn.

Vervolgens moet worden vastgesteld of de rol of het specialisme voldoende afgebakend en toetsbaar is. Bij brede, contextafhankelijke rollen zoals CISO, security consultant of security officer, ligt zware rolspecifieke certificering minder voor de hand. Bij concretere specialismen, zoals pentesten, incident response of werkzaamheden rond kritieke processen, is certificering waarschijnlijk beter denkbaar.

Daarna volgt de risicovraag. Naarmate de mogelijke schade bij ondeugdelijke beroepsuitoefening groter is en het publieke belang zwaarder weegt, is aanvullende kwaliteitsborging beter verdedigbaar. Bij laag of diffuus risico ligt zware certificering niet per se voor de hand. Bij hoog-risico werkzaamheden kan een zwaardere vorm wel worden overwogen.

Vervolgens moet worden beoordeeld of kwaliteit voor opdrachtgevers voldoende zichtbaar is. Als volwassen opdrachtgevers kwaliteit zelf kunnen beoordelen via reputatie, referenties, inkoopcriteria en eigen expertise, lijkt aanvullende persoonscertificering minder urgent. Als opdrachtgevers kwaliteit moeilijk kunnen duiden, is naast persoonscertificering een vraagzijde-instrument nodig, zoals duidelijke rolomschrijvingen, een register, voorbeeldprofielen voor inkoop of een kwaliteitslabel op organisatieniveau.

Daarna moet worden gekeken of er al bestaande certificeringen, beroepsprofielen of keurmerken zijn. Waar bestaande certificeringen aantoonbaar relevante competenties toetsen, ligt mapping of erkenning voor de hand, maar moet duplicatie worden vermeden. Het ECSF kan dienen als Europees ordeningskader; bestaande Nederlandse profielen, zoals PvIB/QIS, kunnen daarop worden geactualiseerd en gemapt.

Als certificering passend lijkt, moeten drie systeemelementen worden ingericht: een norm, een normbeheerder en een beoordelingsproces. De norm moet rol- en competentiegericht zijn. De normbeheerder moet onafhankelijk, legitiem en adaptief zijn. Het beoordelingsproces moet onafhankelijk zijn van opleiding en kan bestaan uit examen, praktijkassessment, portfolio, peer review, ervaringsverificatie of herregistratie.

Daarna wordt de bewijsroute gekozen. Voor basisprofessionaliteit kan registratie van generieke persoonscertificering volstaan. Voor rolspecifieke vakbekwaamheid zijn praktijkgerichte toetsen of assessments nodig. Voor expertstatus ligt beoordeling op basis van aantoonbare praktijkervaring, portfolio en referenties meer voor de hand dan een examen alleen.

Tot slot wordt de reguleringsvorm gekozen. Startpunt is zelfregulering of een privaat sectorschema. Als het stelsel volwassen is, breed draagvlak heeft en marktherkenning krijgt, kan het via inkoop of toezichtsondersteuning worden benut. Wettelijke verplichting is alleen passend als lichtere varianten aantoonbaar tekortschieten bij scherp afgebakende hoog-risico werkzaamheden.

De beslisboom leidt tot vier mogelijke uitkomsten:

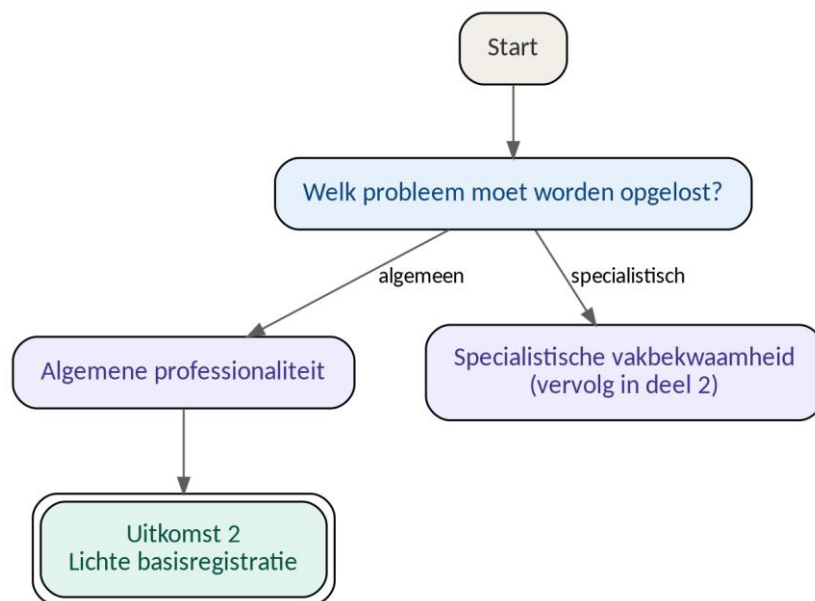
- Geen certificering, maar handreiking of vraagzijde-instrument. Als het probleem vooral zit in transparantie voor opdrachtgevers en de rol onvoldoende afgebakend is.
- Lichte basisregistratie. Als het probleem gaat om algemene professionaliteit, integriteit, vertrouwelijkheid en permanente ontwikkeling.
- Rolspecifieke certificering. Als het gaat om een afgebakend specialisme met toetsbare competenties en voldoende risico.
- Expertstatus of aanvullende bevoegdheid. Als het gaat om senior vakbekwaamheid of hoog-risico werkzaamheden waarbij praktijkervaring, peer review en blijvende ontwikkeling doorslaggevend zijn.

De onderstaande figuren brengen de beslisboom in samenhang in beeld hoe op basis van dit verkennende onderzoek kan worden bepaald of en welke vorm van persoonscertificering mogelijk passend kan zijn voor een specifieke rol of specialisme binnen cybersecurity. De beslisboom bestaat uit vier opeenvolgende onderdelen en loopt van de probleemdefinitie tot de uiteindelijke keuze van reguleringsvorm.

Legenda: Beige = start- of vervolgpunt, blauw = beslispunt of vraag, paars = route of tussenstap, groen = tussenuitkomst, blauw = einduitkomst (keuze reguleringsvorm).

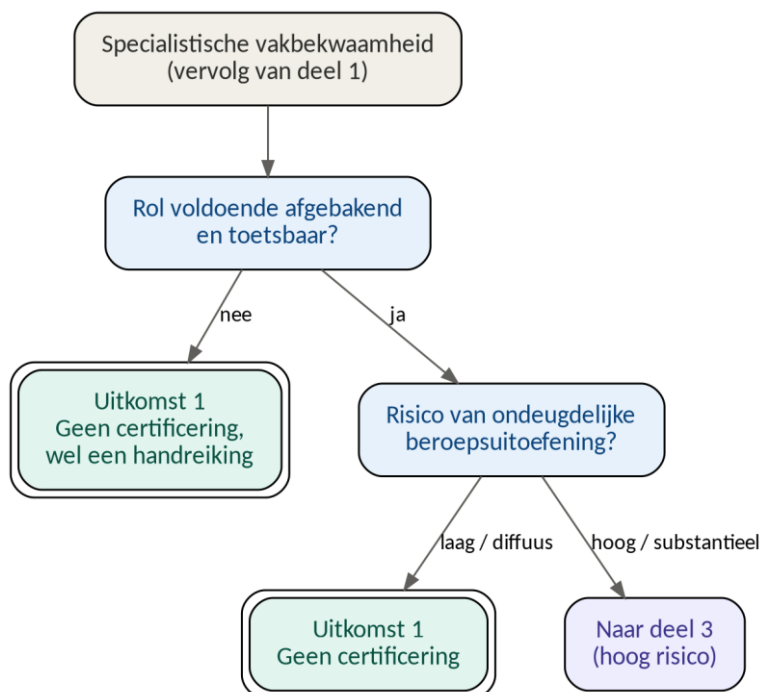
Deel 1 – Probleemdefinitie

De beslisboom start met de vraag welk probleem moet worden opgelost. Bij algemene professionaliteit volgt direct uitkomst 2, een lichte vorm van basisregistratie. Bij specialistische vakbekwaamheid wordt de boom in deel 2 vervolgd.



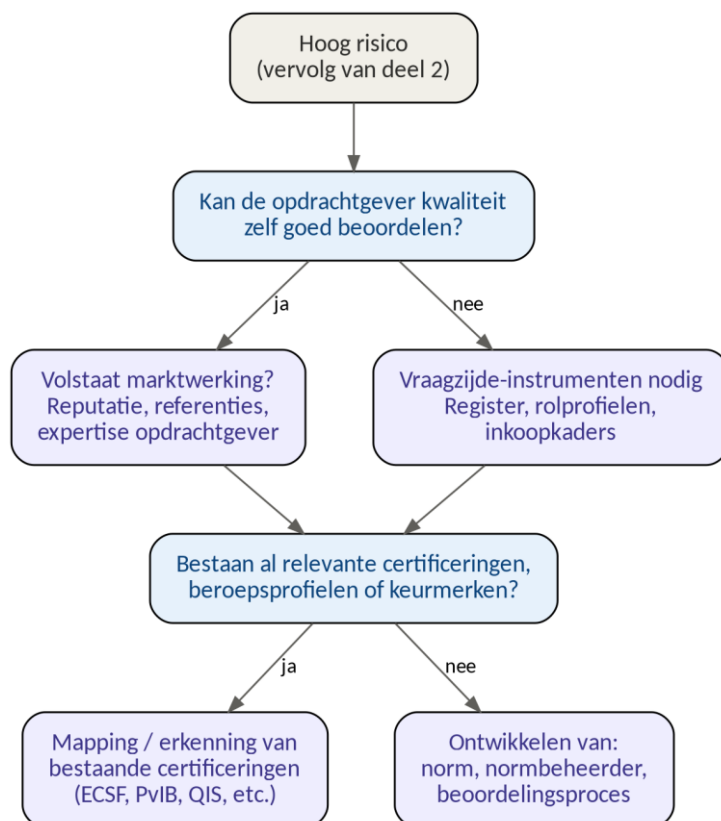
Deel 2 – Afbakening en risico

Voor specialistische vakbekwaamheid wordt eerst getoetst of de rol voldoende afgebakend en toetsbaar is. Is dat niet het geval, dan volgt uitkomst 1: geen certificering, wel een handreiking. Is de rol wel afgebakend, dan wordt het risico van ondeugdelijke beroepsuitoefening beoordeeld. Bij een laag of diffuus risico volgt eveneens uitkomst 1 (zonder handreiking); bij een hoog of substantieel risico gaat de boom verder in deel 3.



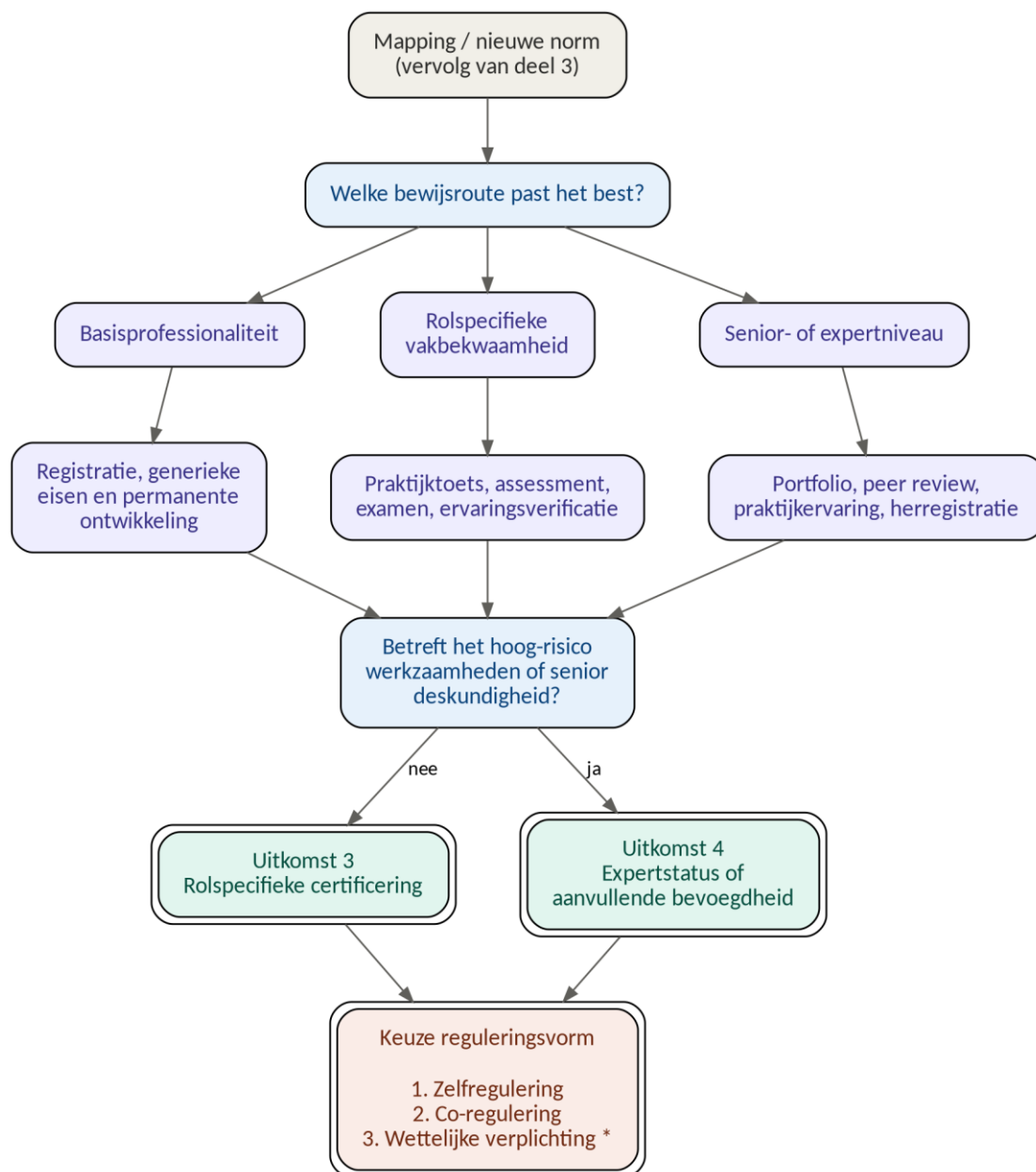
Deel 3 – Vraagzijde en bestaande instrumenten

Bij een hoog risico wordt eerst gezien of de opdrachtgever de kwaliteit zelf goed kan beoordelen. Kan dat, dan wordt gezien of marktwerking via reputatie en referenties volstaat; kan dat niet, dan zijn vraagzijde-instrumenten nodig zoals een register, rolprofielen of inkoopkaders. Beide paden komen samen bij de vraag of er al relevante certificeringen, beroepsprofielen of keurmerken bestaan. Is dat het geval, dan ligt mapping of erkenning van bestaande certificeringen – zoals ECSF – voor de hand; is dat niet het geval, dan moet een nieuwe norm, een normbeheerder en een beoordelingsproces worden ontwikkeld.



Deel 4 – Bewijsroute, uitkomst en reguleringsvorm

Vervolgens wordt bepaald welke bewijsroute het beste past: basisprofessionaliteit (registratie met generieke eisen en permanente ontwikkeling), rolspecifieke vakbekwaamheid (praktijktoets, assessment of ervaringsverificatie), of senior- of expertniveau (portfolio, peer review en herregistratie). Daarna wordt beoordeeld of het gaat om hoog-risico werkzaamheden of senior deskundigheid. Is dat niet het geval, dan volgt uitkomst 3: rolspecifieke certificering. Is dat wel het geval, dan volgt uitkomst 4: expertstatus of een aanvullende bevoegdheid. Beide uitkomsten leiden tot de uiteindelijke keuze van reguleringsvorm.



* Wettelijke verplichting komt alleen in beeld indien lichtere varianten (zelfregulering, co-regulering) aantoonbaar tekortschieten bij scherp afgebakende hoog-risico werkzaamheden.

HOOFDSTUK 4

CONCLUSIES EN AANBEVELINGEN

Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies van de verkenning weergegeven en worden aanbevelingen gedaan voor mogelijke vervolgstappen. Daarbij geldt nadrukkelijk het verkennende karakter van het onderzoek als uitgangspunt. De conclusies zijn gebaseerd op een oriëntatie op enkele openbare bronnen, een beknopte vergelijking met het Verenigd Koninkrijk en Litouwen en een beperkt aantal interviews. Zij zijn daarom niet bedoeld als eindoordeel over de wenselijkheid van persoonscertificering, maar als richtinggevende inzichten die kunnen bijdragen aan de verdere discussie in de sector en aan eventueel vervolgonderzoek. De aanbevelingen zijn vanuit hetzelfde uitgangspunt licht geformuleerd: zij zijn gericht op het expliciteren van aannames, het verkleinen van onzekerheden en het voorbereiden van onderbouwde keuzes. Het doel is derhalve niet het vastleggen van een koers gericht op het komen tot een stelsel.

4.1 Conclusies

De centrale vraag van deze verkenning is welke vorm van persoonscertificering passend zou kunnen zijn voor professionals in de cybersecuritysector in Nederland. De conclusies zijn hieronder geordend langs de twee doelstellingen van het onderzoek: inzicht in de mogelijke vormen van certificering en een beeld van welke vormen passend en haalbaar kunnen zijn.

Aan deze conclusies liggen een aantal aannames ten grondslag die in deze verkenning niet zelfstandig onderzocht of aangetoond zijn. Verondersteld wordt dat de cybersecuritysector relevante kwaliteitsverschillen kent, dat onvoldoende vakbekwame professionals en aanbieders actief zijn en dat ondeugdelijke beroepsuitoefening aanzienlijke schade kan veroorzaken. Daarnaast gaan we ervan uit dat vooral minder cybervolwassen opdrachtgevers moeite hebben om de expertise en de kwaliteit van aanbieders en betrokken professionals te beoordelen. Een aanname is namelijk dat functietitels, opleidingen, certificaten, referenties en reputatie niet altijd voldoende houvast voor hen bieden. Persoonsgebonden kwaliteitsborging kan dit probleem mogelijk verkleinen, maar biedt geen zekerheid en kan ook leiden tot schijnzekerheid, extra kosten en hogere toetredingsdrempels. Deze aannames moeten bij eventuele vervolgstappen nader worden getoetst en waar mogelijk worden gekwantificeerd.

Mogelijke vormen van certificering in algemene zin

1. **Nederland kent geen samenhangend nationaal of sectoraal stelsel voor persoonsgebonden kwaliteitsborging van cyberprofessionals; er zijn wel veel (private) vormen van persoonscertificeringen.** Het Nederlandse certificeringslandschap voor cybersecurity is vooral ingericht op organisaties, producten en diensten. In de praktijk wordt de ruimte op persoonsniveau ingenomen door private, vaak internationale persoonscertificeringen, veelal op Angelsaksische leest geschoeid. Deze zijn sterk verankerd in werving, selectie en opdrachtverlening, maar tegelijk versnipperd, onderling moeilijk vergelijkbaar en vastgesteld buiten de invloedssfeer van de Nederlandse sector. Ze verschillen bovendien in doel, niveau, toetsingsvorm, ervaringsvereisten en onderhoudseisen, waardoor hun betekenis voor Nederlandse opdrachtgevers niet altijd transparant of onderling

vergelijkbaar is. Eerdere Nederlandse initiatieven, het onderzoek uit 2011 en het QIS-programma, zijn tot in de ontwerpfasen gekomen, maar hebben niet geleid tot een volledig operationeel stelsel. Uit openbare bronnen is niet vast te stellen waarom dat zo is; dat is mogelijk een relevante kennislacune en verdient misschien vervolgonderzoek.

2. **Persoonscertificering is geen eenduidig instrument, maar een reeks keuzes.** De verkenning laat zien dat vormen van persoonsgebonden kwaliteitsborging sterk uiteenlopen. Op Europees niveau biedt het ECSF een ordenend kader van rolprofielen, maar geen certificeringsschema. Het Verenigd Koninkrijk kent een uitgewerkt model van professionele registratie met oplopende titels, specialismen, erkende beoordelende partijen en permanente ontwikkeling. Litouwen legt de nadruk op een breder skills-ecosysteem, waarin certificering één element is naast onderwijs en arbeidsmarktbeleid. In Nederland laat het NOREA-register voor IT-auditors in het bijzonder zien dat persoonscertificering in een verwant domein kan functioneren. Mogelijke vormen verschillen daarmee langs een aantal assen: generiek of specialistisch, kennistoets of praktijkbewijs, eenmalig of periodiek, vrijwillig of verplicht.
3. **De werking van een stelsel lijkt minder af te hangen van de registratie zelf dan van de mechanismen eromheen.** Registratie alleen biedt onvoldoende kwaliteitsborging. De vergelijking met gereguleerde beroepen, zoals artsen, advocaten en IT-auditors, suggereert dat de kracht van een register vooral ligt in de combinatie van competentienormen, onafhankelijk beoordeeld praktijkbewijs, periodieke herbeoordeling, professionele gedragsnormen en consequenties bij aantoonbaar disfunctioneren. Dat laatste element ontbreekt in cybersecurity vrijwel: er is geen license to operate die kan worden verloren. Zonder een dergelijk mechanisme bestaat het risico dat een register vooral symbolische waarde krijgt. Uit deze verkenning kan niet worden vastgesteld welk van deze mechanismen doorslaggevend zijn of welk effect zij afzonderlijk hebben.
4. **Het kabinetsbeleid biedt mogelijk een bruikbaar afwegingskader.** Het kabinetsstandpunt over conformiteitsbeoordeling brengt persoonscertificering uitdrukkelijk binnen bereik en onderscheidt drie vormen met oplopende overheidsbemoeienis: bevordering van vrijwillige certificering, toezichtsondersteuning en opname in regelgeving. Het uitgangspunt is dat eerst wordt gezien of het beleidsdoel zonder regelgeving bereikbaar is en dat de sector voldoende organisatiegraad en draagkracht moet hebben om een stelsel van persoonscertificering mogelijk vorm te geven. Daarbij geldt dat certificering overheidstoezicht niet vervangt en geen volledige garantie biedt tegen incidenten.

Passende en haalbare vormen voor de Nederlandse cybersecuritysector

5. **De verkenning biedt onvoldoende basis om vast te stellen dat een algemeen tekort aan individuele vakbekwaamheid het centrale kwaliteitsprobleem van de Nederlandse cybersecuritysector is.** Respondenten verschillen van mening over de urgentie en de omvang van het kwaliteitsvraagstuk en meerdere respondenten vragen om een expliciete kosten-batenafweging. Het meest gedeelde signaal betreft de vraagzijde: opdrachtgevers zonder eigen cybersecuritykennis, waaronder delen van het MKB, kunnen de kwaliteit van professionals en aanbieders moeilijk beoordelen. Persoonscertificering lijkt dit probleem hooguit gedeeltelijk op te lossen. Naarmate certificering specialistischer wordt, neemt de inhoudelijke waarde toe, maar wordt de uitkomst voor niet-ingewijde opdrachtgevers minder goed bruikbaar. Een eventueel stelsel zal daarom waarschijnlijk gepaard moeten gaan met instrumenten die de vraagzijde ondersteunen.
6. **Een generiek vakbekwaamheidscertificaat voor 'de cyberprofessional' lijkt de minst passende vorm.** Cybersecurity is geen homogeen beroep, maar een verzamelbegrip voor uiteenlopende specialismen met verschillende kennisbases, risicoprofielen en mate van

toetsbaarheid. Functietitels zijn bovendien weinig uniform. Rol- en competentiegerichte kwaliteitsborging, met ruimte voor praktijkbewijs, lijkt meer perspectief te bieden. Waar rol, vaardigheidsprofiel en toetsbare praktijk sterk samenvallen, zoals bij pentesten, is certificering beter denkbaar dan bij contextafhankelijke rollen zoals CISO of security consultant.

Tegelijkertijd bestaat onder respondenten geen consensus over het juiste schaalniveau. Een modulaire, op vaardigheden gebaseerde opzet, die uitdrukkelijk niet als harde poortwachter functioneert, wordt als mogelijke tussenweg genoemd.

7. **Houdbaarheid en toegankelijkheid zijn bepalend voor de haalbaarheid.** Technologie, dreigingslandschap en met name AI ontwikkelen zich sneller dan opleidingen, normen en examens kunnen bijhouden. Een certificaat toont competentie aan op het moment van toetsing; zonder periodieke actualisatie en permanente ontwikkeling ontstaat het risico van schijnzekerheid. Hercertificering moet niet uitsluitend berusten op het verzamelen van opleidingspunten. Zij bevatten idealiter een combinatie van actuele beroepsuitoefening, relevante ontwikkeling en periodieke herbeoordeling van competenties. De zwaarte en frequentie moeten risicogestuurd per specialisme worden bepaald. Tegelijk kampt de sector met een (structureel) tekort aan professionals. Een stelsel dat drempels opwerpt voor zij-instromers, zelfstandigen of mensen zonder formeel diploma maar met aantoonbare praktijkkennis, kan dat tekort onbedoeld vergroten. Het nog weinig consistente opleidingslandschap, met name op mbo- en hbo-niveau, maakt het bovendien lastig om certificering op diploma's te baseren.
8. **Voor zover certificering passend is, lijkt een gelaagde, selectieve en stapsgewijze benadering het meest haalbaar.** Uit de analyse en de ontwerpprincipes komt het beeld naar voren van een gelaagde opbouw die kan lopen van een lichte basisregistratie via rolspecifieke certificering naar een expertstatus op basis van aantoonbare praktijk. Een start bij een beperkt aantal specialismen, waar risico, beperkte zichtbaarheid van kwaliteit en toetsbaarheid samenkomen, lijkt realistischer dan een stelsel voor het hele vakgebied. Wat reguleringsvorm betreft, hebben zelfregulering en co-regulering de voorkeur van de meeste respondenten, waarbij overheidsinkoop en risicogestuurd toezicht mogelijke aangrijpingspunten zijn. Een wettelijke verplichting wordt door de meeste respondenten als voorbarig gezien en lijkt hooguit als sluitstuk denkbaar voor scherp afgebakende hoog-risicowerkzaamheden. Het vraagstuk wordt bovendien vrijwel unaniem in een Europese context geplaatst: een nationale aanpak die vooruitloopt op Europese ontwikkelingen, riskeert dubbeling

Samenvattend laat de verkenning zien dat persoonscertificering nog geen vanzelfsprekende oplossing lijkt te zijn voor de kwaliteitsborging in de cybersecuritysector, maar ook niet op voorhand moet worden uitgesloten. De beslisboom in hoofdstuk 3 laat zien dat de uitkomst per rol of specialisme kan verschillen en dat ook de uitkomst 'geen certificering, maar een vraagzijde-instrument' in een aantal gevallen passend kan zijn. Welke vorm uiteindelijk het meest passend en haalbaar is, kan op basis van deze verkenning niet worden vastgesteld en vraagt om nader onderzoek en uitwerking met de sector.

4.2 Aanbevelingen

Onderstaande aanbevelingen zijn bedoeld als mogelijke vervolgstappen voor de opdrachtgevers en de betrokken partijen in de sector. In lijn met het verkennende karakter van het onderzoek zijn de aanbevelingen bewust terughoudend geformuleerd. Zij helpen om onzekerheden te verkleinen, draagvlak te toetsen en bouwstenen te ontwikkelen die ook waardevol zijn als uiteindelijk niet voor (zwaardere) certificering wordt gekozen.

1. **Scherp het probleem en de doelgroep verder aan.** Het verdient aanbeveling om, voorafgaand aan keuzes over een stelsel van persoonscertificering, nader in beeld te brengen

welk kwaliteitsprobleem precies wordt opgelost, bij welke doelgroepen het zich voordoet en hoe groot het is. Denk daarbij aan inzicht in de inkooppraktijk, ervaren knelpunten bij opdrachtgevers en de verhouding tussen verwachte kosten en baten. De signalen over de vraagzijde, met name over het MKB en niet-ingewijde opdrachtgevers, zijn in deze verkenning grotendeels indirect naar voren gekomen. Het ligt daarom voor de hand deze groepen in een eventueel vervolg rechtstreeks te betrekken.

2. **Voer het gesprek in de sector over richting en eigenaarschap.** De ontwerpprincipes en de beslisboom uit deze verkenning kunnen mogelijk dienen als basis voor een gezamenlijk gesprek met onder meer beroepsverenigingen, brancheorganisaties, opleiders, certificerende instellingen, opdrachtgevers en toezichthouders. Doel is te toetsen in hoeverre er draagvlak is voor persoonsgebonden kwaliteitsborging, welke partijen een trekkersrol zouden kunnen vervullen en hoe een scheiding tussen normontwikkeling, beoordeling en opleiding kan worden geborgd. Dit gesprek geeft ook zicht op de (door)ontwikkeling van de organisatiegraad van de sector, die volgens het kabinetsstandpunt een voorwaarde is voor een zelf- of co-regulerende aanpak.
3. **Maak het bestaande certificeringslandschap inzichtelijk voordat iets nieuws wordt ontwikkeld.** Overweeg een verkenning naar het *mappen* van gangbare private certificeringen op de ECSF-rolprofielen. Daarbij kan zichtbaar worden gemaakt welke certificaten welke competenties dekken, welke vorm van toetsing zij hanteren en waar lacunes bestaan. Een dergelijk overzicht heeft waarde ongeacht de latere keuze voor een stelsel en voorkomt dat bestaande certificaten worden gedupliceerd.
4. **Verken instrumenten die de vraagzijde op korte termijn kunnen ondersteunen.** Te denken valt aan een handreiking voor opdrachtgevers met heldere rolomschrijvingen, een toelichting op de betekenis van veelvoorkomende certificaten en voorbeeldprofielen voor inkoop en werving. Aansluiting bij bestaande instrumenten, zoals de keurmerken voor cybersecuritydiensten en de inkooppraktijk van (semi)publieke organisaties, ligt daarbij voor de hand. Dergelijke instrumenten kunnen de transparantie vergroten zonder nieuwe toetredingsdrempels op te werpen.
5. **Onderzoek de haalbaarheid van een beperkte pilot bij een afgebakend specialisme.** Mocht uit de voorgaande stappen voldoende draagvlak blijken, dan kan worden verkend of ervaring kan worden opgedaan met rolspecifieke kwaliteitsborging bij een specialisme waar risico, beperkte zichtbaarheid van kwaliteit en toetsbaarheid samenkomen. Selecteer een specialisme op basis van cumulatieve criteria, zoals aanzienlijke potentiële schade bij ondeugdelijke uitvoering, beperkte zichtbaarheid van kwaliteit voor opdrachtgevers, voldoende afgebakende en toetsbare competenties en (verwachte) onvoldoende werking van lichtere instrumenten, zoals referenties, organisatiekeurmerken, inkoopcriteria of bestaande certificeringen. In een dergelijke pilot kunnen erkenning van bestaande certificaten, praktijkbewijs, herregistratie en de effecten op instroom, kosten en herkenbaarheid bij opdrachtgevers worden getoetst.
6. **Volg en benut Europese ontwikkelingen.** Gezien de breed gedeelde verwachting dat het vraagstuk in Europees verband zal worden opgepakt, verdient het aanbeveling ontwikkelingen rond het ECSF en de uitvoering van NIS2 nauwgezet te volgen en waar mogelijk actief inbreng te leveren. Daarnaast kan worden gevolgd in hoeverre de Cyberbeveiligingswet in de Nederlandse praktijk bijdraagt aan kwaliteitsborging van professionals. Enkele respondenten zien een evaluatie na enkele jaren als een logisch moment om de wenselijkheid van zwaardere vormen van regulering opnieuw te bezien.
7. **Verbind vervolgstappen met onderwijs, arbeidsmarkt en toegankelijkheid.** Het Litouwse voorbeeld en de interviews laten zien dat certificering pas betekenis krijgt in samenhang met opleiding en praktijkervaring. Het ligt waarschijnlijk voor de hand om eventuele vervolgstappen te verbinden met de bredere arbeidsmarkt- en onderwijsagenda

binnen bijvoorbeeld het Digitaal Talent Nederland – Cyber programma. Aandachtspunten zijn onder meer de ontwikkeling van het opleidingsaanbod op mbo- en hbo-niveau, de erkenning van eerder verworven competenties en de toegankelijkheid voor zij-instromers.

Bijlage 1.

Overzicht gesprekspartners

Voor dit onderzoek zijn interviews gehouden met één of meer vertegenwoordigers uit onderstaande organisaties, in alfabetische volgorde:

- Agentschap van de Europese Unie voor cyberbeveiliging (ENISA)
- Deloitte
- CISO van een staatsdeelneming
- Nationaal Cyber Security Centrum (NCSC) en Adviesraad NCSC
- NEN Nederland (Stichting Koninklijk Nederlands Normalisatie Instituut)
- NL Digital
- Politie/Cybercrime PPS
- PricewaterhouseCoopers

Bijlage 2. Kader conformiteitsbeoordeling

Het kabinetsstandpunt (Kamerstuk 29304, nr. 6, 2016, met het onderliggende ICN-rapport "Het gebruik van conformiteitsbeoordeling en accreditatie in het overheidsbeleid") is een toetsingskader, met betrekking tot "een product, dienst, persoon, ontwerp of systeem"; persoonscertificering valt dus uitdrukkelijk binnen de reikwijdte. Hieronder staat in het kort eerst de kern van het kabinetsstandpunt, daarna de toepassing op cyberprofessionals.

Kern van het kabinetsstandpunt

Er zijn drie manieren waarop de overheid conformiteitsbeoordeling (waaronder certificering) kan inzetten. In oplopende mate van overheidsbemoeienis:

1. Bevordering zonder regelgevingsrelatie — de sector zet certificering vrijwillig in om zich te onderscheiden in de markt; de overheid kan dit hooguit stimuleren, niet verplichten. Het gaat hier om zelfregulering.
2. Toezichtsondersteuning — een toezichthouder houdt in zijn toezicht rekening met vrijwillig behaalde certificaten, zonder dat het certificaat zelf verplicht is. Overheid en private partijen hebben beiden een rol in de persoonscertificering (co-regulering).
3. Verplicht in regelgeving — certificering wordt een wettelijke eis om iets te mogen doen.

Volgorde en criteria

Het kabinet kiest expliciet voor een stapsgewijze, terughoudende benadering; eerst kijken of manier 1 of 2 volstaat en pas als dat onvoldoende is, overwegen om te verplichten via regelgeving (manier 3). Bij die afweging spelen twee aspecten een hoofdrol:

- de aard van het publieke belang (bij ernstige veiligheidsrisico's ligt volledige overlaten aan vrijwillig privaat initiatief niet voor de hand);
- of de sector voldoende organisatiegraad, structuur en draagkracht heeft om een certificeringsregeling zelf vorm en inhoud te geven.

Rolverdeling en grenzen

Certificering blijft een privaat instrument met een klantrelatie tussen een conformiteitsbeoordelingsinstantie (CBI) en de beoordeelde partij. Het kabinet is hier expliciet over de grenzen: certificering kan overheidstoezicht nooit vervangen en biedt geen volledige garantie tegen incidenten, een CBI heeft geen publieke handhavingsbevoegdheden en certificering is niet geschikt om louter toezichtskosten te besparen. CBI's die *wettelijke* (verplichte) conformiteitsbeoordeling uitvoeren moeten worden geaccrediteerd door de Raad voor Accreditatie (RvA).



WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al ruim 85 jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen, is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

Berenschot B.V.

Van Deventerlaan 31-51, 3528 AG UTRECHT
Postbus 8039, 3503 RA UTRECHT
030 2 916 916
www.berenschot.nl