NOREA stuurt mee

De nieuwe EU Cybersecurity Act

8 september 2019

Tom Vreeburg

Een jaar geleden kwam ik als bestuurslid van Zeker-OnLine in contact met een werkgroep van cloud stakeholders (CSPCert), ingesteld op initiatief van de Europese Commissie. Zij werkten aan een advies voor de European Union Agency for Cybersecurity (ENISA), die belast is met de taak staat een schema voor cybersecurity-certificering van clouddiensten op te stellen.

Mijn interesse was direct gewekt en het afgelopen jaar heb ik daar namens NOREA samen met hoogleraar Egon Berghout (ESAA) en de registeraccountants Bert Tuinsma en Bianca Smit (beiden van Zeker-OnLine) intensief aan mogen meewerken. Het gezamenlijke resultaat is een advies van 170 pagina's dat de werkgroep op 12 juni 2019 aan de Europese Commissie heeft aangeboden.[1]

Een van de onderwerpen die Europese Unie hoog op haar politieke prioriteitenlijstje heeft staan, is de *Digital Single Market* (DSM). EU-brede initiatieven op dit terrein zullen ervoor zorgen dat er in Europa één markt voor goederen, diensten, personen, kapitaal en data ontstaat die optimaal digitaal wordt ondersteund. Geen versnippering dus, met 28 deelmarkten van afzonderlijke lidstaten met elk hun eigen faciliteiten en regelgeving, maar een centraal vanuit de Europese Unie geregelde markt.

De afgelopen jaren hebben we al wat wet- en regelgeving hiervoor gezien: de *Directive on Security of Networks and Information Systems* (NIS Directive) en de *General Data Protection Regulation* (GDPR, in Nederland: de AVG). Daar is sinds 27 juni de nieuwe *EU Cybersecurity Act* bijgekomen. [2])

Een heel circus

De voorbereiding van Europese wetten is een heel circus waar een enorm aantal mensen en partijen aan meedoen, zie tekstkader 'Beleid en flankerende initiatieven'. Niet vreemd dus, dat het steevast tijdrovende processen met lange doorlooptijden zijn. De concepttekst van een wet wordt opgesteld in een *trialoog*. Dat is een overleggroep van de Europese Commissie, het Europees Parlement en de Europese Raad van Ministers. De trialoog voor de Cybersecurity Act was in december 2018 klaar.
Daarna gingen linguïsten en juristen met het concept aan de slag en vervolgens heeft het Europees Parlement de concept Act op 12 maart 2019 aangenomen. >

Op 17 april hebben het Europees Parlement en de Europese Raad de Act vastgesteld als *Regulation* (EU) 2019/881 en op 7 juni 2019 is hij gepubliceerd. Omdat de Act als regulation (Europese verordening) rechtstreekse werking heeft, hoeft hij niet in de wetgeving van de individuele lidstaten te worden opgenomen en treedt hij voor de hele EU twintig dagen na publicatie automatisch in werking. Dat was dus op 27 juni 2019. De lidstaten hebben vanaf dat moment twee jaar de tijd om randvoorwaarden te creëren, zoals de nationale cybersecurity certificeringsautoriteiten instellen, de accreditatie van *conformity assessment bodies* regelen, et cetera.

Beleid en onderzoek

De activiteiten van de Europese Commissie bestaan uit beleid, waaronder wet- en regelgeving, en onderzoek. CSPCert, de 'stakeholder werkgroep' waar ik in participeerde, valt onder de categorie 'beleid'. Deze werkgroep kende een open inschrijving, met expliciete expertise-criteria waaraan kandidaten moesten voldoen. Ze volgde een transparante werkwijze, gemonitord door de Europese Commissie. Die let daarbij vooral op een evenwichtige samenstelling van de werkgroep en *buy-in* van belangrijke stakeholders. Deze manier van werken leidt in de regel tot uitkomsten die terechtkomen in het beleid van de Europese Commissie.

Onder de categorie onderzoek vallen onderzoeken en innovatieprojecten. De Europese Commissie schrijft hiervoor tenders uit en een groep onafhankelijke experts selecteert uit de binnengekomen voorstellen de voorstellen die het meeste nut opleveren voor bedrijfsleven en samenleving. Deze projecten worden betaald uit budgetten die daarvoor binnen de EU beschikbaar zijn. De Europese Commissie moet de handen vrij kunnen houden en mag daarom geen beleidsmatige conclusies verbinden aan de uitkomsten van deze projecten.

Zo is de EU in 2014 het innovatieprogramma *Horizon 2020* gestart. Dit programma heeft een looptijd van zes jaar en een budget van 80 miljard euro. Vanuit dit programma is onder meer het project *EU Security Certification* (EU-SEC, 3 miljoen euro budget) gefinancierd. Andere gesubsidieerde projecten zijn *Concordia, Echo, Sparta en CyberSec4Europe*, met een totaalbudget van 63,5 miljoen euro. Al deze projecten hebben met Cybersecurity te maken en vier van de vijf projecten houden zich specifiek bezig met certificering van Cybersecurity.

Namens NOREA zat ik in de werkgroep CSPCert, een zware stakeholderwerkgroep waarvoor de Europese Commissie weliswaar het initiatief heeft genomen, maar die geheel door stakeholders gerund en gefund is.3) Daar is dus geen budget vanuit de EU aan te pas gekomen.

Op initiatief van het project *Partnering Trust* van het ministerie van Economische Zaken en Klimaat (EZK) namen NOREA, Zeker-OnLine[4]) en de Erasmus Universiteit deel in de publiek-private stakeholderwerkgroep *CSPCert*. Partnering Trust, met Zeker-OnLine als een van de participanten, is ingesteld door het ministerie van Economische Zaken. Doel van het project is ervoor te zorgen dat voor (online) ICT-diensten uniforme eisen gaan gelden. Gelet op de cruciale rol van die diensten zijn uniforme eisen dringend

nodig voor trust in de sector: uniforme eisen stellen aanbieders in staat de veiligheid en betrouwbaarheid van hun aanbod helder te specificeren en de kwaliteit van hun diensten op uniforme wijze via audits en certificeringen aan te tonen.

Wat houdt de Cybersecurity Act in?

Interessant voor IT-auditors is vooral het framework voor cybersecurity-certificering dat in de Act is opgenomen. Dit framework somt de partijen op die bij de certificering betrokken zijn en schetst de hoofdlijnen van de certificeringsprocessen. De cybersecurity-certificering geldt EU-breed, wat inhoudt dat een certificaat dat in een van de lidstaten is afgegeven, automatisch ook wordt erkend door alle andere lidstaten. De Europese Commissie stelt een *Rolling Workprogramme* op, een beleidsdocument dat voor een periode van meerdere jaren aangeeft welke certificeringsschema's zij ENISA[5]) zal vragen op te stellen.

Met de Cybersecurity Act krijgt ENISA een nieuwe rol en wordt ze de centrale *European Union Agency for Cybersecurity*. Met andere woorden: ENISA wordt de Europese spin in het web voor cybersecurity. De Act beschrijft uitvoerig haar mandaat, de taken, de organisatie, de werkwijze en de wijze van budgettering. ENISA wordt bijvoorbeeld EU-breed verantwoordelijk voor de overkoepelende regie en het toezicht op de uitvoering van het rolling workprogramme. Binnen die kaders stelt elke lidstaat een *National Cybersecurity Certification Authority* (NCCA) in, die binnen de lidstaat regie voert en toezicht houdt. In de European Cybersecurity Certification Group (ECCG) werken de NCCA's en ENISA samen aan de uitvoering van het rolling workprogramme.

ENISA zal op verzoek van de Europese Commissie of de ECCG een schema opstellen voor iedere soort certificering – denk bijvoorbeeld aan de certificering van clouddiensten of Internet-of-Things apparaten. Wat daar allemaal in moet staan, is in detail te vinden in artikel 54 van de Act. Belangrijk element is dat het schema moet beschrijven welke *assurance levels* er onderkend worden – voor ons IT-auditors een verwarrende term, omdat de Act met assurance level niet de mate van zekerheid bedoelt, maar het vereiste beveiligingsniveau voor een product, dienst of proces. De drie assurance levels die de Act benoemt, zijn: *basic*, *substantial* en *high*. De op te stellen schema's zullen beschrijven welke criteria per assurance level gelden. Ook komt erin te staan hoe via een *conformity assessment* is vast te stellen of een product, dienst of proces aan deze criteria voldoet. Vreemd genoeg biedt de Act geen handreiking om te bepalen welk assurance level voor welk product, welke dienst, of welk proces van toepassing is. Wel bevat de Act een paar opvallende bepalingen, zoals:

- Als een schema toestaat dat een assurance level 'basic' kan worden vastgesteld via een *conformity self assessment*, dan leidt dit niet tot een Europees Certificaat maar tot een door de leverancier zelf afgegeven *European Statement of Conformity*.
- De Europese Certificaten worden afgegeven door geaccrediteerde *Conformity Assessment Bodies* of door de NCCA. Het afgeven van certificaten voor assurance level 'high' is voorbehouden aan de NCCA's. Overigens hebben die voor deze taak wel een accreditatie van hun nationale accreditatie-instantie nodig.
- Alle certificaten en EU Statements of Conformity moeten door ENISA en de betreffende NCCA geregistreerd worden.
- De Act benoemt voor de verschillende assurance levels enkele verschillen voor de wijze waarop een conformity assessment moet worden uitgevoerd.

De cybersecurity-certificering is nu niet verplicht, maar dat kan nog veranderen. De Act bepaalt dat de Europese Commissie ENISA en haar mandaat uiterlijk 28 juni 2024 evalueert. De Europese Commissie zal deze evaluatie gebruiken om te bepalen of certificering van bepaalde producten, diensten en processen verplicht moet worden.

Voorbeeld: assurance level 'high'

Artikel 52, lid 7 van de Act geeft de volgende beschrijving van assurance level 'high' en de voor certificering uit te voeren werkzaamheden:

'Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau "hoog", biedt de zekerheid dat de ICT-producten, -diensten en -processen waarvoor dat certificaat is afgegeven voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken'.

'De te ondernemen evaluatiewerkzaamheden behelzen ten minste het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, testen of bij de ICT-producten, -diensten of -processen de beveiligingsfuncties correct, volgens de huidige stand van de techniek, worden toegepast, en het testen van hun weerbaarheid tegen deskundige aanvallers door middel van penetratietests. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen'.

xx

Brug tussen ISO- en ISAE-wereld

Uit het bovenstaande blijkt al dat het Framework qua denkwijze aansluit bij de ISO-wereld. Dat werd extra duidelijk tijdens een overleg met vertegenwoordigers van de Europese Commissie: zij zien het certificaat als een kwaliteitszegel voor cybersecurity van bijvoorbeeld een clouddienst, vergelijkbaar met een ISO-productcertificaat voor de kwaliteit van drinkglazen en ruiten. Daarbij laten ze buiten beschouwing dat ook

processen waarover extern verantwoording moet worden afgelegd, gebruikmaken van clouddiensten. Belangrijk daarbij is het een gegeven dat een clouddienst nooit op zichzelf staat, maar altijd bestaat uit een samenhangende verzameling van allerlei clouddiensten, geleverd door verschillende partijen. Een SaaS-dienst maakt bijvoorbeeld altijd gebruik van een hostingpartij en soms zelfs van meerdere hostingpartijen. Vaak neemt de klant ook *managed services* af voor *security management*, *patch management*, et cetera. Hoe dit geregeld is, verschilt per dienst en per leverancier. Veelal worden diensten afgenomen volgens het cafetariamodel. Dat maakt de legpuzzel van diensten extra complex. Maar om een certificaat bij een SaaS-dienst te kunnen afgeven, ontkom je er niet aan de hele puzzel van diensten die aan de SaaS-dienst ten grondslag ligt, te leggen en vast te stellen dat elk van de sub-service-puzzelstukjes aan de criteria voor certificering voldoet. De ketting is immers zo sterk als de zwakste schakel. Bij ISO gebeurt dat nauwelijks. ISO kijkt naar het managementsysteem van de SaaS-leverancier en gaat niet verder dan vaststellen dat deze leverancier bij het afsluiten van een contract voor een sub-service nagaat of zijn sub-leverancier een ISO-certificaat voor die sub-service heeft. Dat is een werkwijze van grote stappen snel thuis, en zoals ik er tegenaan kijk is op die manier geen verantwoorde uitspraak mogelijk over de veiligheid van een SaaS-dienst.

De ISAE-wereld springt daar heel anders mee om. Na eerst alle sub-services in beeld te hebben gebracht, plaatst de auditor die een ISAE-opdracht uitvoert ze doorgaans in het assurancerapport via een carve-out buiten de scope. Daarmee maakt de auditor expliciet welke sub-services niet beoordeeld zijn. Het is dan in elk geval duidelijk dat het de gebruiker van het assurancerapport is die vervolgens voor de schone taak staat om op basis van alle beschikbare assurancerapporten over sub-services vast te stellen dat de gehele keten aan alle veiligheidseisen voldoet. Iedere IT-auditor of accountant die bij zijn controle te maken krijgt met serviceorganisaties kent dit spel en weet hoe complex het kan zijn. Dit is ook precies wat wij bij Zeker-OnLine doen voordat we een keurmerk afgeven.

Wil het Europees Certificaat werkelijk het vertrouwen in de veiligheid van bijvoorbeeld een bepaalde clouddienst kunnen vergroten, dan is dus meer nodig dan de ISO-benadering. Er moet minstens een plek worden ingeruimd voor een conformity assessmentmethode, gebaseerd op de ISAE. Dat was dan ook onze insteek in de CSPCert-werkgroep. Daarbij liepen we tegen het probleem op dat de Europese Commissie en de meeste leden van de CSPCert-groep niet wisten wat de auditwereld onder assurance verstaat – overigens hadden ze ook nog nooit van NOREA gehoord. Daar moest dus nog heel wat evangelisatiewerk gebeuren. Gelukkige bijkomstigheid was dat vertegenwoordigers van twee buitenlandse nationale certificeringsprogramma's al in CSPCert zaten[6]). Het ene programma is gebaseerd op ISO, het andere op ISAE. Hierdoor werd het een stuk simpeler om een brug tussen beide werelden te slaan. Dat heeft ons geholpen om in het advies aan ENISA een op ISAE gebaseerde attestrapportage als een van de mogelijke conformity assessmentmethoden opgenomen te krijgen.

Assurance op basis van ISAE geeft meer zekerheid dan ISO omdat je ook de werking vaststelt. De extra kosten hiervan kunnen beperkt blijven, omdat er al veel (hosting) partijen zijn die een assurancerapport hebben dat hergebruikt zou kunnen worden.

Hoe ziet ons advies aan ENISA eruit?

Ons advies aan ENISA is in feite een nadere invulling van de in de Act opgenomen beschrijving van de componenten van het schema. De twee kernelementen zijn de certificeringscriteria en de toegestane conformity assessmentmethoden.

Om de toepasselijke criteria te bepalen, heeft de werkgroep de zes meest gebruikte normenkaders in Europa geanalyseerd. Het resultaat was een normenkader dat de grote gemene deler is van deze zes.

Onderliggende normenkaders

Om de certiferingscriteria in haar advies aan ENISA te bepalen heeft de werkgroep de volgende Europese normenkaders geanalyseerd:

Cloud Computing Schemes Meta-Framework (CCM), van ENISA

- ISO/IEC 27002
- ISO/IEC 27017
- ISO/IEC 27018

ANSSI SecNumCloud, uit Frankrijk

BSI C5, uit Duitsland

Wat de conformity assessment methoden betreft, heeft de werkgroep de volgende drie varianten in haar advies opgenomen:

- evidence based;
- ISO-based;
- ISAE-based;

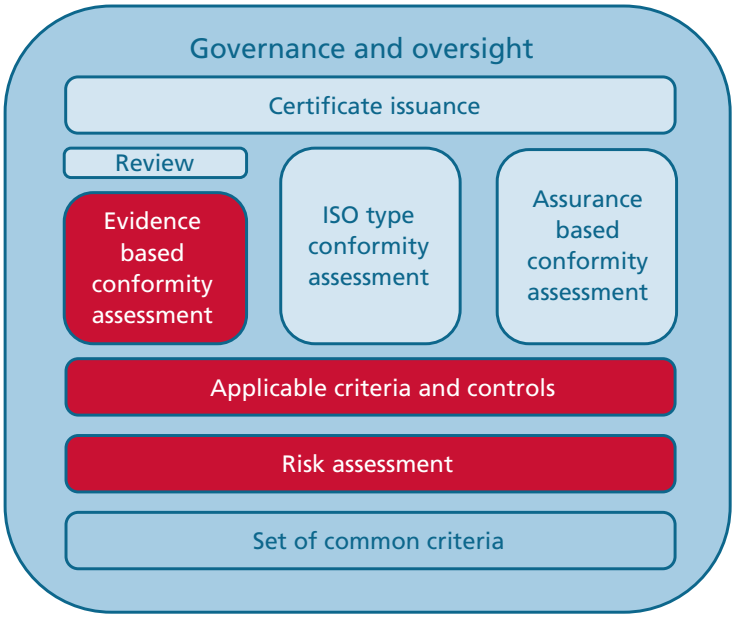
De *evidence-based conformity assessment* is een door de leverancier zelf uitgevoerde en gedocumenteerde self-assessment die vervolgens door een geaccrediteerde conformity assessment body wordt gereviewd. Volgens de werkgroep zou een pure self-assessment, zonder externe review, niet voldoende zijn gezien het object en de doelstelling van het certificaat voor cybersecurity. Vandaar dat we een variant ontwikkeld hebben waarin de self-assessment wordt aangevuld met een externe (dossier-)review. Dat betekent dat niet de qua trust zwakkere Statement of Conformity door de leverancier zelf wordt afgegeven, maar het meer trust creërende Europees Cybersecurity Certificaat door de conformity assessment body. Dit model schijnt in Duitsland al te werken, maar ik vraag me af of

conformity assessment bodies in het algemeen bereid zijn om deze verantwoordelijkheid op basis van een dossier review te dragen.

De *ISO-based conformity assessment* is een op basis van ISO-standaarden[7]) uitgevoerde conformity assessment. Let wel: in tegenstelling tot wat veel mensen denken, is deze assessment weliswaar gebaseerd op ISO-standaarden, maar leidt die niet tot een ISO-certificaat omdat het onderliggende normenkader geen ISO-standaard, is. In plaats daarvan leidt het tot het meer zekerheid gevende Europees Cybersecurity Certificaat.

De *ISAE-based conformity assessment* is een audit volgens ISAE 3000A of 3402 (of gelijkwaardige standaard), uitmondend in een attestrapport. Om van dat attestrapport tot een certificaat te komen, is aanvullend nog een certificeringsproces met twee stappen nodig: een evaluatie en een certificeringsbeslissing. Omdat de ISAE daar niet in voorziet, is het aan een van de geaccrediteerde body's om dat certificeringsproces uit te voeren.

Figuur 1 geeft in een notendop weer welke inrichting van de certificering wij in ons advies voorstellen.



Figuur 1: Voorstel werkgroep voor inrichting certificering

De rode blokken zijn de verantwoordelijkheid van de leverancier van een dienst. De lichtblauwer blokken zijn de verantwoordelijkheid van de conformity assessment body, met de belangrijke uitzondering dat het afgeven van een certificaat voor assurance level 'high' voorbehouden is aan de NCCA. De donkerblauwe blokken zijn verantwoordelijkheden van ENISA, de NCCA's en de Raden van Accreditatie.

In het advies hebben we ook opgenomen dat tijdens een conformity assessment voor de assurance levels 'substantial' en 'high' de *operational effectiveness* (werking) van de maatregelen moet worden vastgesteld.

Hoe nu verder?

ENISA en de Europese Commissie hebben ons advies enthousiast ontvangen – ENISA typeert het als een gedegen stuk werk dat 'al bijna een schema is'. ENISA gaat een schema opstellen voor de cybersecurity in de cloud zodra de Europese Commissie hierom vraagt. Maar op dit moment is ENISA daar nog niet aan toe, omdat de organisatie de handen vol heeft aan de ingewikkelde klus de Act procedureel in te richten. Het verzoek van de Europese Commissie is begin volgend jaar te verwachten en ENISA heeft al aangegeven zeker een jaar nodig te hebben om het schema op te stellen.

In de tussentijd is het zaak dat NOREA nadrukkelijk de vinger aan de pols blijft houden, omdat ENISA een aantal beslissingen moet nemen die gevolgen kunnen hebben voor RE's. Bijvoorbeeld hoe de accreditatie wordt ingericht. Artikel 60 van de Act bepaalt dat conformity assessment bodies worden geaccrediteerd conform Regulation (EC) No 765/2008. Dat zou betekenen dat RE's en de organisaties waar zij voor werken een accreditatie van de (Nederlandse) Raad voor Accreditatie nodig hebben. Dat is iets wat wij nu niet kennen en wat bureaucratische rompslomp en extra kosten meebrengt. Wellicht is dit te voorkomen door de body die het certificaat afgeeft te laten accrediteren. Dat zou als voordeel hebben dat de ISAE-rapporten die nu al door serviceorganisaties worden opgesteld, met wat (kleine) aanpassingen kunnen blijven bestaan als basis voor een Europees Certificaat.

Tot slot

Door het bestaan van NOREA heeft Nederland binnen Europa een unieke positie. Er is geen enkel land dat het beroep zo goed georganiseerd heeft als Nederland. Het was voor de Europese Commissie een absolute eyeopener dat een klein land als Nederland een beroepsgroep heeft van 1.800 IT-auditprofessionals die allemaal een post masteropleiding hebben afgerond van minimaal 60 ECTS[8]). En die als beroepsgroep ook nog eens erkend zijn door de nationale beroepsorganisatie van Register Accountants en daardoor op gelijkwaardige voet mogen meewerken aan financial audits. Dat punt hebben we bijzonder duidelijk gemaakt en gaan we als NOREA ook gebruiken bij het volgen van ENISA wanneer ze hun schema voor cybersecurity certificering van cloud diensten gaan ontwikkelen.

Noten

[1] Tekst van het CSPCert-advies: https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view (geraadpleegd op 9 augustus 2019).

[2] Tekst van de Act: https://eur-lex.europa.eu/eli/reg/2019/881/oj (geraadpleegd op 9 augustus 2019).

[3] CSPCert is een zware werkgroep met 32 drafting members, 25 observer members en 4 vertegenwoordigers van de EC. Zie: https://cspcerteurope.blogspot.com/p/about-us.html (geraadpleegd op 9 augustus 2019).

[4] Zeker-OnLine is een stichting zonder winstoogmerk die als doel heeft de betrouwbaarheid van onlinediensten (clouddiensten) vast te stellen: https://www.zeker-online.nl.

[5] ENISA: European Union Agency for Cybersecurity: https://www.enisa.europa.eu/about-enisa (geraadpleegd op 9 augustus 2019). De organisatie werd in 2004 opgericht als adviesorganisatie onder de naam 'European Network and Information Security Agency'. Met de invoering van de EU Cybersecurity Act heeft ENISA een meer leidende rol gekregen.

[6] SecNumCloud van het Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) uit Frankrijk en de Cloud Computing Compliance Controls Catalogue (C5) van het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI). SecNumCloud is geheel gebaseerd op ISO-regelgeving, terwijl C5 gebaseerd is op attestrapportages volgens ISAE 3000/3402.

[7] ISO/IEC 17000:2004, ISO/IEC 17021:2015, ISO/IEC 17065:2012 en ISO 19011:2018.

[8] ECTS is de Europese gestandaardiseerde methode om de zwaarte van een opleiding uit te drukken. 60 ECTS-punten staat voor een jaar opleiding in het hoger onderwijs.

T.B. (Tom) Vreeburg RE | Bestuurslid van de Stichting Zeker-OnLine

Tom Vreeburg was tot 1 juli 2017 werkzaam als partner IT Audit bij EY. Daar was hij onder meer verantwoordelijk voor het afgeven van assurancerapportages bij serviceorganisaties (ISAE3402, SOC2). Tom is daarnaast voorzitter geweest van de Commissie voor de Organisatie van de Informatie Voorziening van het NBA en is een van de oprichters van XBRL Nederland. Hij was van 2009 tot 2016 bestuurslid van NOREA en is nu nog voorzitter van de Visitatiecommissie Opleidingen en lid van de Raad van Beroep.

Namens NOREA is hij lid van de CSPCert stakeholder werkgroep van de Europese Commissie.