IT-assurance versus IT-certificering

Wat biedt mij (voldoende) zekerheid?

Drs. ing. Ronald Koorn RE CISA en Suzanne Stoof MSc RA

Er is veel begripsverwarring over de inhoud, toepassing en geboden zekerheid door IT-assurance en -certificering. Het gebruik van termen als 'certificerings-audit', 'ISO-auditing', 'privacycertificering' en 'certificering van de jaarrekening' vergroot de onduidelijkheid. Dit artikel geeft uitleg over beide typen onderzoeken en beschrijft welke overwegingen genomen kunnen worden om antwoord te krijgen op de vragen van:

- **afnemers van (uitbestede) IT-diensten: 'Kan ik het beste om een ISO-certificaat of een IT-assurancerapport vragen?'**
- **serviceproviders: 'Zal ik zowel een ISO-certificaat als een IT-assurancerapport of één van beide aan mijn klanten aanbieden?'**
- **auditors: 'Hoe ga ik in mijn audit om met een beschikbaar ISO-certificaat?'**

Drs. ing. R.F. Koorn RE
is partner bij KPMG Advisory.
koorn.ronald@kpmg.nl

Mw. S. Stoof MSc RA
is assistent manager bij KPMG Accountants en adviseur bij KPMG Advisory.
stoof.suzanne@kpmg.nl

Inleiding

In toenemende mate komen zowel IT-gerelateerde[1] ISO-certificaten als IT-assurancerapporten in dezelfde omgeving voor. Denk hierbij bijvoorbeeld aan ISO 27001-certificaten voor informatiebeveiliging en de COS/Richtlijn 3000/3402 assurancerapporten voor algemene IT-beheersingsmaatregelen. Ook al kennen ze gelijkenissen, het is belangrijk dat afnemers en aanbieders de verschillen en toepassingsgebieden goed kunnen onderscheiden. Een verdieping daarbij is welke vorm van assurance en/of certificering gewenst is in welke situatie. Verderop in dit artikel wordt een aantal veelvoorkomende vormen en varianten van beide besproken.

De discussie over welke type zekerheid gewenst is voor de afnemer van ICT-diensten is vervroegd. Waar voorheen de keuze hiervoor pas na de uitbesteding of invoering van nieuwe systemen werd gemaakt, is dit nu veelal onderdeel van de RFP-procedure. Dat wordt mede ingegeven door wet- of regelgeving die voorschrijft dat er zekerheid moet worden verkregen over uitbestede activiteiten. Het management van de uitbestedende partij blijft immers verantwoordelijk voor de uitbestede processen.

Randvoorwaarde bij het juiste begrip bij afnemers en aanbieders van IT-diensten is dat IT-auditors niet alleen het onderscheid tussen assurance en certificering doorgronden, maar tevens hoe ze in één onderzoek tezamen moeten worden behandeld. Hierbij wordt ingegaan op het al dan niet kunnen steunen op een ISO-certificaat in een assurancerapport en vice versa.

1 De inhoud van dit artikel is ook toepasbaar op niet IT-gebieden, zoals inzake kwaliteit, duurzaamheid, e.d.; gezien de samenstelling van de lezersgroep zijn deze buiten beschouwing gebleven. Dit geldt evenzo voor het niet in dit artikel behandelen van product- en persoonscertificering.

Assurance

Om de overeenkomsten en verschillen tussen assurance en certificering te begrijpen, wordt hieronder beschreven wat de term 'assurance' omvat.

Aard

In het Raamwerk Assuranceopdrachten door IT-auditors is opgenomen dat een assuranceopdracht onder meer de volgende elementen dient te bevatten:

- *Doel assuranceopdracht.* Afgezien van de vaktechnische doelstelling is het doel om derde partijen die vertrouwen op een dienst of product de zekerheid te bieden dat die voldoet aan een overeengekomen normenkader. Volgens de beroepsvoorschriften mogen er twee soorten van assuranceopdrachten worden uitgevoerd: tot het verkrijgen van een beperkte of een redelijke mate van zekerheid. Bij een redelijke mate van zekerheid wordt een positief geformuleerd oordeel – inzake het voldoen aan een normenkader – gerapporteerd aan de verspreidingsgroep, bij een beperkte mate is sprake van een negatief geformuleerde conclusie: 'Op grond van onze in dit rapport beschreven werkzaamheden is ons niets gebleken op basis waarvan wij zouden moeten concluderen dat de interne beheersingsmaatregelen volgens de criteria XYZ niet in alle van materieel belang zijnde opzichten effectief zijn'. Absolute zekerheid is vrijwel nooit mogelijk, tenzij de waarnemingen van de IT-auditor een integraal karakter hebben (zoals bij volledige data-analyse).
- *Partijen.* Bij een assuranceopdracht zijn drie partijen betrokken: (IT-)auditor, verantwoordelijke partij en beoogde gebruiker(s). Er kan ook sprake zijn van IT-assurance indien zowel degene die zekerheid ontleent aan een assurancerapport als de auditee en (interne) IT-auditor zich in één organisatie bevinden.
- *Object van onderzoek.* Dit houdt het door de opdrachtgever gedefinieerde onderwerp in dat door de auditor wordt geëvalueerd of getoetst. Dit kan een (governance)structuur, strategie, (informatie)systeem, proces, product of ander logisch samenstel van componenten zijn.
- *Toetsingsnormen.* Dit zijn de eisen of criteria die worden gebruikt voor het evalueren of toetsen van het object van onderzoek waaronder, voor zover van belang, die voor presentatie en toelichting. Als er geen standaardnormenkader beschikbaar is kan er, op basis van algemeen aan normenkaders te stellen eisen, een specifieke set van toetsingsnormen worden gespecificeerd. Deze algemene eisen betreffen ([NORE02]):
  - *objectiviteit*: de mate waarin normen(stelsels) vrij zijn van persoonlijke beïnvloeding;
  - *eenduidigheid*: de mate van precisering en eenduidigheid van formulering;
  - *relevantie*: de mate waarin normen(stelsels) bruikbaar zijn voor bepaalde auditopdrachten;
  - *herleidbaarheid*: de mate waarin kan worden vastgesteld waaraan normen(stelsels) zijn ontleend;
  - *zorgvuldigheid*: de mate waarin het normenstelsel beantwoordt, al dan niet juridisch verankerd, aan de maatschappelijke opvattingen over behoorlijk IT-gebruik.
- *Assurancerapport.* Dit resultaat van het onderzoek betreft een schriftelijk rapport van de auditor met een oordeel of conclusie omtrent het object van onderzoek. Er kan sprake zijn van een goedkeurend oordeel, een oordeel met beperking of een afkeurend oordeel. Oordeelsonthouding is niet mogelijk, dan zal het leiden tot een afkeurend oordeel of het teruggeven van de opdracht.

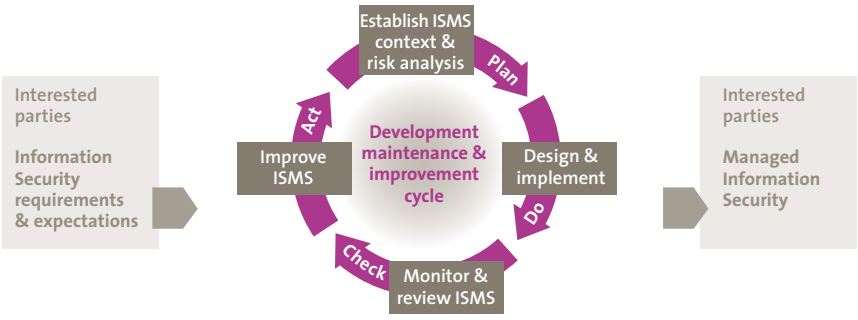
Typen

Hoewel voor de term 'assurance' duidelijk is beschreven welke elementen assurance dient te bevatten, zijn er op de markt diverse vormen op basis waarvan assurance verstrekt kan worden. Tussen deze vormen van assurance bestaan ook weer overeenkomsten en verschillen. Een bekende en overkoepelende vorm van assurance is de ISAE 3000. ISAE 3000 is in Nederland geïmplementeerd onder de naam Standaard 3000 (NBA) en Richtlijn 3000 (NOREA).

Er kan onderscheid worden gemaakt tussen SOC 1-, SOC 2- en SOC 3-rapporten. Voor het onderscheid tussen de diverse vormen van IT-assurance verwijzen wij naar het artikel eerder in deze Compact 'Nieuwe ontwikkelingen IT-gerelateerde Service Organisation Control-rapportages, SOC 2 en SOC 3' van Han Boer en Jaap van Beek.

Andere bekende vormen zijn nog softwarecertificering[2], ZekeRE Zorg (DBC- en AWBZ-registratie en -facturering), ZekeRE Business (elektronisch zakendoen) en Trust Services. Zie verder [Oeve02].

2 Softwarecertificering is eigenlijk vorm van IT-assurance met een oordeel over betrouwbaarheidsfunctionaliteiten.



Figuur 1. **Managementsysteem voor informatiebeveiliging met Plan-Do-Check-Act-cyclus.**

Eisen aan de auditor die een assurancerapport verstrekt

Niet iedereen mag een assurancerapport verstrekken. In de Nederlandse vertaling van de ISAE 3402-standaard (bekend als Richtlijn 3402 en Standaard 3402, opgesteld door respectievelijk NOREA en NIVRA) ([NORE10]) wordt vermeld dat alleen een 'beroepsbeoefenaar' bevoegd is om een ISAE 3402-assurancerapport te verstrekken. Voor een beroepsbeoefenaar wordt door de NOREA verwezen naar de IT-auditor, mits deze voldoet aan het Reglement Gedragscode 'Code of Ethics'. Deze code is van toepassing op iedere in het RE-register ingeschreven IT-auditor. Hetzelfde geldt voor RA's die zijn ingeschreven bij het NBA/NIVRA. Een ISAE 3402-assurancerapport kan daarom alleen door een ingeschreven RE of RA worden verstrekt.

Ook bij privacyaudits staat opgenomen dat de Registeraccountant (RA) of de Register EDP-auditor (RE), die beschikt over de aanvullende vereiste gespecialiseerde kennis en ervaring zoals aangegeven in paragraaf 12 van de richtlijn 'Assurance-opdrachten tot bescherming van persoonsgegevens', deze privacyaudits mogen uitvoeren.

Certificering

Het certificeren is alom bekend van de ISO 9001-certificaten bij menige organisatie, alleen de inhoud van certificering is minder bekend. De oorsprong van certificering ligt dan ook in het verantwoorden over kwaliteitsmanagementsystemen, in eerste instantie bij de Amerikaanse overheid en (defensie-)industrie. De ISO 9001-standaard heeft uiteindelijk in 1987 het levenslicht gezien, waarna er in de afgelopen 25 jaar vele zijn gevolgd – met als bekendste op IT-gebied de ISO 27001 voor informatiebeveiliging. In dit artikel richten wij ons op de IT-gerelateerde certificeringsstandaarden (zie kader 1 op blz. 16).

Aard

Certificatie betreft het door een onafhankelijke, geaccrediteerde partij laten vaststellen of het managementsysteem van de betreffende organisatie voldoet aan alle eisen op een bepaald gebied. Het managementsysteem is de wijze waarop een organisatie of proces bestuurd wordt, oftewel de organisatiestructuur en de samenhangende beleidsregels, afspraken en werkwijzen binnen een bedrijf ten behoeve van een planmatige en systematische beheersing en verbetering van bedrijfsprocessen en -procedures om vooraf bepaalde doelstellingen te realiseren. Onderdeel hiervan vormt de door Deming ontwikkelde 'Plan-Do-Check-Act'-cirkel voor het continu verminderen van variatie in de procesuitvoering. Variatie gaat namelijk ten koste van de kwaliteit van een product of dienst.

De specifieke certificeringseisen of -criteria zijn opgenomen in een certificeringsstandaard of beoordelingsrichtlijn; de wijze van certificering voor een bepaalde standaard is opgenomen in een zogeheten certificatieschema. Deze standaarden en schema's kunnen worden beheerd door zowel publieke als private partijen (zie verder onder 'Overige vormen').

Gebruik van 'certificering' in software- en privacycertificering is misleidend vanwege het assurancekarakter

In figuur 1 is gevisualiseerd hoe een managementsysteem voor ISO 27001 (Information Security Management System, ISMS) op hoofdlijnen functioneert.

Het certificaat wordt over het algemeen voor een periode van drie jaar toegekend, mits blijvend aan de eisen wordt voldaan. Na de initiële certificeringsaudit vindt één of meer keren per jaar een controle- of surveillanceaudit plaats. Na drie jaar volgt er een nieuwe cyclus, tenzij het certificaat door de certificatie-instelling of de overheid[3] wordt ingetrokken of de organisatie de certificering niet continueert.

Typen

In feite is sprake van vier hoofdtypen van certificering:

- *Organisatie- of procescertificering.* Een procescertificaat verklaart dat een organisatie met haar specifieke vervaardigings- of verwerkingsproces voldoet aan de certificeringscriteria of bepaalde technische specificaties. Deze zijn dan veelal vastgelegd in een norm of in een attest (zie hieronder).
- *Productcertificering.* Idem voor een product of (technische) component.
- *Attest.* Bij een productcertificaat gaat het over de eigenschappen van een product, bij een attest gaat het over de toepassing van een product: een attest is een verklaring dat een product of systeem geschikt is voor de beoogde toepassing. Het attest beschrijft het product of het systeem. Eenmaal afgegeven vinden normaliter geen controles meer plaats.
- *Persoonscertificering.* Een persoonscertificaat is een bewijs dat een persoon heeft aangetoond aan vastgestelde vakbekwaamheidseisen te voldoen.

Voor de eerste en laatste zijn er certificatie-instellingen en voor de tweede testlaboratoria/ inspectie-instellingen en kalibratielaboratoria (voor meetinstrumenten). In het vervolg van dit artikel laten wij de product- en persoonscertificering buiten beschouwing.

Certificeringsaanpak

Om vast te stellen of een organisatie een certificaat verdient voert een geaccrediteerde certificatie-instelling een certificatie-audit uit. Een certificatie-audit bestaat veelal uit een aantal hoofdfasen:

1. *Aanvraag, scoping en risicoanalyse.* In de voorbereidende fase zal een organisatie naast haar doelstellingen voor de certificering ook de reikwijdte ervan moeten bepalen. Dit gebeurt in een zg. Verklaring van Toepasselijkheid ('Statement of Applicability'). In deze verklaring staat vermeld welke processen en/of locaties van een organisatie en welke normen uit de standaard van toepassing zijn. Deze verklaring wordt op het uiteindelijke certificaat opgenomen. In deze fase wordt tevens kennisgenomen van de uitgevoerde risicoanalyse en de selectie van maatregelen door de organisatie. Derhalve hoeft niet per definitie de gehele set van maatregelen uit een ISO-standaard te worden geïmplementeerd.
2. *Documentatieonderzoek.* De opzet van het managementsysteem wordt vastgesteld aan de hand van de documentatie, vergelijkbaar met een opzetbeoordeling of Test of Design.
3. *Implementatieonderzoek.* Vervolgens onderzoekt de certificerende partij de (corrigerende) maatregelen om de risico's uit de risicoanalyse en/of documentatie op te heffen. Hieruit komen al dan niet tekortkomingen. In de certificaatsperiode van drie jaar dienen alle geselecteerde maatregelen een keer aan bod te komen.
4. *Afstemmen certificatierapport en afgifte certificaat.* Na de afstemming van het certificatierapport besluit de leadauditor over de ernst van de geconstateerde tekortkomingen ten opzichte van de certificeringseisen. Hierbij is sprake van kritieke (major) en niet-kritieke (minor) non-conformiteiten. Een kritieke non-conformiteit houdt onmiddellijk een hoog risico in dat binnen drie maanden verholpen moet zijn, een niet-kritieke moet voor de volgende certificeringsaudit zijn opgelost[4]. Hierbij zal de certificatie-instelling terugkeren om een oorzaakanalyse, corrigerende maatregelen en de implementatie daarvan te beoordelen. Uiteindelijk zal worden overgegaan tot afgifte van het openbare certificaat, het certificatierapport met de eventueel geconstateerde non-conformiteiten blijft vertrouwelijk.

Eventueel kan er nog een proefbeoordeling plaatsvinden tussen stappen 1 en 2 om te bepalen in hoeverre de organisatie gereed is om voor de formele certificeringsaudit op te gaan. De bevindingen uit deze eventuele proefbeoordeling kunnen worden (her)gebruikt voor de formele certificering als deze binnen vier maanden na de proefbeoordeling plaatsvindt.

3 Zoals toen de OPTA besloot om de registratie van DigiNotar als leverancier van elektronische handtekeningen (certificaten) in te trekken.

4 Indien na een jaar de niet-kritieke non-conformiteit niet is verholpen, wordt deze per definitie naar een kritieke non-conformiteit gepromoveerd.

Kader 1. **Standaardisatieorganen en IT-standaarden**

Er zijn internationaal en nationaal verschillende standaardisatieorganen die assurance- en met name certificeringsstandaarden opstellen en beheren, zoals:

- *algemene internationale standaardisatieorganisaties*: de International Organization for Standardization (ISO), de International Electrotechnical Commission (IEC) en de International Telecommunication Union (ITU);
- *specifieke internationale organisaties:* de Institute of Electrical and Electronics Engineers (IEEE), de Internet Engineering Task Force (IETF) en het World Wide Web Consortium (W3C);
- *Europese organisaties:* zoals de European Committee for Standardization (CEN), de European Committee for Electrotechnical Standardization (CENELEC) en de European Telecommunications Standards Institute (ETSI);
- *nationale organisaties*: American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST) (beide Amerikaans), British Standards Institution (BSI), Deutsches Institut für Normung (DIN) en het Nederlands Normalisatie-instituut (NEN);
- *private partijen of consortia*: zoals EMVCo (Europay MasterCard Visa) voor chipbetaalkaarten en -lezers, de PCI (Payment Card Industry) Security Standards Council voor de beveiligingsstandaard inzake de beveiliging van betaalkaarten, de World Lottery Association (WLA) voor informatiebeveiliging bij loterijen en de Software Improvement Group (SIG) voor softwarekwaliteit.

Tot de relevante IT-gerelateerde certificeringsstandaarden behoren, naast de eerdergenoemde ISO 27001-standaard:

- ISO 20000: IT Service management;
- ETSI TS 101 456: gekwalificeerde elektronische handtekeningen;
- ISO 22301/BS25999: Business Continuity Management;
- ISO 31000: Risicomanagement;
- ISO 29100: Privacy framework;
- NEN 7510: Informatiebeveiliging in de zorg (toepassing van ISO 27001 in de zorgsector);
- ISO 24760: Framework for Identity Management;
- ISO 24745: Biometric Information Protection;
- ISO 27034: IT security techniques – application security;
- ISO 15408: Evaluatiecriteria voor IT-beveiliging (beter bekend als de 'Common Criteria');
- ISO/IEC 29147: Responsible vulnerability disclosure;
- ISO/IEC 13335: IT Security management;
- ISO/IEC 38500: Corporate governance of information technology;
- ISO/IEC 19770: Software Asset Management;
- ISO 15489: voor records management en archivering;
- ISO/IEC 15288:2008: Systems and software engineering – System life cycle processes
- ISO 90003:2004: Software engineering – Guidelines for the application of ISO 9001:2000 to computer software;
- CMMi: Capability Maturity Model integration voor de kwaliteit van softwareontwikkeling.

Eisen aan certificatie-instelling en -auditor

ISO-certificaten kunnen door verschillende certificatie-instellingen en daarvoor werkende auditors worden verstrekt. De accreditatie-eisen aan de organisaties zijn vastgelegd in ISO 17020[5] (algemeen) of ISO 17025 (laboratoria) of EN45011 (productcertificatie).

Certificering mag alleen worden uitgevoerd door goedgekeurde c.q. geaccrediteerde certificatie-instellingen. De Raad voor de Accreditatie houdt toezicht op het goed functioneren van de certificatie-instellingen in Nederland. In bijzondere omstandigheden waarbij de certificatie-instelling opereert binnen een wettelijk kader, is het noodzakelijk dat deze (aanvullend) een zg. aanwijzing voor een bepaalde periode van de overheid krijgt. Dit geldt bijvoorbeeld voor de certificering in het kader van de Wet Elektronische Handtekeningen; de PKI- of certificatiedienstverleners mogen alleen door een door het ministerie van EZ aangewezen certificatie-instelling worden onderzocht.

Iedere certificatie-instelling moet een belangenvertegenwoordiging hebben[6]. In Nederland noemen we dit het College van Deskundigen / Belanghebbenden. De taak van zo'n college is de onpartijdigheid van de instelling te waarborgen. Bij maatschappelijk relevante onderwerpen wordt vaak gebruikgemaakt van één geharmoniseerd certificatieschema. Meestal beheert dit college het certificatieschema. Een dergelijk college is meestal ondergebracht in een rechtspersoon zoals een stichting, zodat het centrale college overeenkomsten kan aangaan met de nationale

5 Conformity assessment – Requirements for the operation of various types of bodies performing inspection.

6 ISO 17021 vereist namelijk dat certificatie-instellingen een eigen orgaan hebben waarin hun onafhankelijkheid en onpartijdigheid wordt geborgd.

accreditatie-instelling. In geval van een centraal college controleert de accreditatie-instelling zowel het centrale college als de certificatie-instellingen die eraan verbonden zijn. Voorbeeld is ECP-EP.nl, die de door haar ontwikkelde certificeringsschema's voor ISO 27001 en TTP.nl (elektronische handtekeningen) in Nederland beheert (zie ook [Koor02]).

Overeenkomsten en verschillen tussen assurance en certificering

Zoals uit bovenstaande beschrijvingen van assurance en certificering blijkt, zijn er diverse overeenkomsten en verschillen tussen assurance en certificering. Belangrijke overeenkomsten zijn dat voor beide vormen drie partijen aanwezig zullen moeten zijn, namelijk de certificerende partij, de verantwoordelijke partij en de partijen die gebruik (willen) maken van diensten van de verantwoordelijke. Daarnaast is bij certificering ook sprake van een object van onderzoek (bijvoorbeeld informatiebeveiliging bij een ISO 27001) en is er sprake van toetsingsnormen waaraan voldaan moet worden.

Belangrijke verschillen tussen assurance en certificering zijn met name gelegen in de scope/diepgang (managementsysteem versus individuele normen/maatregelen) en de manier waarop wordt gerapporteerd over de uitkomsten (assurancerapport versus certificaat) en hiermee ook de doelgroep en verspreidingskring.

De belangrijkste verschillen tussen assurance en certificering zijn weergegeven in tabel 1. Hierbij is voor de duidelijkheid het verschil tussen een 3000/3402-assurance-opdracht en een ISO 27001-certificering opgenomen.

Wederzijds gebruik van IT-assurance en -certificering

In toenemende mate komt zowel IT-assurance als IT-certificering voor in dezelfde omgeving of serviceketen. Indien een organisatie zoals een IT-serviceprovider over beide beschikt is te bezien in hoeverre efficiëntiewinst haalbaar is door zoveel mogelijk de normenkaders en werkingsperioden op elkaar af te stemmen (zie ook de slotparagraaf Marktvisies).

In het geval er op elkaar moet worden gesteund zijn twee situaties te onderscheiden:

- Bij een IT-certificering kan worden gesteund op een IT-assurancerapport indien de normen en werkingsperioden overlappend zijn. Bij afwijkende perioden kan voor de certificering geopteerd worden door te onderzoeken of het managementsysteem de resterende maanden naar behoren heeft gefunctioneerd.
- Wanneer bij IT-assurance moet worden gesteund op een certificering die heeft plaatsgevonden, bijvoorbeeld bij uitbesteding aan een IT-serviceprovider met een ISO 27001-certificaat, gelden er beperkingen. Zeker als het een Type 2-rapport betreft kan niet worden volstaan met een ISO-certificaat, aangezien onduidelijk is welke normen in het betreffende jaar zijn 'geraakt' en aangezien niet alle normen/maatregelen ieder jaar of met voldoende waarnemingen worden onderzocht. Dit betekent dat de meeste auditwerkzaamheden zelfstandig moeten plaatsvinden.

Toekomstige ontwikkelingen

Verschillen en overeenkomsten tussen assurance en certificering zijn voor zowel serviceorganisaties als gebruikersorganisaties vaak nog onduidelijk. Een mogelijke oorzaak hiervoor is de grote hoeveelheid soorten assurance en certificering in de markt. Om goed de waarde en bruikbaarheid van assurance of certificering te kunnen begrijpen is het van belang dat de bewustwording over de verschillen wordt verbeterd.

De afgelopen jaren hebben diverse ontwikkelingen rondom assurance en certificering plaatsgevonden. Er zijn in die periode nieuwe vormen van assurance ontstaan. Zo heeft SAS 70 plaatsgemaakt voor de nieuwe ISAE 3402-standaard (SOC 1); ook de SOC 3-webrapportage is een relatief nieuwe vorm van assurance. Bij certificering blijven de ontwikkelingen eveneens doorgaan.

De verdere ontwikkeling rondom assurance en certificering is lastig te voorspellen. Op basis van de recente ontwikkelingen en de marktvisies die zijn opgenomen in dit artikel (zie blz. 19-21) verwachten wij dat de volgende ontwikkelingen zich in de toekomst voor kunnen doen rondom assurance en certificering:

Bewustzijn over verschillen tussen assurance en certificering moet sterk omhoog

	Assurance (ISAE 3000/3402/3600)	Certificering (ISO 27001)
Rapportage		
Product	Assurancerapport (uitgebreid met standaard-verklaring erin)	Certificaat (kort en gestandaardiseerd)
Managementverklaring	Ja, opgenomen in SOC 1 / 3402-rapport, ook van eventuele onderaannemers	Nee
Organisatie met behalen volledig in control	Nee, het assurancerapport kan afwijkingen bevatten	Ja, van het managementsysteem, niet zozeer van de onderliggende beheersingsmaatregelen. Een organisatie behoudt haar certificaat alleen als alle kritieke non-conformiteiten op korte termijn zijn verholpen. Certificaat bevat geen beschrijving van tekortkomingen.
Doelgroep & verspreidingskring		
Gehanteerde normen specifiek voor organisatie of gebruikersorganisaties	Ja	Nee, standaardset met alleen keuze voor organisatieonderdelen/normen buiten scope
Specifieke doelgroep	Ja, de klanten van de serviceorganisatie	Nee, kunnen zowel klanten als andere belang-hebbenden zijn
Verspreidingskring	Beperkt tot klanten (m.u.v. SOC 3 bij openbaar webzegel)	Algemeen geldend, geen beperking aan verspreidingskring
Gebruik voor (overheids)toezicht	Ja, in toenemende mate verplicht (bijv. bij uitbesteding)	Beperkt, NEN 7510-certificering staat op nominatie om verplicht te worden gesteld voor zorgverleners*
Overige aspecten		
Onderaannemers in scope mogelijk (zgn. 'inclusive-model')	Ja, duidelijk leesbaar voor gebruikersorganisaties, tenzij is gekozen voor 'carve-out'-model	Nee, iedere organisatie heeft eigen certificaat nodig
Diepgang	Ieder jaar bestaan en werking van alle normen, op basis van toereikende steekproef	Over driejaarsperiode van (bestaan van) alle normen
Zekerheid verstrekt door RE of RA	Ja	Nee, niet verplicht, uitsluitend door geaccrediteerde onafhankelijke en deskundige certificatie-instellingen en auditors
Mate van zekerheid	Beperkte of redelijke mate van zekerheid	Alleen redelijke mate van zekerheid
Geldig in de toekomst	Nee	Ja
Beschrijving van test-werkzaamheden opgenomen	Ja, verplicht in ISAE 3402 (inclusief testresultaten), gebruikelijk in ISAE 3000	Nee
Steunen op internal audits	Ja, als IAD (-er) voldoet aan bekwaamheids-, onafhankelijkheids- en opleidingseisen	Ja
Oordeel over werking (toetsing over bepaalde periode)	Ja, alleen bij type 2, type 1 omvat alleen opzet en bestaan	Nee, in feite alleen opzet en bestaan
Globale inspanning (bandbreedte bij overeenkomstige organisatie en scope)	25-70 dagen (in daaropvolgende jaren 70-90% van initiële audit)	6-18 dagen (in tweede en derde jaar ca. 40-55% van initiële audit, vervolgens weer hercertificering)
Vast normenkader en scope	Nee, geen vast normenkader, beheersings-maatregelen worden specifiek gemaakt voor de serviceorganisatie en haar klanten	Ja, conform relevante (ISO-) standaard, voorgedefinieerde set van maatregelen

**) Zie ook [Justo3], waarin wordt gesteld dat certificering vooral dan een geschikt instrument is als de keten van privaat toezicht voldoende betrouwbaar is, de activiteiten van de private toezichthouders voldoende controleerbaar zijn, en er voldoende draagvlak bestaat bij de organisatie.*

Tabel 1. **Verschillen tussen assurance en certificering.**

Een ISO 27001-certificering kan wel steunen op een IT-assurance-opdracht, omgekeerd vrijwel niet

- Door de toename van wet- en regelgeving en het zichtbaar kunnen nemen van verantwoordelijkheid voor de uitbestede processen verwachten wij dat de vraag naar assurance en certificering de komende jaren zal toenemen. Door onduidelijkheden in de markt over de overeenkomsten en verschillen tussen certificering en assurance, en doordat (potentiële) klanten om verschillende vormen van zekerheid vragen, verwachten wij dat steeds meer serviceorganisaties een combinatie van certificering en assurance zullen aanbieden aan (potentiële) gebruikersorganisaties. De aanpak zal hierbij meer verschuiven naar certificering/ISO 27001 als basis (opzet en bestaan), waarbij aanvullend ook de werking aangetoond zal worden met een IT-assurancerapport.
- Zoals te lezen valt in de visies uit de markt (zie de slotparagraaf), wordt verwacht dat certificering in waarde zal dalen en dat er in toenemende mate geïntegreerd, dus over naleving van meerdere normenkaders, gaat worden gemonitord en gerapporteerd (zg. Integrated Reporting op basis van breed Business Control Framework). Dit geeft overkoepelend inzicht en verlicht tevens de als hoog ervaren auditdruk.
- De toekomst van IT-certificering en IT-assurance ligt wellicht in de combinatie van beide, alsmede verdere professionalisering van Continuous Auditing, Monitoring en Assurance. Wij verwachten dat het frequenter auditen een logische vervolgstap zal zijn naar een bredere beheersingsscope met het monitoren van meerdere audit- en complianceonderwerpen; dit staat ook wel bekend als IT GRC (Governance, Risk & Compliance). Er is in de markt ook meer vraag naar tussentijdse informatie over de kwaliteit en beheersing van uitbestede processen. Hierbij zijn tussentijdse KPI/KRI-rapportages van belang, die al dan niet worden geaudit, en a tempo Continuous Assurancerapportages waarop te reageren en sturen valt.
- Gerelateerd aan assurance zijn SOC 2 en SOC 3 relatief nieuw. Onze verwachting is dat deze vormen snel populair zullen worden. Vanuit marketingoverwegingen is meer vraag naar SOC 3 te verwachten, wellicht met name bij organisaties die daarmee de grootste 'vertrouwenssprong' kunnen maken (zoals SaaS/cloud-leveranciers).
- De ontwikkelingen zullen daarnaast verschillen per branche. Uit de marktvisies blijkt dat één van de belangrijkste redenen voor het verstrekken van een assurancerapport of certificaat door een serviceorganisatie de klantwens is. Op dit moment verschilt de vraag naar assurance of certificering per sector. Zo is in de IT-sector zowel assurance als certificering gebruikelijk. Daarentegen is voor bijvoorbeeld uitbestede processen door pensioenfondsen,waaronder pensioenadministratie en vermogensbeheer, de vraag naar assurance (en dan specifiek ISAE 3402) gebruikelijk. Het beschikken over een ISAE 3402-rapport zegt natuurlijk nog weinig over de scope en het normenkader die het rapport zal bevatten en de frequentie waarmee wordt gerapporteerd. Dus zowel aanbieders als afnemers van assurance of certificering zullen explicieter moeten afstemmen welke eisen en wensen er zijn om ervoor te zorgen dat het product zijn relevante rol behoudt of versterkt en niet verwordt tot een 'tick in de box'.

Marktvisies

Wij hebben twee afnemers en twee aanbieders van IT-assurance en/of ISO 27001 een aantal vragen gesteld over hun visie rondom dit onderwerp. Deze paragraaf bevat een kort overzicht van de reacties.

Wie is verantwoordelijk?

Aanbieders

- CFO was en is voor zowel de ISO 27001 als de ISAE 3402 de eindverantwoordelijke. De uitvoering ligt bij de afdeling Risk Management & Compliance.

Afnemers

- De verantwoordelijkheid voor informatiebeveiliging ligt bij de afdeling Information Risk Management. De 'Corporate Information Security Manager' is gestart met 3402-traject onder verantwoordelijkheid van IRM met begeleiding vanuit Internal Audit. Op dit moment is het onderwerp teruggegeven aan de ICT-dienstenorganisatie en is daarmee een vast onderdeel van de uitbestedingsstrategie (overeenkomst) en het interne IT Control Framework.
- De afdeling ICT is verantwoordelijk voor de informatiebeveiliging en vraagt in dat kader TPM's aan de IT-dienstenleveranciers. In specifieke situaties heeft de accountant van de afdeling ICT de mogelijkheid gekregen om onderzoek te doen om een beeld te krijgen of de dienstverlening conform de gemaakte afspraken wordt geleverd.

Waarom gekozen voor zowel IT-assurance als ISO 27001-certificering?

Aanbieders

- In de praktijk betekent gecertificeerd zijn voor veel bedrijven een jaar lang opzet en bestaan onderhouden en pas rond de jaarlijkse audit verhoogde aandacht voor de werking, ondanks dat de Kwaliteitsafdeling de PDCA-cyclus op gang houdt. IT-assurance dwingt de organisatie tot continuïteit en aantoonbaarheid van activiteiten en vermindert daarmee de 'dip' na de jaarlijkse audit en de 'spike' voor de volgende audit.
- Wij waren al ISO 27001- en ISO 9001-gecertificeerd omdat dat tot onze dienstverlening behoort. Het hebben van beide certificaten en een ISAE 3402-rapport wordt ook door veel van onze klanten geëist.

Afnemers

- In 1999 was BS17999 een logische keuze omdat men behoefte had aan een best-practices op het gebied van informatiebeveiliging. En een absolute voorwaarde om een vergunning van de toezichthouder te verkrijgen. In die tijd waren alle IT-processen intern belegd in tegenstelling tot nu. Daarom is in 2006 ook besloten om IT-assurance te vragen aan iedere relevante IT-leverancier over de door hem geleverde diensten.
- Onze IT-diensten zijn uitbesteed. De afdeling ICT ontvangt van één van de providers een ISAE 3000-verklaring omdat deze 'free format' is en getoetst wordt op basis van het referentiekader dat de organisatie en serviceprovider overeengekomen zijn. De providers laten uit hoofde van de contracteisen zich certificeren op basis van ISO 27001.

In hoeverre is er overlap IT-assurance – ISO 27001-certificering?

Aanbieders

- In feite geen overlap. IT-assurance, mits goed opgezet, is een verlengstuk van normeringen / certificering en een middel om de doelen die geleid hebben tot en voortkomen uit de certificeringstrajecten beter te onderhouden en dus kwaliteit en continuïteit beter te waarborgen. IT-assurance helpt ook om de verantwoordelijkheid daar te beleggen waar die thuishoort.
- In 3402 is een aantal controledoelstellingen uit de ISO-certificaten overgenomen en uitgewerkt. Deze zijn aangevuld met vooral specifieke HR-doelstellingen.

Afnemers

- Bij een aantal algemene aspecten is er sprake van overlapping, zoals bij fysieke beveiliging. Bij de assuranceverklaringen kunnen providers waar nodig dan ook gebruikmaken van de resultaten uit ISO 27001-verklaringen. De providers zijn overigens contractueel verplicht ook zo'n verklaring te hebben.
- IT-assuranceverklaring maakt deel uit van de verantwoording aan de toezichthouder in het kader van de totale bedrijfsvoering. ISO 27001-certificering is onderdeel van de aanbestedingstrajecten. Reden hiervoor is een zekerheid te hebben dat de provider zijn organisatie op een beheerste wijze heeft ingericht.

Communicatie met klanten over verschillen en overeenkomsten tussen assurance en certificering?

Aanbieders

- Veelal nog ad-hoc, reactieve communicatie n.a.v. vragen. Intern gaat nadere toelichting worden opgesteld voor intern gebruik, voor proposals en/of andere externe communicatie.
- Bij klanten wordt het rapport op verzoek aangeboden en toegelicht door onze afdeling of de relatiemanager.

Afnemers

- We moeten het verschil tussen beide typen externe verantwoording door serviceproviders vaak aan onze eigen organisatie uitleggen.
- Certificering maakt onderdeel uit van een contract tussen de organisatie en de serviceprovider. Over een verschil tussen certificering en assurance wordt niet gesproken.

Voor wie is het assurancerapport en ISO-certificaat bedoeld?

Aanbieders

- De ISO-certificaten zijn voor de volle breedte, dus zowel voor partners, interne en externe klanten bedoeld. IT-assurance is specifiek opgezet voor één klant, met de bedoeling het in de toekomst generiek te maken omdat deze klant inziet dat IT-assurance voor de volledige dienstverlening bijdraagt aan kwaliteitsverbetering en tegemoetkomt aan de vraag van klanten.
- ISO-certificaten voor al onze klanten. Assurance-rapport voor de klanten waar wij resultaatverplichte opdrachten voor uitvoeren.

Afnemers

- Als derde partijen primaire IT-processen voor ons uitvoeren is er bijna altijd sprake van een 3402-verklaring. Dit laatste is ook noodzakelijk in het kader van financiële en operationele auditwerkzaamheden. In alle andere gevallen maakt het voldoen aan de ISO 2700x-kwaliteitsnorm standaard onderdeel uit van onze inkoopvoorwaarden.
- We maken intern zeer beperkt gebruik van ISO 27001-verklaringen van leveranciers.

Wat zijn neveneffecten van beide trajecten?

Aanbieders

- Uit het IT-assurancetraject zijn diverse efficiëntieslagen naar voren gekomen. Een IT-assurancetraject dwingt om nog eens goed stil te staan bij wat men doet, de noodzaak van wat men doet en zo ja, of en hoe dat meetbaar en aantoonbaar te maken is. Expliciete keuzes moeten worden gemaakt. Hierdoor kan qua efficiëntie veel worden gewonnen maar ook commercieel; activiteiten die niet zijn overeengekomen en/of vastgelegd maar wel nodig blijken kunnen formeel aangeboden worden aan klanten; door werkwijzen in lijn te brengen kan men makkelijker profiteren van elkaars expertise en capaciteit.
- Door integratie van rapportage over de verschillende frameworks hebben we efficiëntie behaald in de auditingkosten en -belasting voor de organisatie.

Afnemers

- We denken wel dat enige kwaliteitsverbetering te meten is. Het is in ieder geval zo dat we de leverancier makkelijker (inhoudelijk) kunnen aanspreken. Dagelijkse problemen in de dienstverlening (veelal procesmatig) worden hiermee echter zelden opgelost.
- Zeer beperkt, de assuranceverklaringen worden voor 'certificeringsdoeleinden' gebruikt.

Wordt Continuous Auditing/Monitoring toegepast?

Aanbieders

- Vanuit de Kwaliteitsafdeling is er een continu doorlopende interne auditcyclus die alle vier de certificeringen dekt. IT-assurance zal in de toekomst helpen om de auditdruk op de organisatie te verminderen en de wijze van auditen kan hierdoor ook veranderen omdat vanuit IT-assurance al veel evidence zal worden geleverd.
- Met de projectthermometers in het kader van de ISAE 3402 (periodieke self-assessments) en de continue monitoring vanuit India.

Afnemers

- Wij passen dit vanaf 2013 toe op al onze belangrijke processen via een Business Control Framework.
- We werken er momenteel aan om dit te bereiken.

Welke ontwikkelingen worden op dit terrein in de toekomst verwacht?

Aanbieders

- Verwacht wordt dat de 'waarde' van certificering steeds minder gaat worden, van een onderscheidend vermogen is certificering verworden tot gemeengoed; iets wat standaard aanwezig is. Klanten, intern en extern, zoeken steeds meer naar zekerheid dat je als leverancier ook daadwerkelijk en continu doet wat er is overeengekomen. Daarbij staat de druk die certificering en assurance leggen op leveranciers in schril contrast met de toenemende vraag naar prijsverlaging. In de IT-outsourcingbranche voorzien we in de nabije toekomst een breekpunt waarbij voor de prijs die klanten willen betalen de gevraagde certificeringen en assurance niet meer zijn op te brengen. De uitdaging is dus om de twee ineen te schuiven; elkaar te laten complementeren en tegelijk dermate toegevoegde waarde voor de organisatie te laten opleveren dat je van kostenpost naar toegevoegde waarde gaat.
- Meer integratie van frameworks en verschillende controledoelstellingen. In de verdere toekomst voorkeur voor een Integrated Assurance-rapport, één rapport voor de onderbouwing van zowel de assurance alsook de certificeringen.

Afnemers

- Wij sturen erop om de auditdruk verder te verminderen. En zoveel mogelijk frameworks (COSO, BCM, CobIt, ISO, Privacy, e.d.) af te dekken met het Business Control Framework-proces en bijbehorende 'in control'-verklaringen.
- Wij verwachten dat het jaarlijks verstrekken van assurancerapportages zijn langste tijd gehad heeft. Reden hiervoor is dat deze alleen maar historische informatie verstrekken waar het lijnmanagement niet op zit te wachten. We zien meer heil in Continuous Auditing/Monitoring en Continuous Assurance.

Met dank aan:

M.J. Maunder-Cockram (Fujitsu)

H. van Breukelen (Sogeti)

B. Lohmeijer (Rabo Vastgoed)

W. Tewarie (UWV)

Literatuur

[Just03] Expertisecentrum Rechtshandhaving, *Handhaving en certificering – een handreiking voor de beleids- en wetgevingspraktijk*, Ministerie van Justitie, 2003.

[Koor02] Drs.ing. R.F. Koorn RE CISA, drs. P. van Walsem RE en M. Lundin CPA CISA, *Auditing and Certification of a Public Key Infrastructure*, Information Systems Control Journal, Volume 5, 2002.

[NORE02] NOREA, Studierapport 3, *Raamwerk voor ontwikkeling normenstelsels en standaarden - Een facilitair instrument bij de beroepsuitoefening*, 2002.

[NORE10] NOREA, *NOREA Richtlijn 3402 assurancerapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie*, 2010 http://www.norea.nl.

[Oeve02] Drs. W.C.N. van Oeveren, dr. ir. P.L. Overbeek RE, ir. L. Yap, drs. P.A. van Walsem, drs. R.P. Schouten RE RA en drs. M.A. Francken RA, drs. K.H.G.J.M. Ho RE RA, drs. L. Hoogeveen, drs. H.G.Th. van Gils RE RA en drs. A.R.J. Basten RE, *Productcatalogus*, Compact, november 2003.

Over de auteurs

Drs. ing. R.F. Koorn RE CISA is partner bij KPMG Advisory. Hij is onder andere verantwoordelijk voor de adviespraktijk Overheid & ICT van KPMG en heeft zich gespecialiseerd in IT-kwaliteitsbeheersing, IT-governance, informatiekwaliteit, e-factureren, e-procurement, informatiebeveiliging en privacy.

Mw. S. Stoof MSc RA is assistent manager bij KPMG Accountants en adviseur bij KPMG Advisory. Zij is werkzaam als accountant bij diverse pensioenuitvoerders en pensioenfondsen, en betrokken bij diverse ISAE 3402- en overige assuranceopdrachten. Daarnaast voert zij IT-auditwerkzaamheden uit, waaronder in het kader van de jaarrekeningcontrole.