Efficiënt omgaan met procescertificering

J.C. Boer RE RA en drs. H.G.Th. van Gils RE RA

De toenemende vraag naar certificering van processen brengt onmiskenbaar kosten met zich mee. Kosten die het gevolg zijn van de roep om extra zekerheid over de mate waarin processen voldoen aan normen. In dit artikel wordt ingegaan op elementen van deze kosten en op welke wijze die kosten te beïnvloeden zijn. Ook wordt ingegaan op de vraag of kosten wel daadwerkelijk certificeringskosten zijn.

Inleiding

Initiatieven om de kwaliteit van producten aan te tonen bestaan al lange tijd. Feitelijk zelfs al sinds de gilden in Nederland, ook al hadden die naast kwaliteit ook wel andere doelen. Duidelijker wordt het in de industriële revolutie wanneer er door arbeidsverdeling op grote schaal behoefte aan kwaliteitscontrole ontstaat. Veelal was dat in de vorm van een kwaliteitscontroleur aan het einde van de productielijn (politioneel en repressief). Nadeel was dat de controle pas achteraf plaatsvond, dus de verspilling bleef. Hoewel de wetenschap in het midden van de vorige eeuw de efficiëntie verhoogde door aan te tonen dat via steekproeven ook een goed beeld van de kwaliteit kon worden verkregen, vonden de controleactiviteiten nog steeds achteraf plaats. Deze controles waren ook voornamelijk productgericht.
Na de tweede wereldoorlog komt in het kwaliteitsdenken de aandacht voor het *proces* sterk naar voren. Preventiekosten moeten vermijdbare kosten (afgekeurd product, herbewerkingskosten, verspilling materiaal, etc.) beperken. Vooral gestuurd door het Amerikaanse Ministerie van Defensie worden kwaliteitsnormen voor processen gedefinieerd en worden kwaliteitscontroleurs opgeleid om processen door te lichten en van een keurmerk te voorzien. Eerst nog alleen voor de wapenindustrie maar weldra ook voor andere productie- en dienstverleningsprocessen. Deze ontwikkeling is de basis geweest voor de bekende ISO-certificering.

De op kwaliteit gerichte procesuitvoerders zien certificering als een middel om verantwoording af te leggen over de geleverde kwaliteit en om zich zelf hiermee impliciet te dechargeren. Commerciële managers zien procescertificaten tegenwoordig als een middel om verkoopargumenten als betrouwbaarheid extra kracht bij te zetten. Afnemers van processen gebruiken de certificering om zich ervan te vergewissen dat ook de zaken waarop ze moeten vertrouwen (bijvoorbeeld procescontinuïteit) inderdaad worden geleverd. Bij het complexer worden van de procesketens (just-in-time verwerking of real-time processing) neemt de afhankelijkheid tussen leverancier en afnemer toe. Naast de relatie worden ketens ook complexer doordat onderdelen bij derden worden ondergebracht (outsourcing), met het doel de efficiency te vergroten en de kosten te verlagen.

Het gebruik van informatietechnologie maakt het mogelijk processen efficiënter in te richten, zodat bijvoorbeeld de buffers tussen de processchakels zo gering mogelijk kunnen worden gehouden. Denk hierbij aan tussenvoorraden in productiesystemen of wachttijden in e-commerce processen. Daardoor is er soms nauwelijks meer tijd om tussen de processtappen kwaliteitscontroles uit te voeren. De elasticiteit om tijdelijke knelpunten in het proces op te vangen wordt hierdoor teruggebracht tot (bijna) nul. Om hier geen hinder van te ondervinden moeten de processen zo goed als een 100%-betrouwbaarheid hebben. Om niet blind te hoeven vertrouwen op processen die buiten het eigen gezichtsveld liggen speelt procescertificering een belangrijke rol.

De accountantsverklaring bij de jaarrekening, de certificering van het product jaarrekening, kent beperkingen die thans ook in het maatschappelijk bewustzijn zijn doorgedrongen. Een gecertificeerde jaarrekening geeft weinig zekerheid over de kwaliteit van de administratieve processen. Bij recente bedrijfsschandalen lag hier juist de pijn. In reactie hierop is de drang ontstaan om, in navolging van de eerder geschetste ontwikkeling van procescontroles, de processen die ten grondslag liggen aan de (financiële) verantwoording te certificeren. We vinden dit terug in de Amerikaanse Sarbanes-Oxley wetgeving en de Nederlandse corporate governance-code zoals vastgesteld door de commissie-Tabaksblat. Bedrijven van enige omvang komen er niet onderuit om expliciet te verklaren dat hun interne processen voldoen aan de maatschappelijk geaccepteerde (nog vast te stellen) kwaliteitsnormen. In geval van een aan de Amerikaanse beurs genoteerd bedrijf zal deze interne verantwoording, op grond van de Sarbanes-Oxley wet, door de externe accountant moeten worden gecertificeerd.

Efficiency

De vraag naar certificering van processen zal de komende jaren naar onze verwachting toenemen. De uitvoering van procescertificering is echter arbeidsintensief. De kosten-nutverhouding wordt daarom niet altijd als evenwichtig gezien. Dit is ook begrijpelijk. Ongenuanceerd gesteld voegt de certificering inhoudelijk niets toe aan het proces. Zij geeft zekerheid over zaken die eigenlijk in orde horen te zijn. Het is als een verpakking. Het kost geld maar als het product eenmaal onbeschadigd zijn eindbestemming heeft bereikt, heeft het meestal geen waarde meer.

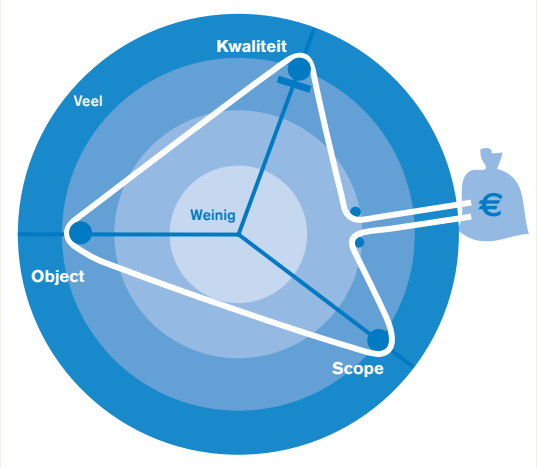
De vraag is dan ook welke mogelijkheden er zijn de balans van kosten en baten zo evenwichtig mogelijk te laten zijn.

Certificering geeft zekerheid
over zaken die eigenlijk in orde horen te zijn.

Verlagen van de kosten?

De eerste mogelijkheid is om de kosten voor certificering te verlagen. Dit kan bijvoorbeeld door er minder tijd aan te besteden of door het inzetten van minder gekwalificeerde (goedkopere) auditors. Veelal zal dat niet de oplossing kunnen zijn, omdat een verminderde inspanning als logisch gevolg zal hebben dat de kwaliteit en/of de diepgang afneemt. Het gevaar van het terugbrengen van het vaktechnisch niveau en een beperktere diepgang is dat er schijnzekerheid ontstaat. Elke keer dat blijkt dat de certificering niet tot het beoogde zekerheidsniveau heeft geleid, doet dan afbreuk aan het vertrouwen in certificeringen. Als deze verwatering optreedt, wat rest er dan? Overigens moeten natuurlijk wel alle mogelijkheden tot het vergroten van de efficiency van de certificeringswerkzaamheden worden benut. Dit kan bijvoorbeeld door gebruik te maken van onderzoeksresultaten van andere audits die om de een of andere reden inzake het te onderzoeken proces hebben plaatsgevonden of bijvoorbeeld door het ontwikkelen en inzetten van efficiënte audit tools.

Figuur 1.
Duivelsdriehoek.



Voor een vaste hoeveelheid geld kan met de elementen kwaliteit, objecten en scope worden geschoven, met dien verstande dat een verhoging van één element per definitie een verlaging van een of beide andere elementen inhoudt. Aangezien het verlagen van de kwaliteit een duidelijke ondergrens heeft om vertrouwen in het certificaat te behouden, is daarin een 'blokkade' aangebracht. Indien alle elementen moeten worden verhoogd, of één element meer dan evenredig moet worden verhoogd, zal dat dus financiële consequenties hebben. Omgekeerd, als ofwel het aantal objecten ofwel de scope verlaagd kan worden, zal dat minder kosten met zich meebrengen.

Toegevoegde waarde voor de eigen organisatie?

De tweede mogelijkheid om de kosten-nutverhouding te verbeteren is de toegevoegde waarde voor de eigen organisatie van certificering in ogenschouw te nemen. Door het nut te verhogen worden de kosten gerechtvaardigd. De ervaring leert dat de meeste energie in een certificeringsproces in de eerste jaren wordt gestoken in het op het vereiste niveau brengen van het proces en het in de tussentijd compenseren van tekortkomingen door (extra) detailcontroles uit te voeren. Door de auditors moet immers kunnen worden vastgesteld dat het proces conform de overeengekomen norm wordt uitgevoerd. Veel organisaties hebben nog niet het niveau van interne beheersing bereikt, waarop de beheersing ook doelmatig is aan te tonen. De processen moeten eerst op dat niveau worden gebracht. Niet alleen om te voldoen aan de norm, maar ook om dit aantoonbaar te maken. De kosten moeten in die gevallen dan ook niet alleen worden afgezet tegen het nut van de certificering, maar ook tegen de toegevoegde waarde die een procesverbetering heeft. Een beheerst proces heeft als toegevoegde waarde minder fouten, snelle signalering van de resterende fouten en overdraagbaarheid.
De afgesproken uitvoeringskwaliteit (de norm) is een aspect dat voor de afnemer deel uitmaakt van de afgenomen diensten en naar zijn perceptie betaalt hij voor deze kwaliteit. Mocht de uitvoerder niet aan deze kwaliteit voldoen, dan zijn de inspanningen van de uitvoerder vooral te beschouwen als procesonderhoud om te voldoen aan de afspraken met de afnemer. De kosten daarvan mogen niet gemakshalve als certificeringskosten worden beschouwd. Ook zonder certificering zou de uitvoerder van het proces moeten voldoen aan hetgeen hij met de afnemer is overeengekomen. De certificering in de vorm van een third-partymededeling (TPM) of een SAS70-report is niet de reden tot het op niveau brengen van de processen, maar de vraag van de klant. De certificering is immers slechts bedoeld om aan te geven dat wat geleverd is, overeenkomt met de afspraken. Zo ook de Sarbanes-Oxley certificering van de managementverklaring over de kwaliteit van de administratieve processen. De norm komt uit de wet en de kosten om processen daaraan te laten voldoen mogen niet worden verward met de certificeringskosten.

Toegevoegde waarde voor de klant?

De derde mogelijkheid om de kosten-nutverhouding te verbeteren is de toegevoegde waarde voor de klantorganisatie, de afnemer van certificering, in ogenschouw te nemen. Inmiddels is er een ruime keuze aan certificaten beschikbaar, zoals de bekende ISO 9000-certificaten, de ISO 17799-certificaten voor informatiebeveiliging, privacycertificaten, third-partymededelingen, trustproducten (als WebTrust en SysTrust) en de Amerikaanse SAS70-mededelingen. Voor een toelichting op dergelijke certificaten wordt verwezen naar Compact 2003/3.

De vraag is echter waar de klant behoefte aan heeft. De auteurs hebben contracten gezien waarin werd aangegeven dat jaarlijks een goedkeurende TPM door een onafhankelijke auditor moest worden afgegeven, zonder dat concreet werd gemaakt wat die TPM dan zou moeten inhouden. In de daaropvolgende discussies bleek dan

ook dat daar geheel niet over was nagedacht en dat er een grote verwachtingskloof was tussen de contractpartners, waarbij de kosten voor het TPM-onderzoek behorende bij de twee verwachtingen meer dan een factor 10 verschilden. Belangrijk is dat de certificeerder wordt betrokken bij het opstellen van een contract tussen opdrachtgever en auditor, om te voorkomen dat er afspraken worden gemaakt die niet reëel zijn gegeven het kostenniveau van de certificering en/of het overeengekomen niveau van dienstaanbieding.

In dit kader is relevant of de certificering:
* betrekking heeft op opzet en bestaan of anders gesteld betrekking heeft op de implementatie. In de SAS 70-systematiek wordt dit een type I-statement genoemd. Een dergelijke certificering heeft betrekking op de situatie op een specifiek moment.
* of gericht is op de werking of exploitatie van een proces, binnen SAS 70 aangeduid als een type II-statement. De certificering heeft betrekking op het functioneren van een proces over een aangeduide periode.

In een eerste reactie wordt altijd gesteld dat alleen de tweede, uitgebreide variant zinvolle toegevoegde waarde levert. De eerste betreft slechts een momentopname en heeft dus een beperkte geldigheid. Maar in beide gevallen doet zich het pikante kenmerk voor dat certificering van een proces per definitie betrekking heeft op het verleden. Echter, het grootste deel van de 'gebruikers' van de certificaten zoekt zekerheid naar de toekomst toe. En voor beide typen certificaten geldt de slogan 'resultaten uit het verleden bieden geen garanties voor de toekomst'...
En daarmee is de vraag weer relevant geworden of het duurdere type II-certificaat wel die extra toegevoegde levert die de afnemer verwacht. Wellicht dat door meer aandacht te schenken aan procedures tussen de contractpartners en de inhoud van de verantwoordingsrapportages van de te onderzoeken organisatie, aangevuld met een onderzoek naar het proces van totstandkoming van die verantwoordingsrapportages, het onderzoek beperkt kan blijven tot een onderzoek van de opzet en het bestaan. Het certificaat geeft voor buitenstaanders een beeld van de omgeving waarin het proces wordt uitgevoerd. Gecombineerd met hun eigen waarnemingen kunnen de betrokkenen hun totale beeld vormen. Het beeld ontstaat door de kwaliteit van de output van het proces en de terugkoppelingen vanuit de procesuitvoerder. Het certificaat vormt één van de onderdelen die bijdragen tot het totaalbeeld van de kwaliteit van het proces.

Een volgende vraag die zich voordoet is of de behoefte van de ontvanger van het certificaat wel duidelijk genoeg is. Aanzienlijke kosten kunnen worden bespaard als een procesaudit zich kan richten op die aspecten die voor de ontvanger relevant zijn. Zo kan tijdens de certificering bijvoorbeeld veel tijd worden besteed aan het beoordelen van de integriteit van de gegevensverwerking in een proces. Mogelijkerwijs is dit voor de auditor moeilijk vast te stellen terwijl de partij die het certificaat ontvangt aan de hand van de uitvoer van het proces zelf eenvoudig de integriteit kan vaststellen. Denkbaar is ook dat in de opdracht voor de TPM-audit staat dat de procesuitvoerder de vertrouwelijkheid van de gegevensverwerking voor zijn opdrachtgevers van groot belang acht en dat deze van de auditor derhalve eist goede aandacht te schenken aan maatregelen die ervoor zorgen dat zijn eigen medewerkers geen ongeautoriseerde toegang tot de gegevensverwerking kunnen verkrijgen. Maar dan blijkt bij de rapportbespreking dat de ontvanger van het certificaat zelf al alle gegevens encrypt voordat de gegevens naar de procesuitvoerder gaan en de opdrachtgever nauwelijks geïnteresseerd is in de maatregelen van de procesuitvoerder op dit gebied, omdat de opdrachtgever zelf al passende maatregelen heeft genomen. Waarschijnlijk kunnen veel kosten bespaard worden als eerst tussen opdrachtgever en procesuitvoerder goed wordt nagegaan welke aspecten in de procescertificering dienen te worden betrokken. Het is goed mogelijk dat dan goed afgebakende, beperkte audits kunnen worden uitgevoerd in plaats van meer algemene c.q. brede audits.

Conclusie

De toenemende vraag naar certificering van processen brengt onmiskenbaar kosten met zich mee. Kosten die het gevolg zijn van de roep om extra zekerheid over de mate waarin processen voldoen aan de normen. De kosten van de certificering zullen beperkt kunnen zijn als het proces volledig voldoet aan de eisen en dit ook eenvoudig is vast te stellen. Het proces moet derhalve controleerbaar zijn. Er is wel eens gesteld dat bij certificering de bewijslast voor een goede kwalitatieve uitvoering wordt omgedraaid. Niet de auditor moet allerlei controles uitvoeren om vast te stellen dat de processen aan de norm voldoen, maar de verantwoordelijke organisatie moet aantoonbaar maken dat de (beheer)processen adequaat worden uitgevoerd. In organisaties die sterk leunen op administratieve processen, zoals banken, zal het aantoonbaar maken van een kwalitatief goede uitvoering niet zo vreemd zijn; die organisaties zijn gewend aan een stelsel van interne controle. Andere (uitvoerings)organisaties, bijvoorbeeld een Information Service Provider, zullen daar veel meer moeite mee hebben. Zij hebben primair hun aandacht gericht op efficiënt draaiende processen en zolang die niet regelmatig verstoord worden 'is het toch goed...'. Maar juist bij deze categorie organisaties komen de meeste verzoeken tot certificering terecht. De kosten voor het op niveau brengen van de processen mogen echter niet worden verward met de kosten van de certificering.

Certificering van een proces biedt geen garanties voor de toekomst.

Bij het maken van afspraken over procescertificering is het gewenst dat hierbij een auditor met certificeringservaring is betrokken. De mogelijkheden zijn divers en nog weinig gestandaardiseerd. Zonder deze betrokkenheid bestaat de kans dat veel zwaardere vormen van certificering worden afgesproken dan noodzakelijk is. Door de advisering van de auditor over de mogelijkheden kan tevens al vroegtijdig inzicht worden verkregen in de kos-

J.C. Boer RE RA
is partner bij KPMG Information Risk Management. Hij heeft meer dan 25 jaar ervaring in het ICT-auditvak. Binnen KPMG IRM Nederland is hij verantwoordelijk voor het competence center 'information systems government'. Door deze verantwoordelijkheid is hij sterk betrokken bij de ontwikkelingen op het terrein van de certificering van processen.

boer.han@kpmg.nl

Drs. H.G.Th. van Gils RE RA
is senior manager bij KPMG Information Risk Management. Hij is trekker van verschillende certificeringsproducten binnen IRM, zoals de third-partymededelingen, softwarecertificering en privacycertificering.

vangils.herman@kpmg.nl

ten die de certificering met zich meebrengt. Al vaak hebben de auteurs meegemaakt dat de certificeringskosten veel hoger liggen dan de betrokkenen hadden verwacht. Daarom is het verstandig in het voortraject al advies aan een auditor te vragen en de ontwikkeling ter hand te nemen van de normenset die de basis voor de certificering moet gaan vormen. Zonder normen is certificering onmogelijk. Een vroegtijdig ingeschakelde auditor kan bijdragen in de kostenbesparing door vooraf goed te bepalen wat de werkelijke behoefte van de ontvanger van het certificaat is en wat dat betekent voor de scope en de te onderzoeken objecten.

Recente publicaties

How Sarbanes-Oxley will change the audit process, Journal of Accountancy, september 2003.

How CIO's should prepare for Sarbanes-Oxley, Gartner, 25 september 2003.

Kosten voor 'Sarbanes-Oxley', Financieel Dagblad, 12 augustus 2003.

Oordelen van gekwalificeerde IT-auditors, Norea, juni 2003.

TPM en corporate governance, themanummer Compact 2003/3.