

Certificering & ict

CERTIFICERING BEDOEGT TRANSPARANTIE, MAAR HOE TRANSPARANT IS CERTIFICERING?

In een steeds complexere en een zich verder globaliserende wereld, waarin ict veelal een vitale rol speelt in de bedrijfsvoering en strategie, nemen risico's toe en is vaker te horen dat er transparantie moet zijn en dat er verantwoording moet kunnen worden afgelegd over de beheersing van deze risico's. Het voor de buiten- en binnenwereld aantoonbaar in control zijn, is daarmee vandaag de dag een belangrijk aandachtspunt voor het management. Niet alleen het algemeen management, maar ook het ict-management wordt hiermee vroeg of laat geconfronteerd. Corporate governance en IT-Governance staan daardoor hoog op de agenda van het topmanagement.

door: Jan Matto en Karoline Muijs-de Graaf

Belangrijke katalysator in het corporate governance proces zijn aanscherpingen in de wet- en regelgeving, gericht op de bescherming van de omgeving van organisaties. Toezichthouders, aandeelhouders, ketenpartners, klanten en bestuurders (vanwege bestuurdersaansprakelijkheid) vragen om inzicht in risicobeheersing. Daar waar het gaat om het managen van risico's gerelateerd aan ict is het geven van inzicht in de mate van beheersing van deze risico's niet altijd eenvoudig. Ict is vervlochten met bedrijfsprocessen, de continuïteit van processen is afhankelijk van ict en de besluitvorming en bedrijfsvoering zijn afhankelijk van de betrouwbaarheid van de informatievoorziening. De beveiliging van de onderliggende data en systemen en de beheersing van ict-gerelateerde processen is hierbij cruciaal.

Ten einde zekerheid te krijgen over de kwaliteit van de ict-dienstverlening, kan het aantrekkelijk zijn de maatregelen, getroffen voor beheersing van risico's, te laten certificeren door een externe onafhankelijke partij. Een certificaat voor gebruik in het openbaar maatschappelijk verkeer geeft duidelijkheid voor de buitenwereld over de interne beheersing van ict. Zeker waar sprake is van outsourcing van ict-services is certificering in toenemende mate gebruikelijk als waarborg voor afnemers van deze services. Maar ook voor intern gebruik heeft een certificaat zeker zijn werking als het gaat om bewustwording te creëren voor de noodzaak voor risicobeheersing en is nuttig als managementinstrument om de kwaliteit van ict-processen te bevorderen en aantoonbaar te maken.

Soorten IT-certificering en IT-normenkaders

Kenmerkend voor certificering is dat deze plaatsvindt op basis van een gedefinieerd normenstelsel en certificatieschema en dat de certificering betrekking kan hebben op verschillende objecten van onderzoek. Er bestaan verrassend veel soorten ict-certificeringen met elk hun eigen doelstelling, herkomst, reikwijdte en normering. Certificering kan plaatsvinden op deelsystemen of deelprocessen of een deel van de ict-organisatie. Certificering kan ook gericht zijn op een bepaald kwaliteitsaspect van ict. Het kan bijvoorbeeld gericht zijn op gegevensbeveiliging of op het voldoen aan privacywetgeving. Ook applicatiesoftware kan worden gecertificeerd. Voor financiële softwarepakketten worden wel certificaten verstrekt met betrekking tot de betrouwbaarheid van de gegevensverwerking en de controleerbaarheid daarvan. Cruciaal voor een succesvolle certificering is dat vooraf

volstrekt duidelijk is wat de scope van de certificering is en vooral ook wat het normenkader exact omvat. Helaas zijn de standaard beschikbare normenkaders niet altijd even hard en helder gedefinieerd en is nadere afbakening, verdieping en aanscherping in normering meestal noodzakelijk.

Er bestaan veel verschillende normenkaders bruikbaar voor certificering. Sommige zijn meer bruikbaar voor strategische ict-domeinen, andere meer bedoeld voor tactisch of operationeel niveau.

Strategisch

Cobit 4.1. Verreweg de bekendste, meest voorkomende en uitgebreide best practice normenset voor certificering op ict-gebied is Cobit 4.1. Cobit is eigenlijk meer een hulpmiddel om de scope voor ict-beoordelingsopdrachten te formuleren, waarbij afhankelijk van de doelstelling van de opdracht (lees certificering) normatief beheersingsmaatregelen kunnen worden gedefinieerd. De aldus verkregen normatieve beheersmaatregelen kunnen vervolgens worden getoetst op bestaan en werking. Cobit 4.1 claimt volledigheid en is dan ook bijzonder uitgebreid en omvangrijk en dient dus met verstand te worden toegepast. Belangrijk is dat een organisatie niet 'Cobit-compliant' kan zijn. Cobit is eigenlijk een 'scoping tool' te gebruiken voor ict-certificering.

Sterk aan Cobit is dat het als één van de weinige normenkaders enige concrete, zij het met de nodige beperkingen, aanknopingspunten biedt voor certificering van processen welke meer op strategisch niveau liggen. Bezwaar van Cobit is zijn sterke 'rulebased' benadering en het feit dat Cobit de wereld van ict probeert te vatten in zogenaamde beheersdoelstellingen. Dat de context van een onderneming en de context van ict-systemen van grote invloed zijn op de aard en zwaarte van de te treffen maatregelen wordt niet afgedekt.

In tegenstelling tot Cobit blinkt de **AS 8015-2005 Australian Standard for Corporate Governance of IT** uit in beperkingen. Het richt zich alleen op IT-Governance. De standaard omvat slechts 12 pagina's. Op het terrein van IT-Governance lijken zich overigens twee stromingen te ontwikkelen. Eén stroming probeert IT-Governance te vatten in performance indicatoren voor de ict-processen en zoekt heil in een soort balance scorecard benadering voor ict-processen. Het meetbaar maken van ict en ict-processen is veelal gericht op efficiency'. De andere stroming richt zich meer op de beheersing van het besluitvormingsproces omtrent ict binnen organisaties en focust meer op verantwoordelijkheden en het borgen van alignment tussen

ict en business'. Gesteld kan worden dat deze benadering meer oog heeft voor de effectiviteit van ict. Alertheid bij het gebruik van het begrip IT-Governance is dus geboden.

Tactisch

ISO 20000. De nieuwe norm NEN-ISO-IEC 20000 (voorheen BS 15000) biedt de ict-servicemanager en uitvoerenden in de ict onder meer een richtlijn om de kwaliteit van de it-servicemanagementprocessen te beoordelen en verbeteren. Met behulp van deze norm kan de organisatie aantonen dat de servicemanagementprocessen goed zijn georganiseerd.

NEN-ISO/IEC 17799. De NEN-ISO/IEC 17799:2005 normen, of wel deel 1 van de BS7799 information technology - security techniques – beter bekend als de Code of practice for information security management. Deze norm houdt zich bezig met informatiebeveiliging in de breedste zin van het woord en levert best practices, richtlijnen en algemene principes voor invoering, onderhoud en management van informatiebeveiliging.

Operationeel

ITIL. Itil staat voor Information Technology Infrastructure Library en is ontwikkeld als een referentiekader voor het inrichten van de processen van een ict-organisatie. Het primaire doel is de kwaliteit van de dienstverlening (servicemanagement) te structureren en te verbeteren. Servicemanagement bestaat uit de sets *service delivery* en *service support*, ofwel het leveren van diensten en het ondersteunen van diensten. Uitgangspunt is dat bij het leveren van diensten afspraken (leveringsvoorwaarden) worden gemaakt over: de kosten, de beschikbaarheid, de benodigde capaciteit, de eventuele continuïteitsplannen en de beveiliging. Deze afspraken worden ondersteund door het afhandelen van klachten en vragen door de servicedesk, het herstellen en voorkomen van verstoringen, het beheren van wijzigingen, het distribueren van hard- en software bij wijzigingen en het inventariseren van alle middelen. Deze afspraken worden veelal vastgelegd in een Service Level Agreement (SLA) en worden in de praktijk beheerd door de servicelevelmanager.

NEN-ISO/IEC 27001. NEN-ISO/IEC 27001, deel 2 BS7799. De eerste norm in de nieuwe ISO/IEC serie 27000, die over het beheer ofwel het managementproces van informatiebeveiliging gaat. ISO/IEC 27001 is gebaseerd op BS7799-2 en is bedoeld voor het vaststellen, implementeren, onderhouden, controleren, beoordelen, onderhouden en verbeteren van een 'Information Security Management System (ISMS)'.
11

