

IT GOVERNANCE IN DE DAGELIJKSE PRAKTIJK

Volgens onderzoeksresultaten gepubliceerd in 2006* blijkt dat bijna de helft van de managers niet weet niet wat compliance en IT Governance is, dat ict-ers minder kennis van de begrippen hebben dan andere managers en dat men bij de overheid minder weet van compliance en IT Governance dan in het bedrijfsleven. In dit artikel worden de ontwikkelingen op het gebied van IT Governance geschetst en worden kaders gegeven voor een toepassing in de praktijk.

door: drs. K. Muijs-de Graaf

De meeste codes voor corporate governance schrijven expliciet voor dat ondernemingen hun risicomanagement op orde moeten hebben. Ook de Nederlandse corporate governance code volgt deze lijn. Belanghebbenden willen vandaag de dag meer en beter geïnformeerd worden over de risico's die een organisatie loopt. Dus ook over de ict-risico's.

Veel organisaties dienen te voldoen vanwege de overheid, de brancheorganisatie, hun beursnotering, of specifieke controlerende instanties aan bepaalde governance codes. Zo moeten Amerikaanse beursgenoteerde ondernemingen voldoen aan de Sarbanes Oxley act en Nederlandse beursgenoteerde ondernemingen aan de Code Tabaksblad. De Nederlandse code wordt gezien als een voorbeeld van 'goed ondernemerschap', waardoor deze code ook wordt nageleefd door ondernemingen zonder beursnotering. Immers, belangrijke onderdelen uit de governance codes, zoals die welke betrekking hebben op

risicomanagement en interne beheersing, zijn voor alle organisaties van belang. Een adequate interne beheersing moet waarborgen dat processen effectief en efficiënt verlopen, dat informatie betrouwbaar is en dat wet- en regelgeving wordt nageleefd.

De (inter)nationale wet- en regelgeving op ict-terrein wordt steeds stringenter. Dit is begrijpelijk, omdat de economische en maatschappelijke gevolgen van het disfunctioneren van de ict voor de organisatie en de betrokkenen (toeleveranciers, klanten, werknemers) toenemen. De archiefwet, eisen vanuit het Burgerlijk Wetboek, Wetboek van Koophandel, Wet elektronische handtekeningen, Wet bescherming persoonsgegevens, eisen vanuit de International Financial Reporting Standards (IFRS), Sarbanes Oxley act, Basel II, het is allemaal wet- en regelgeving die een (in)direct verband hebben met de ict in een organisatie.

Het is de verantwoordelijkheid van de directie om te voldoen aan de wet- en regelgeving. Dus ook waar het gaat om het managen van de ict-risico's en het 'in control' zijn van de gehele ict-voorziening. Het naleven van wet- en regelgeving op ict-gebied alsmede het managen van ict-risico's is veelal belegd bij de ict-manager. Hiervoor kan de ict-manager gebruik maken van de vele normenkaders en best practises.

Normenkaders

Er zijn vele best practice normenkaders om invulling te geven aan IT Governance. Deze normenkaders zijn deels overlapend en deels onderscheidend ten opzichte van elkaar, omdat elk model vanuit een

bepaald perspectief de ict benadert, dan wel heel concreet op ict-onderwerpen ingaat. Overeenkomst is dat deze modellen uitgaan van transparantie en dus controleerbaar zijn. Aangezien het onmogelijk is om in dit artikel alle normenkaders uitvoerig te behandelen, is er voor gekozen om het bekende Amerikaanse COBIT-model en de nieuwe ISO 27001 norm te behandelen.



Het is de verantwoordelijkheid van de directie om te voldoen aan de wet- en regelgeving. Dus ook waar het gaat om het managen van de ict-risico's en het 'in control' zijn van de gehele ict-voorziening. Het naleven van wet- en regelgeving op ict-gebied alsmede het managen van ict-risico's is veelal belegd bij de ict-manager. Hiervoor kan de ict-manager gebruik maken van de vele normenkaders en best practises.

De Amerikaanse Governance code verwijst naar het COBIT-model. De Nederlandse code Tabaksblad verwijst niet specifiek naar een raamwerk. Organisaties die hieraan willen voldoen zijn dus vrij in de keuze van een model of raamwerk. De nieuwe ISO 27001 is in oktober van 2006 uitgeroepen tot internationale norm. De werkwijze is vergelijkbaar met andere ISO normeringen, zoals ISO 9001, waarmee vele organisaties al ervaring hebben. Daarom is dit model ook heel goed toepasbaar voor Nederlandse organisaties.

COBIT-model. Het COBIT-model (Control Objectives for Information and Related Technology) is ontwikkeld door de Information Systems Audit and Control

Foundation (ISACF), het onderzoeksinstituut van de Information Systems Audit and Control Association (ISACA). COBIT consolideert en harmoniseert 41 wereldwijde ict-standaarden in een integraal model. Het model kan gebruikt worden door management, adviseurs, auditors en andere ict- en business professionals, die zich bezighouden met ict-gerelateerde beheersingsvraagstukken van organisaties. COBIT is gebaseerd op de gedachte dat de ict-resources moeten worden beheerst en beheerd op basis van een set van op een natuurlijke wijze gegroepeerde processen. Hierdoor krijgt een organisatie de beschikking over meetbare en betrouwbare informatie voor het realiseren van haar doelstellingen en de ondersteunende ict-dienstverlening. Het doel van COBIT is om het management en de proceseigenaren middels een IT Governance model te ondersteunen bij het begrijpen en beheersen van ict-gerelateerde risico's.

ISO 27001. De ISO 27001 norm is de formele norm van de Britse norm BS7799-2 die in Nederland bekend stond als de Code voor Informatiebeveiliging. De norm omvat eisen aan het managementsysteem voor informatiebeveiliging (hoofdstukken 4 tot en met 8). De Annex A van de norm bevat 133 maatregelen voor informatiebeveiliging, verdeeld in 11 categorieën met daarin 39 beheersdoelstellingen. Uitgangspunt van de ISO 27001 norm is dat het managementsysteem is ingericht volgens de welbekende plan-do-check-act cyclus. Het doel van ISO 27001 is een continu proces van verbetering op het gebied van informa-



HET SPEELVELD IT GOVERNANCE

Het begrip IT Governance wint aan belang vanwege strengere eisen van toezichhouders, klanten, leveranciers en de behoefte aan transparantie in organisaties. IT is vandaag de dag niet meer weg te denken bij de meeste organisaties en vormt dan ook een belangrijk aandachtspunt van de directie voor de realisatie van de ondernemingsstrategie. Immers het waarborgen van de continuïteit van de organisatie en de bedrijfsvoering, alsmede het waarborgen van de betrouwbaarheid van de informatievoorziening (besturen) is een directe verantwoordelijkheid van de directie. Maar ook kwaliteitsaspecten als beschikbaarheid, veiligheid, effectiviteit, efficiency en beheersbaarheid zijn van essentieel belang voor de directie om aandacht aan te geven.

De strategische it-visie en het it-beleid van de directie dient veelal vertaald te worden door het it-management naar tactische en operationele activiteiten (uitvoeren). Ook bij it-outsourcing dienen er goede afspraken gemaakt te worden over de uit te voeren werkzaamheden en de wijze waarop. Er worden afspraken gemaakt middels SLA's en over de prestaties wordt gerapporteerd met behulp van service level rapportages (verantwoording). Aan de hand van de uitkomsten van de service level rapportages kunnen de ict-managers actie ondernemen (besturen) om er voor te zorgen dat de it-doelstellingen kunnen worden gerealiseerd en daarmee bijdragen aan het realiseren van de organisatiedoelstellingen. Vervolgens kan de directie aan de hand van de service level rapportages, maar ook aan de hand van de uitkomsten van audits, verantwoording afleggen over de it-bedrijfsvoering aan belanghebbenden (verantwoorden).

Samengevat is IT Governance: Het besturen, beheersen, uitvoeren en verantwoording afleggen over en het toezicht op de it binnen een organisatie.

tiebeveiliging te implementeren. ISO 27001 voorziet in een standaard raamwerk dat organisaties de mogelijkheid biedt om effectieve beheersingsmaatregelen te ontwikkelen, te implementeren en prestaties te meten. Het voorziet in een gestructureerde risicomangement aanpak die de organisatie helpt met het ontwikkelen en implementeren van een information security management system (ISMS). Het resultaat is een adequaat stelsel van beheersmaatregelen dat waarborgen biedt voor de integriteit, beschikbaarheid en vertrouwelijkheid van gegevens en gegevensverwerking.

Implementatieplan

De impact van het implementeren van een adequate IT Governance structuur is afhankelijk van onder andere de omvang van de organisatie, de complexiteit en afhankelijkheid van de ict-systemen, de gevoeligheid/veiligheid van kritische gegevens, en van de van toepassing zijnde wet- en regelgeving. Ongeacht de impact kan elke organisatie de volgende stappen doorlopen om IT Governance te implementeren:

1. Bewustwording
2. Kiezen model
3. Uitvoeren nulmeting
4. Implementatie
5. Opstellen SLA vanuit IT Governance perspectief
6. Verkrijgen certificering

Bewustwording. Uit tal van onderzoeken blijkt dat veel organisaties nog niet beschikken over een IT-Governance raamwerk. Veelal kunnen verantwoordelijken nauwelijks uitleggen wat het begrip IT-Governance inhoudt, laat staan de vertaling maken naar de impact op hun eigen organisatie en hun eigen verantwoordelijkheid daarin. In eerste instantie zijn de bestuurders van een organisatie primair verantwoordelijk voor de kwaliteit van de ict en kunnen zij zelfs persoonlijk aansprakelijk worden gesteld als er sprake is van onbehoorlijk bestuur. Verder kunnen de toezichhouders waaronder de Raad van Commissarissen dan wel een speciale auditcommissie beoordelen hoe het MT verantwoording draagt voor computersystemen en -applicaties, de beveiliging en noodprocedures en hoe de betrouwbaarheid en continuïteit van de systemen zijn gewaarborgd. Het ict-management is veelal verantwoordelijk voor de implementatie van de diverse maatregelen. Om als ict-manager toegevoegde waarde aan de onderneming te leveren is het zeker belangrijk dat deze afweert van de ins en outs van IT Governance en zo een positie weet te verwerven bij de bestuurders van een organisatie. Om bewustwording te stimuleren is het belangrijk dat directieleden, toezichhouders, klanten en ict-managers met elkaar in overleg treden over de noodzaak en de consequenties van het (niet) op orde hebben van een adequate ict-voorziening.

Kiezen model. Zoals eerder toegelicht

zijn er meerdere IT Governance raamwerken. Het is belangrijk dat de organisatie een weloverwogen besluit neemt voor het model dat geïmplementeerd gaat worden. Belangrijke criteria bij de keuze zijn onder meer de van toepassing zijnde wet- en regelgeving, de eisen van belanghebbenden (zoals leveranciers en klanten) en de eisen die organisatie stelt aan IT Governance.

Uitvoering nulmeting. Om te weten hoe de organisatie er voor staat op het gebied van IT Governance dient een nulmeting uitgevoerd te worden aan de hand van het gekozen model. Dan pas kan worden vastgesteld welke zaken nog ingeregeld kunnen en moeten worden. De te implementeren maatregelen zullen bedrijfseconomische vraagstukken met zich mee brengen. Het spreekt voor zich dat organisaties met complexe ict-systemen en een grote afhankelijkheid van de werking van de ict mogelijk na de nulmeting tot de conclusie komen dat alle categorieën, doelstellingen en maatregelen van belang zijn voor hun bedrijfsvoering. Zo nodig kunnen additionele, niet in het betreffende model genoemde, beheersdoelstellingen en beveiligingsmaatregelen aan het stelsel worden toegevoegd. Andere organisaties met wellicht minder gevoelige gegevens kunnen alleen de relevante zaken uit het gekozen model kiezen die passen bij hun bedrijfsproces en beveiligingsbehoeften.

Implementatie. De implementatie van de tekortkomingen kan het beste pro-

jectmatig worden uitgevoerd. Deze activiteiten zullen redelijk wat tijd in beslag nemen van het management en de betrokken medewerkers en veelal ook investeringen c.q. kosten met zich mee brengen.

Opstellen SLA vanuit IT Governance perspectief. Afspraken die met elkaar gemaakt worden vanuit IT Governance kunnen het beste worden vastgelegd in Service Levels Agreements. Rapportage kan plaatsvinden aan de hand van een Service Level Rapport (verantwoording). Dit rapport is voor de ontvanger de input om gepaste maatregelen te nemen (besturen), dan wel te weten dat de organisatie in control is op ict-gebied (beheersen).

Verkrijgen certificering. Na invoering van IT Governance kan de organisatie een eigen beoordeling uitvoeren om zich er van te verzekeren dat de fysieke, logische en organisatorische maatregelen adequaat functioneren middels een interne audit. Een andere stap is het laten certificeren van het systeem door een externe partij. Ook bij outsourcing kan een certificaat worden aangevraagd, waarmee de derde partij kan aantonen dat er toe-reikende maatregelen zijn getroffen die waarborgen dat de ict-voorziening in control is.

Certificatie brengt additionele kosten met zich mee. Veelal wordt dit terugverdiend door meer doelmatigheid. Daarnaast voorkomt de organisatie dat klanten telkens auditors langs sturen om de kwaliteit van

de ict-organisatie te beoordelen. Met een certificering versterkt de organisatie het vertrouwen tussen handelspartners, toezichhouders, accountants en niet te vergeten de klanten.

Opgemerkt dient te worden dat er vele soorten certificeringen zijn met verschillende reikwijdtes, geldigheid, kostprijzen en mate van zekerheid.

Certificaten

Veel voorkomende certificeringen zijn de Third Party memoranda. Sinds kort kunnen bedrijven/organisaties zich ook laten certificeren volgens ISO 27001.

Een Third Party Memorandum of derden mededeling betreft een uitspraak over een nader vast te stellen scope en normenkader. Dit houdt in dat afhankelijk van de doelgroep een scope wordt vastgesteld die bestaat uit het te onderzoeken 'object', het te hanteren normenkader gebaseerd op één of meerdere kwaliteitsaspecten als integriteit, vertrouwelijkheid, continuïteit en beschikbaarheid en de reikwijdte (opzet, bestaan, werking). Het rapport wordt veelal voor één jaar afgegeven en betreft een uitspraak over het afgelopen jaar.

Met het ISO 27001 certificaat kan een organisatie laten zien dat het interne stelsel van beheersmaatregelen onder meer voldoet aan:

1. Eisen op het gebied van Corporate Governance en Business Continuity.

2. Eisen op het gebied van wet- en regelgeving.
3. Eisen op het gebied van contractuele afspraken met klanten.
4. De aanwezigheid van een adequaat risicomangementproces dat voorziet in het identificeren en beheersen van risico's en het formaliseren van informatiebeveiligingsprocessen, procedures en documentatie.
5. De eis dat het management zich heeft geëngaat aan informatiebeveiliging.

Het certificaat wordt afgegeven voor een periode van drie jaar. Voordeel is dat er getoetst wordt aan een standaard normenkader en dat de aanpak overeenkomt met de ISO 9001, waar vele organisaties reeds ervaring mee hebben. Afhankelijk van de beoogde doelstelling van de certificering en de eisen van belanghebbende kan het type certificaat worden vastgesteld dat benodigd is.

Mevr. drs. K. Muijs-de Graaf RARO is internal auditor bij Kender-Thijssen Solutions BV te Veenendaal en betrokken bij de ontwikkeling van het in portfolio nemen van IT Governance diensten. Tevens is zij o.a. verbonden aan de Hogeschool Arnhem & Nijmegen (Bedrijfskundige Informatica) en bij de Voortgezette Educatie voor Registeraccountants als gastdocent IT Governance.

*Het onderzoek is uitgevoerd door Marqit.