Benchmarking op basis van standaarden als CobIT en Code voor Informatiebeveiliging

Drs. J.C. de Boer RE en ir. K.M. Lof RE

Managers en auditors worden in toenemende mate geconfronteerd met de beheersing van ICT binnen organisaties. De IT Risk Management Benchmarking-methode verschaft u het benodigde inzicht in de beheersing van ICT in uw organisatie. Het is hierbij mogelijk volgens internationaal geaccepteerde standaarden, zoals CobIT en ISO 17799, te rapporteren.

Inleiding

Enige jaren geleden hebben we in Compact de mogelijkheid om benchmarking te gebruiken bij het beoordelen van de General IT Controls ([Somm97]) uiteengezet. Mede door het opkomen van ICT-governance, de strengere regelgeving en de daarmee samenhangende ontwikkeling dat stakeholders meer grip willen hebben op ICT, is het gebruik van dit hulpmiddel de afgelopen jaren sterk toegenomen. IT Risk Management Benchmarking wordt niet alleen ingezet in het kader van jaarrekeningcontroles en quick scans op de ICT-organisatie, maar ook bij uitgebreide doorlichtingen van ICT-organisaties die in opdracht van het management en de toezichthouders worden uitgevoerd.

Een andere ontwikkeling is dat een framework als CobIT en de maatregelen zoals deze zijn weergegeven in de Code voor Informatiebeveiliging (BS7799 en ISO 17799), steeds vaker door organisaties worden geaccepteerd en geadopteerd als standaard.

De toenemende vraag die wij wereldwijd in onze praktijk zien naar benchmarks, het inzichtelijk willen hebben van ICT-risico's en de acceptatie van diverse standaarden zijn de aanleiding geweest om het KPMG-product IT Risk Management Benchmarking uit te breiden. Het resultaat hiervan is een verbeterde en geactualiseerde vragenlijst, aanvullende rapportagemogelijkheden en mogelijkheden om het product als self-control assessment in te zetten in grotere of sterk gedecentraliseerde organisaties. Met dit product worden organisaties in staat gesteld ICT-processen, bijbehorende risico's en beheersingsmaatregelen in kaart te brengen en te toetsen met vergelijkbare organisaties en aan breed geaccepteerde standaarden zoals CobIT en de Code voor Informatiebeveiliging. De informatie uit de vergelijking stelt organisaties in staat de beheersingsmaatregelen rond de ICT-toepassingen te verbeteren en tot een kosteneffectieve balans te komen tussen risico's en beheersingsmaatregelen.

Drs. J.C. de Boer RE
is als senior manager werkzaam bij KPMG Information Risk Management. Hij heeft ervaring opgedaan met een breed scala van audit- en adviesopdrachten op het gebied van ICT. De opdrachten die hij uitvoert zijn onder andere IT benchmarking-opdrachten, doorlichtingen van en quality assurance op automatiseringsprojecten en -organisaties, het professionaliseren van ICT-organisaties/afdelingen en het outsourcen van de ICT-auditfunctie. Tevens is hij wereldwijd verantwoordelijk voor IT Risk Management Benchmarking.

deboer.janjc@kpmg.nl

Ir. K.M. Lof RE
is als senior manager werkzaam bij KPMG Information Risk Management. Belangrijke aandachtsgebieden in zijn werk zijn het inrichten en evalueren van ICT Governance-structuren en -processen, het onderzoeken van de kwaliteit van ICT-organisaties, het uitvoeren van periodieke projectreviews en het begeleiden van organisaties bij het verder professionaliseren van de informatievoorziening. Hij heeft een belangrijke bijdrage geleverd aan de recente uitbreiding van het internationale KPMG-product IT Risk Management Benchmarking.

lof.mark@kpmg.nl

Inmiddels is een groot aantal benchmarkingonderzoeken uitgevoerd. Zo beschikt KPMG momenteel over een internationale database met ongeveer 1900 organisaties. Deze gegevens zijn afkomstig uit 29 verschillende landen, waardoor zowel nationale als internationale vergelijking mogelijk is.

In dit artikel wordt ingegaan op de recente ontwikkelingen ten aanzien van IT Risk Management Benchmarking (ITRMB).

Aanpak ITRMB-onderzoek

Het benchmarkingonderzoek bestaat uit het systematisch verzamelen van gegevens over de ICT-risico's en de getroffen beheersingsmaatregelen. Om te komen tot een zinvolle vergelijking van organisaties is in de benchmarkingmethode een driedeling aangebracht. Afhankelijk van de diepgang van het onderzoek beoordelen wij de betreffende organisatie op de volgende aspecten:

- ICT-risico's: wat is het risicoprofiel van de informatievoorziening binnen de organisatie die wordt onderzocht?
- ICT-controls: welke beheersingsmaatregelen zijn door de organisatie getroffen om de risico's te beheersen ten aanzien van de ICT-processen?
- effectiviteit van beheersingsmaatregelen: hoe effectief zijn de getroffen maatregelen? Loopt de organisatie in de huidige situatie een onverantwoord groot risico, of investeert zij wellicht te veel in bepaalde maatregelen?

ICT-risico's

Het eerste deel van een onderzoek bestaat uit een inventarisatie van de inherente ICT-risico's. Op een schaal van 1 tot 5 wordt een risico-inschatting gemaakt van de situatie waarin de organisatie zich bevindt (laag, gemiddeld, aanzienlijk, hoog, extreem hoog). Bij het vaststellen van het risicoprofiel worden de volgende acht aandachtsgebieden onderkend:

Business Focus
De organisatie en haar bedrijfsprocessen worden ondersteund door ICT-toepassingen. Er is een risico dat de wensen en eisen ten aanzien van informatievoorziening niet gerealiseerd worden of dat ICT niet op een passende manier is geïntegreerd in de organisatie, de organisatiestrategie en haar toekomstige plannen. Verliezen kunnen onder andere ontstaan door inefficiënte toepassing van ICT-systemen, inadequaat management van ICT-risico's en het investeren in ICT-toepassingen die de bedrijfsstrategie en -plannen niet ondersteunen.

Information Assets
De informatie (information assets) die een organisatie bezit, kan resulteren in verliezen. Dergelijk verlies kan zijn: direct financieel (fraude, diefstal) of indirect financieel (bijvoorbeeld imagoschade of verlies van bedrijfsgevoelige informatie of intellectuele eigendommen).

Dependence on IT
Dit risico beschrijft de impact van verlies (van delen) van de ICT-infrastructuur. Hoe meer de organisatie afhankelijk is van ICT-systemen, des te groter is het potentiële verlies (financieel of reputatie). Het verlies kan het resultaat zijn van: het niet kunnen uitvoeren van bedrijfsprocessen tot het systeem is hersteld, elektronische beheersingsmaatregelen die niet langer efficiënt zijn en ontevreden gebruikers die deadlines niet hebben gehaald.

Dependence on Internal IT Staff
Dit is het risico dat de aard en de mate van afhankelijkheid van intern ICT-personeel kan leiden tot verliezen. Deze kunnen het gevolg zijn van verlies van specifieke kennis of expertise van individuen of van extra kosten om kennis op te bouwen.

Dependence on 3rd parties
Het risico bestaat dat de organisatie verliezen leidt als gevolg van afhankelijkheid van derde partijen als outsourcers/co-sourcers, leveranciers, contractanten en consultants. Verliezen kunnen het resultaat zijn van verlies of reductie van belangrijke expertise, gebrek aan begrip van de bedrijfsprocessen door derden en excessieve kosten in vergelijking met de mogelijkheid tot een eigen ICT-afdeling.

Reliability of IT systems
Het risico bestaat dat gebrek aan betrouwbaarheid leidt tot verliezen. Deze kunnen voortkomen uit inconsistente of inaccurate verwerking van gegevens, benodigde herstelwerkzaamheden voor verwerkingsproblemen of het gebruik van inefficiënte processen, of schaduwadministraties, veroorzaakt door een gebrek aan vertrouwen in ICT-systemen.

Changes to IT
Het risico bestaat dat verliezen ontstaan door de mate van verandering in de ICT-omgeving. Zij kunnen worden veroorzaakt door inefficiënte projecten die niet voldoen aan de bedrijfsbehoeften, fouten en verlies aan betrouwbaarheid in applicaties door continu onderhoud en kleine veranderingen, of doordat de impact van veranderingen niet volledig wordt begrepen.

Legislative & regulatory environment
Het risico bestaat dat het niet voldoen aan wet- en regelgeving ten aanzien van verwerking, opslag en gebruik van informatie leidt tot imago- en financiële schade. Voorbeelden van regulering waaraan dient te worden voldaan, zijn de Wet bescherming persoonsgegevens, de Wet computercriminaliteit, de Sarbanes-Oxley Act 2002 en de International Financial Reporting Standards.

Het resultaat van de risico-inschatting wordt grafisch weergegeven (zie figuur 1). De zwarte lijn in de grafiek geeft het inherente risico weer van de organisatie voordat rekening gehouden is met de ingerichte beheersingsmaatregelen. De verschillende kwartielen geven de verdeling weer van het risicoprofiel van de organisaties waarmee vergeleken is. In dit voorbeeld heeft de organisatie een lager risico voor het aandachtsgebied *Dependence on IT Internal Staff* dan de gehele populatie waarmee vergeleken is. Voor het aandachtsgebied *Business Focus* heeft driekwart van de populatie een hoger risicoprofiel.

Praktijkvoorbeeld 1
De kracht van productieorganisatie X is dat zij innovatief is in het produceren van nieuwe kunststoffen. De recepturen van deze producten en de productiewijze zijn vastgelegd in het centrale ERP-systeem. De waarde van deze informatie is van strategisch belang voor deze organisatie. Indien de gegevens over recepturen bekend worden bij concurrenten heeft dat direct effect op het concurrentievoordeel. De risico-inschatting voor het onderdeel *Information Assets* is derhalve hoog.

Deze productieorganisatie heeft een standaard-ERP-systeem in gebruik binnen een relatief eenvoudige netwerkomgeving. Er is geen grote afhankelijkheid van interne ICT-medewerkers doordat kennis van het ERP-systeem en de netwerkomgeving ruimschoots buiten de eigen organisatie voorhanden is. Risico-inschatting voor het aandachtsgebied *Dependence on IT Internal Staff* is daarom laag.

ICT-beheersingsmaatregelen

Het tweede deel van het onderzoek heeft betrekking op het vaststellen van de mate waarin er beheersingsmaatregelen zijn genomen. Op een schaal van 1 tot 5 wordt een inschatting gemaakt op welk niveau de organisatie zich bevindt waar het gaat om het nemen van maatregelen.
De achterliggende gedachte van de scores 1 tot en met 5 is:

1. De organisatie heeft geen maatregelen getroffen.
2. De organisatie heeft informele maatregelen getroffen.
3. De organisatie heeft formele maatregelen getroffen.
4. De organisatie beheerst de maatregelen en stuurt.
5. Er is een evaluatiecyclus om de maatregelen bij en af te stellen op de wensen uit de organisatie (proactief).

De inventarisatie van de beheersingsmaatregelen wordt gegroepeerd rondom de volgende zes aandachtsgebieden:

Management of IT
Dit aandachtsgebied betreft de beheersingsmaatregelen rondom de ICT-managementvraagstukken, zoals managementbetrokkenheid, informatieplanning, aansturing en inrichting ICT-organisatie, naleving wet- en regelgeving, leveranciersmanagement, rapportage over kwaliteit van dienstverlening en ICT-kostenbeheersing.

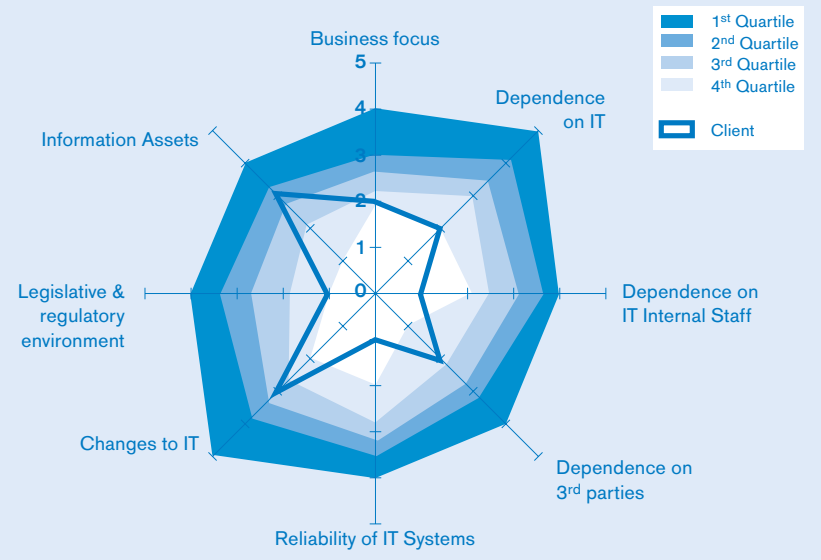
Project and Change Management
Het aandachtsgebied Project and Change Management bevat de beheersingsmaatregelen gericht op het waarborgen dat de veranderingen in de ICT-omgeving beheerst en succesvol zijn. Hierbij kan worden gedacht aan: projectmanagement en systeemontwikkelmethoden en -technieken, organisatorisch verandermanagement, gebruikersbetrokkenheid en documentatie.

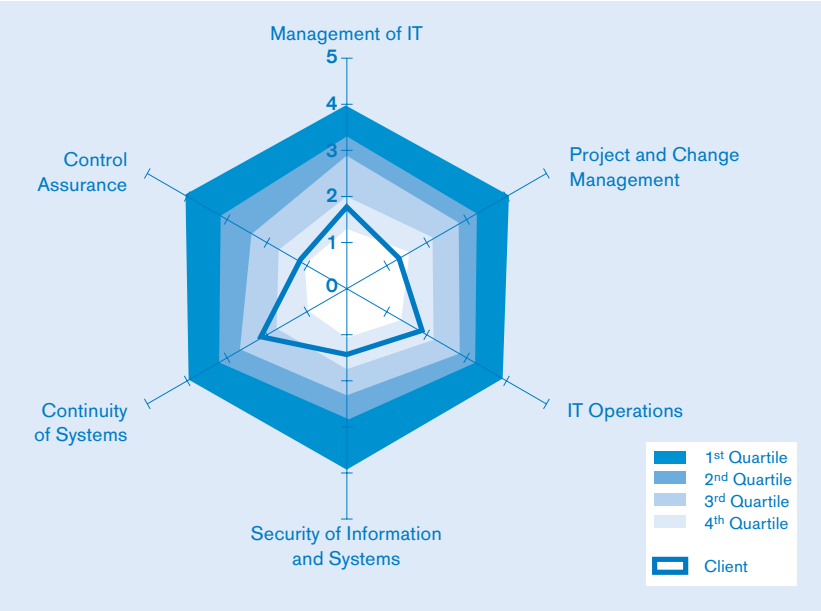
IT Operations
IT Operations is het aandachtsgebied dat betrekking heeft op de beheersingsmaatregelen voor het waarborgen dat de dagelijkse ICT-beheeractiviteiten adequaat worden uitgevoerd. Denk hierbij aan: incidentenbeheer, configuratiebeheer, service level management, capaciteitsbeheer.

Security of Information and Systems
Security of Information and Systems betreft het aandachtsgebied met beheersingsmaatregelen voor het waarborgen van de beveiliging van de informatiesystemen. Onderdelen zijn beveiligingsbeleid, beveiligingsfunctie, logische toegangsbeveiliging en beveiliging van externe toegang.

Continuity of Systems
Het aandachtsgebied Continuity of Systems bevat de beheersingsmaatregelen voor het waarborgen van de beschikbaarheid van de systemen. Onderdelen zijn: back-up en recovery, fysieke beveiliging, voorzieningen in de computerruimte en contingency planning.

Figuur 1. Inherent risicoprofiel van een organisatie.





Figuur 2. Samenvattend overzicht van beheersingsmaatregelen.

Control Assurance

Het aandachtsgebied Control Assurance betreft de beheersingsmaatregelen voor het waarborgen dat voldaan wordt aan de binnen de organisatie gestelde richtlijnen en standaarden, en maatregelen voor het adequaat beheersen van de aan ICT gerelateerde risico's. Onderdelen zijn project en quality assurance, audit of IT en risk management.

De inventarisatie van de beheersingsmaatregelen wordt grafisch weergegeven (zie de figuren 2 en 3) in zogenaamde spinnenwebgrafieken. De grafiek geeft de mate van volwassenheid van de beheersingsmaatregelen weer. Hierbij wordt een vergelijking gemaakt met het volwassenheidsniveau van de onderzochte populatie.

Praktijkvoorbeeld 2

Productieorganisatie Y is gestart met het professionaliseren van de ICT-beheerorganisatie. De aandacht is hierbij in eerste instantie gericht geweest op het beheersen van de externe relaties. Hiertoe zijn in een jaar tijd voor alle externe ICT-dienstverleners de contracten geëvalueerd en opnieuw vastgesteld. Belangrijke verbetering in de contracten is een periodieke evaluatie van de dienstverlening. De afdeling Inkoop is betrokken bij het leveranciersmanagement. De organisatie krijgt voor het onderdeel *Manage Third Party Services* een score 3 (zie figuur 3). Het beheren van de externe relaties is geformaliseerd en wordt consistent toegepast voor alle ICT-leveranciers.

De *Incident en Problem Management*-processen zijn op dit moment nog informeel ingericht. Er is geen heldere en eenduidige procedure voor het melden van incidenten. De gebruikers moeten voor verschillende systemen contact opnemen met verschillende medewerkers. Lang niet alle gemelde problemen worden geregistreerd. Het *Problem Management*-proces maakt nog maar beperkt gebruik van de mogelijkheden uit het configuratiebeheertool. De organisatie krijgt voor het onderdeel *Incident en Problem Management* een score 2.

Effectiviteit van beheersingsmaatregelen

De effectiviteit van de beheersingsmaatregelen kan worden vastgesteld door te evalueren of de geïnventariseerde inherente risico's voldoende worden beheerst door de ingerichte beheersingsmaatregelen. De ICT-beheersingsmaatregelen kunnen één of meer ICT-risico's beheersen. Het resultaat van deze evaluatie, het restrisico, wordt weergegeven met behulp van (de kleuren van) een verkeerslicht.

De evaluatie maakt direct inzichtelijk of de getroffen maatregelen toereikend zijn, en hoe hoog het restrisico is. De context van de auditomgeving wordt op deze wijze bewust meegenomen in de beoordeling van de kwaliteit van de beheersing. Een hoge score qua beheersingsmaatregelen zegt op zichzelf niet alles. Een score 3, 'de organisatie heeft formele maatregelen getroffen', voor de beheersingsmaatregelen kan in de situatie met een laag risicoprofiel meer dan toereikend zijn; in een situatie met een hoog risicoprofiel kan een score 3 niet voldoende zijn.

Figuur 4 laat zien dat het hoge risicoprofiel voor het aandachtsgebied *Changes to IT* hogere eisen stelt aan de huidige beheersingsmaatregelen voor *Project and Change Management*.

Deze evaluatie van de ingerichte beheersingsmaatregelen versus de inherente risico's geeft belangrijke aanknopingspunten voor het management en de auditor welke punten te verbeteren. Door een risicoanalyse uit te voeren en deze vervolgens grafisch af te zetten tegen de uitkomsten van de evaluatie van de beheersingsprocessen wordt een meerwaarde bereikt ten aanzien van gangbare standaarden als CobIT en ISO 17799.

Rapportagemogelijkheden op basis van standaarden

CobIT

De door KPMG gehanteerde beheersingsmaatregelen binnen IT Risk Management Benchmarking sluiten aan bij de beheersingsmaatregelen binnen CobIT (Control Objectives for Information and related Technology). CobIT is een niet-technisch, internationaal bekend referentiekader voor ICT-gerelateerde beheersingsprocessen. Het CobIT-framework is een raamwerk dat bestaat uit drie verschillende onderdelen:

- IT Processes;
- Information Criteria;
- IT Resources.

IT Processes

CobIT onderscheidt een aantal processen die de IT-resources beheren. Deze beheersingsprocessen zijn gegroepeerd in vier domeinen. De vier domeinen geven de managementcyclus van Plan-Do-Check-Act weer:

- *Planning & Organisation*. Dit domein bevat de strategische en tactische beheersingsprocessen gericht op aansturing van de informatievoorziening binnen de organisatie.
- *Acquisition & Implementation*. Dit domein bevat de beheersingsprocessen gericht op het beheerst ontwikkelen en implementeren van nieuwe systemen of systeemaanpassingen.
- *Delivery & Support*. Dit domein bevat de beheersingsprocessen gericht op het exploiteren en beheren van de in gebruik zijnde systemen en infrastructuren.
- *Monitoring*. Dit domein bevat de beheersingsprocessen gericht op het periodiek evalueren van de kwaliteit van de ICT-dienstverlening.

Information Criteria

De toepassingen en mogelijkheden van informatievoorziening worden ingezet om een bijdrage te leveren aan de organisatiedoelstellingen. Om na te kunnen gaan of deze bijdrage geleverd wordt, is er een aantal criteria gedefinieerd om de informatievoorziening te kunnen beoordelen. De volgende zeven criteria worden onderscheiden: effectiviteit, efficiëntie, integriteit, vertrouwelijkheid, beschikbaarheid, naleving standaarden en betrouwbaarheid.

IT Resources

IT-resources worden door beheerprocessen ingezet voor het leveren van een bijdrage aan de informatievoorziening binnen een organisatie. De volgende IT-resources worden onderkend: mensen, applicatiesystemen, technologie, faciliteiten en gegevens.

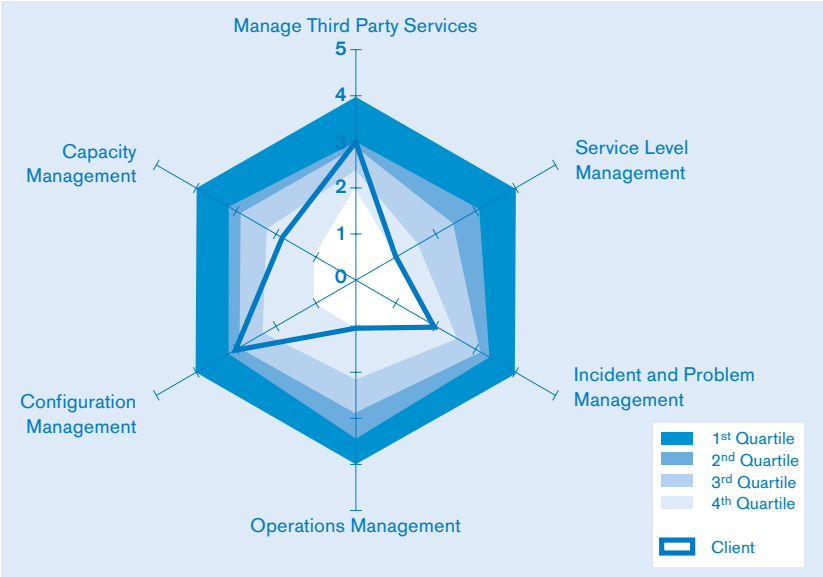
De nieuwste versie van het product IT Risk Management Benchmarking beschikt over mogelijkheden om volgens bovengenoemde indeling van ICT-processen te rapporteren. In de figuren 5 en 6 zijn enkele voorbeelden van de rapportages opgenomen.

In figuur 6 wordt een voorbeeld gegeven waarin het domein *Planning & Organisation* in detail is uitgewerkt. Ook hierbij worden de resultaten van de betreffende cliënt uitgezet tegen de benchmarkpopulatie in de database.

Code voor Informatiebeveiliging (ISO 17799)

In de praktijk zien wij een toenemende behoefte van organisaties om zich te conformeren aan de Code voor Informatiebeveiliging. De gehanteerde beheersingsmaatregelen binnen IT Risk Management Benchmarking sluiten aan op deze ontwikkeling. De nieuwste versie van het product IT Risk Management Benchmarking beschikt dan ook over mogelijkheden om volgens deze indeling van beheersingsmaatregelen te rapporteren. In figuur 7 is een voorbeeld van een rapportage opgenomen.

Deze rapportage laat een overzicht zien van de mate waarin een organisatie voldoet aan de beveiligingsstandaarden uit de Code voor Informatiebeveiliging. Zij is bedoeld om een overallbeeld te geven en niet geschikt voor een certificeringstraject.

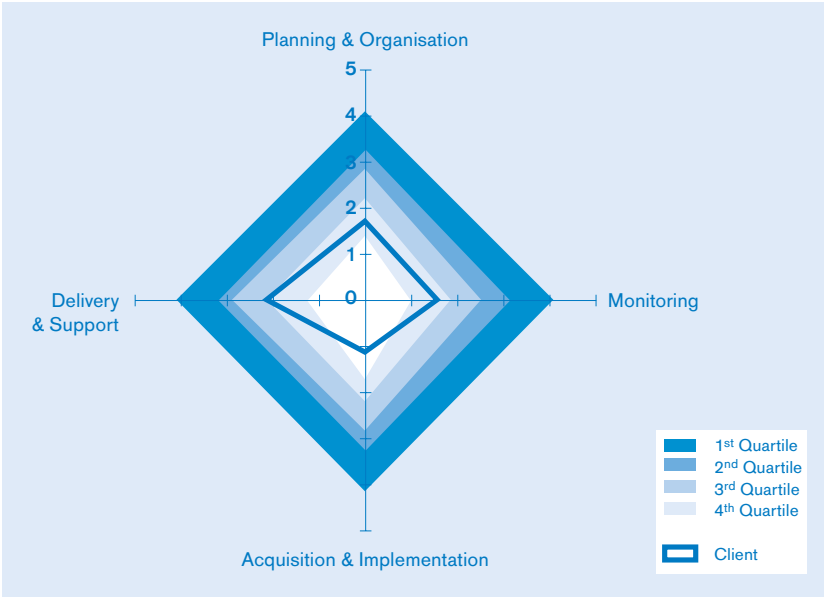


Figuur 3. Detailoverzicht van beheersingsmaatregelen voor het onderdeel IT Operations.

Figuur 4. Effectiviteit van beheersings-maatregelen.

Control Areas	Controls	Business focus	Information Assets	Dependence on IT	Dependence on IT Internal Staff	Dependence on 3rd parties	Reliability of IT Systems	Changes to IT	Legislative & regulatory environment	Controls Score
Management of IT	Board/Senior Management Involvement	●	○		●	●			●	2
	IT Strategy	●	○		●	●				2
	IT Cost and Investment Management	●	●		●	●			●	3
	Management Reporting of IT Performance	●	○		●	●				2
	Legal and Regulatory Compliance	○	●		●	○			●	1
	Manage Human Resources	●		●	●					2
Project and Change Management	Development Methodology	○					●	●		1
	Project Management	○			●		●	●		1
	User Participation	●			●		●	○		2
	End User Computing		○					○	●	2
	Documentation	●		●	●		●	○		2
	Business Change Process	○					●	●		1
	Technical Change Management	○			●		●	●		1
IT Operations	Manage Third Party Services	●	●			●				3
	Service Level Management	○	●			○				1
	Incident and Problem Management	●		●			●			2
	Operations Management	○		○			●			1
	Configuration Management			●			●	●		3
	Capacity Management	●		●			●			2
Security of Information and Systems	Security Policy		●						●	1
	Security Administration		○	●						2
	Logical Access Control Facilities		●		●					1
	External Communications		○			●				2
Continuity of Systems	Backup of Data and Systems		●	●			●		●	3
	Continuity Planning			○			●			1
	Physical Access Control		○	●			●			2
	Protection of the Environment		●	●			●			3
Control Assurance	Risk Management		●		●	○	●		●	1
	Audit of IT		○	●	●		●	○	●	2
	Quality and Project Assurance				●		●	●		1
	Assessment of Control Adequacy	○	●	○	●	○	●	●	●	1
Risks Score		2	3	2	1	2	1	3	1	

Figuur 5. Samenvattend overzicht van beheersings-maatregelen volgens CobIT.

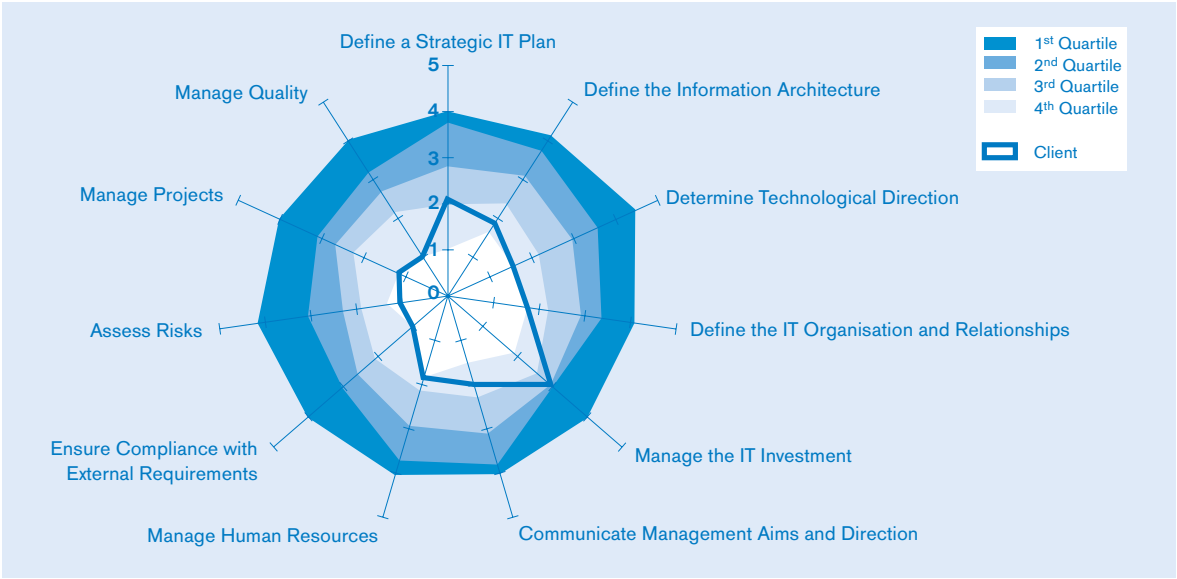


Toepassing

Het IT Risk Management Benchmarking-product bestaat uit een elektronische vragenlijst en een centrale database inclusief rapportgenerator. Om de kwaliteit van de gegevens te waarborgen zijn er verschillende beveiligings- en reviewfunctionaliteiten ingebouwd. Het product is ontwikkeld door gebruik te maken van het tool WebQubus.

Voor de auditors zijn er verschillende mogelijkheden het product te gebruiken. Zo zijn er een pc-applicatie en een webapplicatie. Met de pc-applicatie kunnen auditors die op locatie bij een cliënt werken, de vragenlijst off line invullen en verwerken. De webapplicatie biedt de medewerkers de mogelijkheid de vragenlijst direct vast te leggen in de centrale database.

Nadat de beantwoording van de vragenlijst door een KPMG-medewerker is vastgelegd in het WebQubus-tool,



Figuur 6. Detailoverzicht van beheersingsmaatregelen Planning & Organisation.

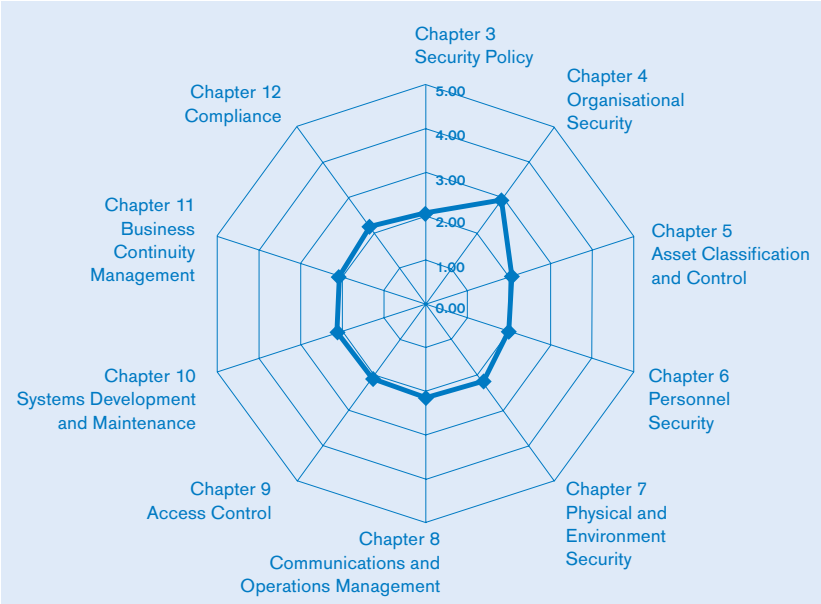
wordt de opdrachtmanager uitgenodigd de beantwoording te reviewen. Kwaliteitsbewaking van de ingevulde antwoorden is belangrijk opdat de database niet vervuild raakt met onjuiste antwoorden of onvolledige antwoordensets. De opdrachtmanager geeft na een beoordeling van de vastlegging van de antwoorden een akkoord. De vastgelegde antwoordenset wordt gevalideerd op volledigheid van een aantal onderwerpen en vastgelegd in de centrale database. De invuller en de opdrachtmanager worden automatisch op de hoogte gebracht van het resultaat van deze validatie.

Het is mogelijk een benchmarkrapport op te laten stellen nadat de validatie succesvol is verlopen. De medewerker geeft aan welke criteria (bijvoorbeeld branchecode of omvang ICT-organisatie) gehanteerd dienen te worden bij het selecteren van de populatie waarmee vergeleken wordt. Het aangevraagde rapport wordt binnen vijf minuten door de rapportgenerator via e-mail verstuurd.

Self-control assessment

De ontwikkelde structuur van een centrale database en een elektronische vragenlijst die via het web ingevuld kan worden, biedt vele mogelijkheden om gebruikt te worden bij self-control assessments of auditopdrachten binnen grotere organisaties.

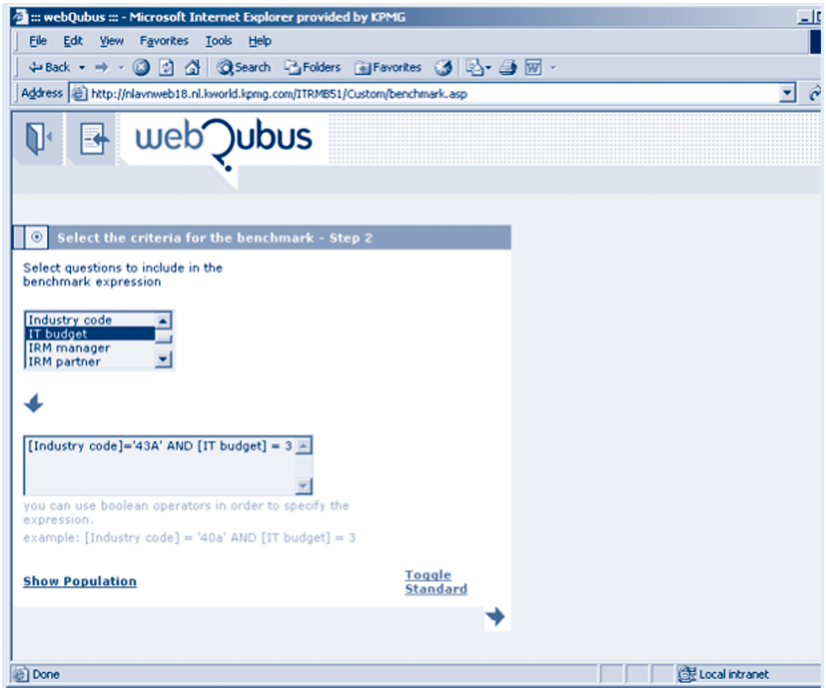
Figuur 7. Score beheersingsmaatregelen volgens ISO 17799.



Denk bijvoorbeeld aan een organisatie met een groot aantal organisatie-eenheden al dan niet verspreid over de gehele wereld. In toenemende mate wordt in dergelijke organisaties aan de verantwoordelijke directieleden van werkmaatschappijen gevraagd te verklaren dat zij voldoen aan de organisatiebrede richtlijnen. Deze verklaringen zijn ook wel bekend onder de term Letter of Representation. Verantwoording over de beheersing van de informatievoorziening en het voldoen aan de organisatiebrede ICT-richtlijnen is hierin vaak opgenomen.

De ontwikkelde tooling maakt het mogelijk dat het management van iedere organisatie-eenheid op een uniforme manier on line kan verklaren of de eenheid daadwerkelijk voldoet aan het verwachte niveau van beheersing van de informatievoorziening en de organisatiebrede richtlijnen. Het management beantwoordt de vragen uit het IT Risk Management Benchmarking-tool en wordt via de rapportage op de hoogte gebracht van de mate van compliance aan de organisatiebrede richtlijnen. De centrale en uniforme vastlegging van de verschillende beantwoordingen biedt voor bijvoorbeeld de interne accountantsdienst en eventuele andere controlerende instanties een uitstekend startpunt voor hun reviewwerkzaamheden. Tevens kan zij een kostenbesparing opleveren (bijvoorbeeld: reiskosten, kosten van uniformering van verzamelde gegevens en interpretatie van de resultaten, rapportagekosten).

Figuur 8. Het tool WebQubus.



Conclusie

In dit artikel is een overzicht gegeven van de mogelijkheid van benchmarking en rapportering op basis van algemeen aanvaarde standaarden. Een methodiek als IT Risk Management Benchmarking speelt in op de behoefte van organisaties om zich te spiegelen aan andere organisaties. Tevens sluit zij aan op algemene referentiekaders als CobIT en de Code voor Informatiebeveiliging. Afhankelijk van de diepgang van het onderzoek wordt inzicht gegeven in:

- de ICT-risico's: het risicoprofiel van de informatievoorziening;
- de ICT-controls: de mate waarin beheersingsmaatregelen zijn genomen om de risico's te beheersen ten aanzien van de ICT-processen;
- de effectiviteit van beheersingsmaatregelen: de effectiviteit van de maatregelen die zijn getroffen.

Benchmarks leveren organisaties een aanzienlijke hoeveelheid marktinformatie op waardoor het gebruik ervan in zijn algemeenheid als een toegevoegde waarde kan worden gezien.

De toenemende wet- en regelgeving op het gebied van Corporate Governance (zoals de Sarbanes-Oxley Act 2002) vraagt om verantwoording van beheersing van de bedrijfsprocessen. Beheersing van de informatievoorziening is een integraal onderdeel van de beheersing binnen een organisatie. We zien dan ook in toenemende mate een vraag naar verantwoording over de beheersing van de informatievoorziening. IT Risk Management Benchmarking verschaft het benodigde inzicht in de kwaliteit van de beheersing van de informatievoorziening binnen een organisatie. Tevens is de ontwikkelde tooling dusdanig opgezet dat zij eenvoudig kan worden aangepast voor andere doeleinden, waaronder (self-) control assessments.

Literatuur

[ISAC00] CobIT, *Control Objectives*, third edition, ISACA/ IT Governance Institute, 2000.

[NEN00] *Code voor informatiebeveiliging, Een leidraad voor beleid en implementatie*, Nederlands Normalisatie-instituut, 2000.

[Somm97] E.R van Sommeren, J.C. Boer en J.A.M. Donkers, *Benchmarking van Informatietechnologie*, Automatisering Gids, oktober 1997.