Risicomanagement en certificering in outsourcingland

Ing. C. Slob

In de wereld van outsourcing zijn risicomanagement, beveiliging en kwaliteit van groot belang. Met het oog op deze verantwoordelijkheidsterreinen zijn binnen Capgemini Outsourcing de laatste jaren enkele specifieke maatregelen getroffen en projecten uitgevoerd, zoals BS7799-2-certificering, Regulatory Compliant QMS en volledige ITIL-compliancy. In dit artikel komen de vragen 'Hoe ga je als outsourcer om met risicomanagement?', Waarom BS7799-2?; 'Wat is het effect van rightshoring?'; 'Welke hulpmiddelen gebruik je?'; 'Welke problemen kom je tegen?'; 'Wat betekenen deze zaken voor de organisatie en de klanten?' en 'Welke rol spelen recente ontwikkelingen als SOX en LSF hierbij?' aan de orde.

Inleiding

Als outsourcer ben je verantwoordelijk voor de systemen van klanten met daarop hun kritische bedrijfsprocessen en gegevens. Kwaliteit en risicomanagement zijn daarom binnen de wereld van outsourcing essentieel. Vooral de laatste jaren is een toenemende druk ten aanzien van kwaliteit en beveiliging merkbaar. Deze druk uit zich onder andere in de volgende verschijnselen:

- Als outsourcer word je geconfronteerd met een toenemend aantal audits door of namens klanten.
- Aantoonbaarheid wordt ook buiten Regulatory Compliant-systemen (zoals FDA en SOX) steeds belangrijker.
- Er is sprake van een toenemend aantal dreigingen van buiten af.
- Er is sprake van een toenemend aantal eisen vanuit wet- en regelgeving.

Daarnaast is er een steeds grotere druk tot kostenbesparing, die weliswaar tegenstrijdig lijkt met de bovenstaande ontwikkelingen maar in de praktijk daarmee heel goed is te combineren, hoewel er natuurlijk in eerste instantie investeringen noodzakelijk zijn.

Ing. C. Slob
is Quality en Security Manager binnen Capgemini Outsourcing BV en als zodanig verantwoordelijk voor het kwaliteits- en beveiligingsbeleid. Daarvoor was hij tien jaar werkzaam als project- en programmamanager binnen de sector products van Capgemini Nederland BV.

kees.slob@capgemini.com

Opzet Quality Management Systeem (QMS)

Het QMS is opgezet als paraplu voor kwaliteit, beveiliging en het zogenaamde 'Regulatory Compliant QMS', speciaal bedoeld voor klanten waar de regels van de Amerikaanse Food and Drugs Administration of zijn Europese tegenhanger van toepassing zijn. Deze opzet is bewust gekozen om een aantal zaken, zoals managementattentie, verbeterloop en dashboards, in één keer standaard voor alle systemen te regelen. Daarnaast zijn de ITIL-processen direct als onderdeel binnen het standaard-QMS opgenomen. Dit laatste omdat de ITIL-processen binnen outsourcing de primaire bedrijfsprocessen vormen en er vanuit audits veel druk op deze processen staat. Verder is bewust gekozen voor internationale normen en standaarden (zoals ISO 9001:2000, BS7799-2, BS15000) als basis voor de verschillende systemen, iets wat binnen een internationaal bedrijf essentieel is om internationaal te kunnen samenwerken.

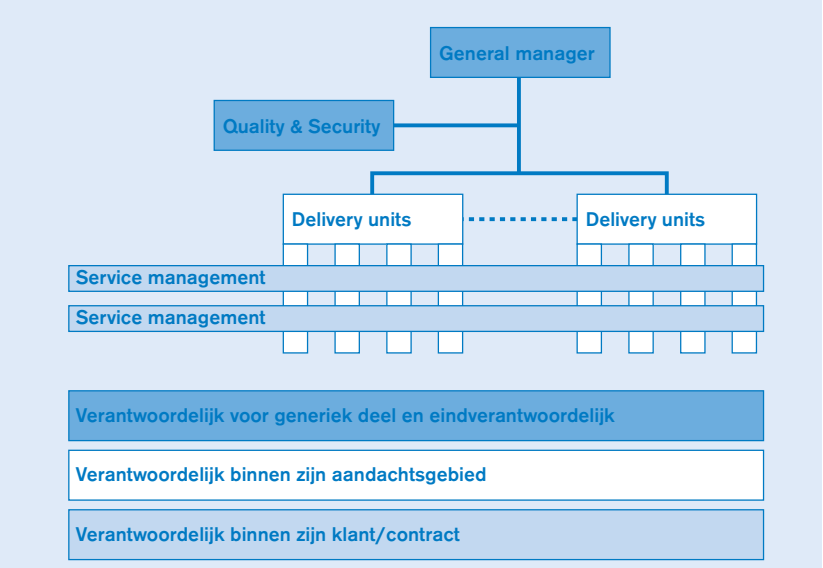
Zoals in figuur 1 is aangegeven, is binnen het QMS sprake van twee hoofdblokken, namelijk die zaken die voor alle klanten van toepassing zijn en zaken die alleen van toepassing zijn indien dit specifiek met een bepaalde klant is afgesproken. Voorbeelden van deze laatste zijn toepassing van de regels van het Regulatory Compliant QMS, maar ook zaken binnen security zoals uitwijk, dubbel uitgevoerde systemen en dergelijke.

Figuur 1. Structuur van QMS.

Tijdens de opzet en implementatie van het totale systeem zijn de volgende aspecten van belang:

- Het is belangrijk om uit te gaan van één systeem. De verschillende systemen los implementeren lijkt in eerste instantie eenvoudiger, maar leidt uiteindelijk tot verwarring en doublures in processen.
- Zaken als Regulatory Compliancy en extra beveiliging zijn toevoegingen op het standaardproces en houden geen andere werkwijze in. Daarnaast is het van belang dat ook deze toevoegingen weer zoveel mogelijk standaard zijn, en niet verschillend per klant.
- Neem als basis internationale normen en standaarden. Lokale standaarden en normen blijken goed in te passen in deze internationale kaders en deze aanpak maakt internationale samenwerking een stuk eenvoudiger.
- Bewustwording en continue aandacht zijn een vereiste. Het alleen opzetten en implementeren van dit soort systemen heeft in de praktijk maar een zeer tijdelijk effect.
- De opzet en implementatie van dit soort systemen is niet iets wat men er even bij doet. Een projectmatige aanpak met volledige managementondersteuning is essentieel.

Figuur 2. QMS-organisatie.



De organisatie rond het QMS is opgezet zoals aangegeven in figuur 2. Uitgangspunt hierbij is dat iedereen verantwoordelijk is binnen zijn aandachtsgebied/scope en daarop ook wordt gemeten. Hiervoor worden dashboards in de vorm van balanced scorecards gebruikt op bedrijfsniveau, maar ook per service manager, contract en (sub-)delivery unit. Deze dashboards worden via het intranet gepubliceerd, en binnen de verschillende overlegorganen maandelijks besproken. Een voorbeeld van een dergelijk dashboard is weergegeven in figuur 3. Het gaat hier om het dashboard op bedrijfsniveau. Op de lager liggende niveaus is er sprake van meer detail. Op bedrijfsniveau worden de Key Performance Indicators jaarlijks in het managementteam gedefinieerd, en wordt het verloop maandelijks besproken. Naast een aantal vaste zaken zoals marge, sales hitrate, klanttevredenheid en het halen van de service levels, kunnen hieraan jaarlijks specifieke speerpunten worden toegevoegd.

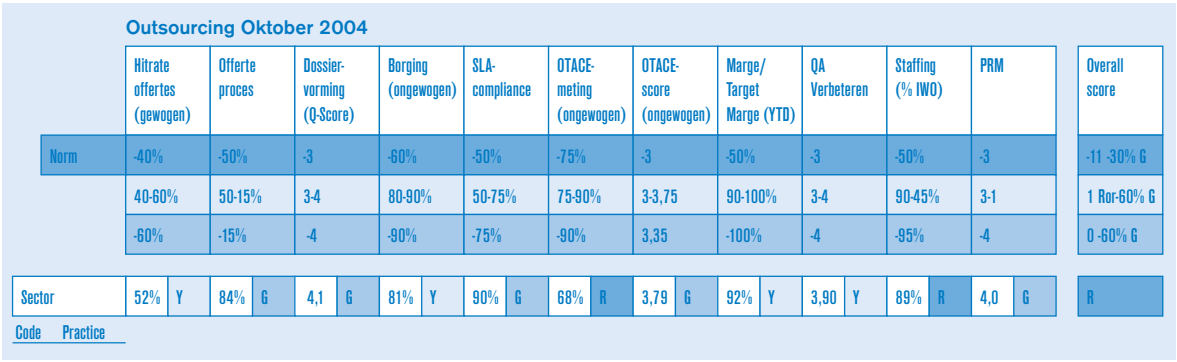
Naast de al genoemde dashboards worden tal van andere maatregelen ingezet. Er worden regelmatig audits gehouden vanuit de stafafdeling en de interne accountants, naast de certificeringsaudits voor ISO 9001:2000 en BS7799-2 die tweemaal per jaar plaatsvinden door KEMA, TPM-audits door KPMG en audits door of namens klanten ten behoeve van hun jaarrekeningcontrole of wet- en regelgeving. De aandachtspunten uit deze audits worden vervolgens centraal vastgelegd en bewaakt. Verder is er een standaardpresentatie over kwaliteit en beveiliging binnen het introductieprogramma voor nieuwe medewerkers en zijn deze aspecten een regelmatig terugkerend onderwerp bij unitmeetings en andere vormen van overleg, om het hoe en waarom van het QMS levend te houden.

Rightshoring

Een ontwikkeling van de laatste jaren is het uitvoeren van werkzaamheden in zogenaamde lagelonenlanden, zoals Spanje, India en China, en landen in het voormalige Oostblok, zoals Polen. Deze ontwikkeling roept vooral in het kader van risicobeheersing en kwaliteit ook een aantal vragen op, zoals:

- Hoe past deze ontwikkeling binnen onze processen?
- Hoe gaan we om met taal- en cultuurverschillen?
- Hoe kunnen we voldoende controle uitoefenen om de kwaliteit te garanderen?
- Wat betekent deze ontwikkeling voor onze certificering?
- Hoe past deze ontwikkeling binnen de eisen vanuit de wet- en regelgeving voor onze klanten?
- Hoe regel je het contact?

Binnen Capgemini Outsourcing hebben we een aantal maatregelen genomen om deze uitdagingen het hoofd



Figuur 3. Dashboard.

te bieden en het risico te beperken. Al onze ITIL-processen zijn internationaal gelijk, terwijl het QMS en de securityprocessen zijn opgezet vanuit dezelfde basis met lokale invulling, en het RC-QMS is opgezet op basis van internationale 'best practices'. Verder gebruiken we ten behoeve van het primaire proces internationaal dezelfde tools (callregistratie, asset management, configuration management, knowledge management, etc.) en werken alle vestigingen met certificering tegen dezelfde internationale normen. Zo is bijvoorbeeld Capgemini India ook gecertificeerd volgens ISO 9001:2000 en BS7799-2. Daarnaast hebben we er in Nederland voor gekozen om voor het contact en de controle te werken met een man ter plaatse. Met bovenstaande maatregelen blijken de risico's van rightshoring niet groter of zelfs kleiner dan wanneer je gebruikmaakt van een lokale derde partij om werkzaamheden uit te voeren.

Risicomanagement

Een belangrijk onderdeel binnen outsourcing is risicomanagement, waarbij de volgende aspecten een belangrijke rol spelen:

- generieke risico's over alle klanten en contracten, zoals mensen, gebouwen, financiën, offertes en delivery;
- risico's bij een bepaalde klant, zoals een bepaald type dienstverlening, een dispuut, financiën of maatschappelijke factoren (actiegroepen, etc.);
- risico's binnen een bepaald contract door nieuwe technieken, afwijkende service levels, etc.;
- risico's ten aanzien van bepaalde typen dienstverlening.

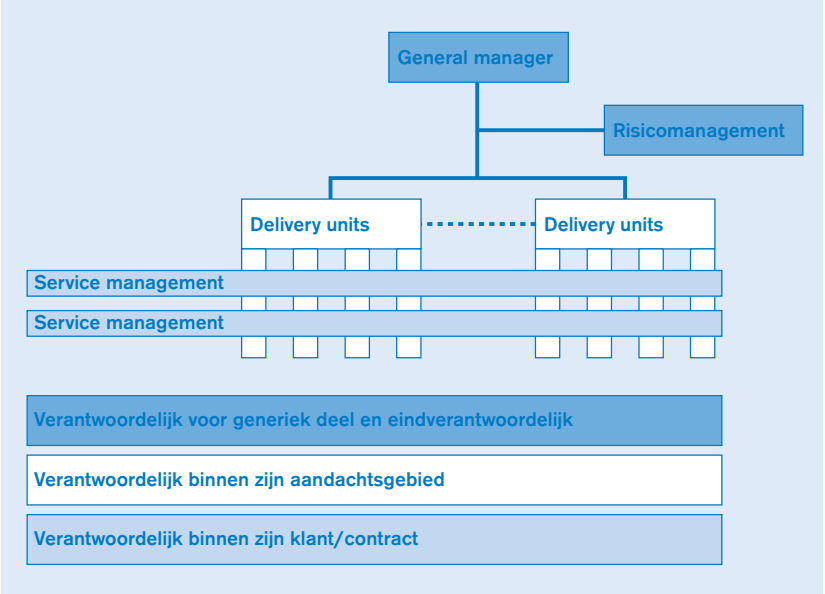
Nu kan men risicomanagement zien als een apart aandachtsgebied los van kwaliteit en beveiliging, maar door het overlappen van veel aspecten hebben wij ervoor gekozen om risicomanagement te integreren binnen onze normale processen en managementsystemen. Dit blijkt al uit het in figuur 4 weergegeven organigram rond risicomanagement, dat volledig overeenkomt met het in figuur 2 weergegeven organigram rond kwaliteit en beveiliging.

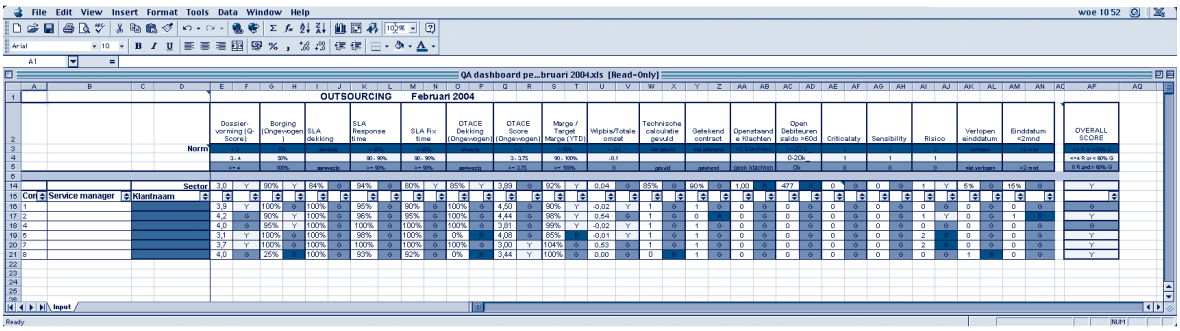
Daarnaast worden de risicoaspecten meegenomen in de generieke dashboards, zowel op bedrijfsniveau als per unit, service manager en contract. Verder zijn er ten aanzien van risicomanagement enkele specifieke maatregelen genomen:

- Ten aanzien van beveiliging wordt er jaarlijks een risicoanalyse uitgevoerd, en is er bij gevoelige klanten regelmatig overleg via de service manager en jaarlijks via de security manager.
- Binnen contracten wordt er maandelijks een risicoanalyse uitgevoerd via de rapportage van de service manager, is risicoanalyse een vast onderdeel van het change proces, en is risicomanagement een vast onderdeel van het maandelijkse overleg tussen de service manager en het lijnmanagement.
- Bij nieuwe dienstverlening is risicoanalyse een vast onderdeel in elk stadium van het offerteproces met een formele review door de risicomanager.

Naast bovenstaande specifieke zaken is er een portal ontwikkeld met hierin alle gegevens per klant en contract waarin naast kwaliteit en financiële zaken ook een risicoprofiel is opgenomen, dat maandelijks tijdens het overleg tussen de service manager en het lijnmanagement wordt bijgewerkt. Een voorbeeld van dit risicoprofiel is weergegeven in figuur 6.

Figuur 4. Organisatie risicomanagement.





Figuur 5. Dashboard per contract.

Recente ontwikkelingen als SOX en LSF

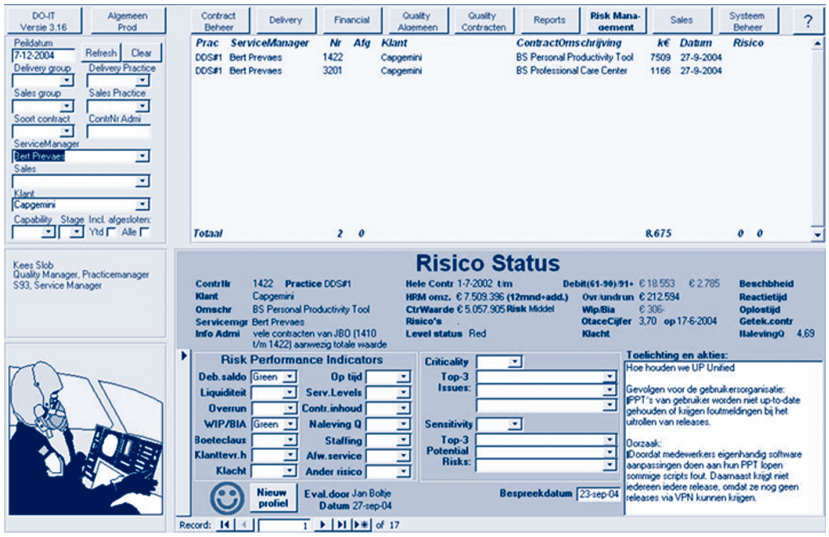
Het laatste jaar worden we binnen outsourcing steeds meer geconfronteerd met vragen rond SOX compliancy van onze dienstverlening. Daarnaast is er sprake van een ontwikkeling waarbij we zien dat er steeds meer audits worden uitgevoerd door of namens onze klanten met als gevolg een toenemende druk bij die klanten op de organisatie, medewerkers die 'auditmoe' worden, en dat je als leverancier geconfronteerd wordt met steeds weer verschillende normenkaders en toenemende kosten. Deze ontwikkeling is natuurlijk wel te verklaren door de toenemende druk op onze klanten door internationale wet- en regelgeving, waarbij naast SOX ook LSF (Loi sur la sécurité financière; wetgeving over de betrouwbaarheid van financiële systemen in Europa) een rol speelt. Een ontwikkeling die je als outsourcer stelt voor een aantal uitdagingen om de gevolgen hiervan het hoofd te bieden. De keuze die wij als Capgemini Outsourcing hebben gemaakt, is het opstarten van een project met als deliverable eind 2005 een SAS 70 type 2-verklaring met betrekking tot onze dienstverlening.
Dit besluit is genomen omdat wij het werken volgens SAS 70 voor een outsourcer noodzakelijk achten. De aanpak is gebaseerd op de volgende uitgangspunten:

- De huidige certificeringen vormen de basis.
- Het normenkader is internationaal binnen Capgemini gelijk.
- De verklaring wordt lokaal afgegeven.
- De noodzakelijke controles worden belegd binnen de generieke processen.
- Het project wordt uitgevoerd in samenwerking met de interne accountants waarbij we proefaudits zullen laten uitvoeren door een externe partij.

Hiermee verwachten wij de noodzaak van specifieke klantaudits tot een minimum te kunnen beperken, waardoor de druk op de organisatie afneemt en de medewerkers weer het gevoel krijgen dat ze normaal hun werk kunnen doen zonder zich regelmatig te moeten verantwoorden tegenover auditors.

De eerste ervaringen met het project geven aan dat het voldoen aan SAS 70 type 2 niet zozeer een kwestie is van veranderen van werkwijzen en het uitvoeren van andere processen, maar dat het belangrijkste aandachtspunt zit in de aantoonbaarheid, zowel met betrekking tot de uitvoering als de controle op deze uitvoering. Dit geeft gelijk aan dat eisen die voor gewone klanten moeten worden geregeld, steeds meer opschuiven naar de eisen die voor Regulatory Compliant-klanten al heel normaal zijn.

Figuur 6. Risicoprofiel binnen portal.



Conclusie

De huidige ontwikkelingen in de markt rond wet- en regelgeving (SOX en LSF) leggen weliswaar een behoorlijke druk op outsourcingpartijen, maar de hiermee samenhangende eisen zijn niet dusdanig dat de op dit moment ingerichte processen niet langer toereikend zijn. Wel is er een toenemende druk op aantoonbaarheid van uitvoering en controle op deze uitvoering. Dit is echter in QMS-systemen die zijn gebaseerd op internationale normen op een redelijk eenvoudige wijze in te passen. Wel brengt dit in eerste instantie extra kosten met zich mee, die zich echter uiteindelijk zullen vertalen in een kwalitatief betere en voorspelbaardere dienstverlening en daarmee gepaard gaande lagere kosten. Immers, het onder druk oplossen van problemen geeft in het algemeen meer kosten dan het voorkomen van deze problemen.