Een introductie van Ronald Jonker

SAP-compliance en business improvement

Drs. R.A. Jonker RE RA
is partner bij KPMG IT Advisory. Hij geeft leiding aan de SAP-adviesdienstverlening van KPMG in Nederland. Hij adviseert op een breed scala van onderwerpen, zoals haalbaarheidsstudies, implementatiestrategie, procesverbetering, security & controls, migratiestrategie, testen, data-analyse en controls monitoring. Hij is gecertificeerd ASAP-consultant en schrijver van een groot aantal artikelen op zijn vakgebied.
jonker.ronald@kpmg

Drs. M.A.P. op het Veld RE
is senior manager bij KPMG IT Advisory. Zijn werkzaamheden zijn gericht op audit- en adviesdiensten, onder andere op het gebied van Enterprise Resource Planning (ERP)-systemen zoals SAP. Hierbij behoort het adviseren op het gebied van tool based monitoring/auditing, GRC, SOX, Control Frameworks en optimalisatietrajecten tot zijn specialisaties. Daarnaast is hij docent aan de TIAS-opleiding EDP-Auditing en gastdocent aan de postdoctorale accountancyopleiding van de Universiteit van Tilburg. Verder is hij medeverantwoordelijk voor SAP Advisory services binnen KPMG IT Advisory Nederland.
ophetveld.maurice@kpmg.nl

Drs. B. Coolen RE
is manager bij KPMG IT Advisory en werkzaam binnen KPMG's SAP Advisory groep. Hij heeft ervaring opgedaan met een breed scala aan ERP-gerelateerde advies- en auditopdrachten. Hij is betrokken geweest bij diverse opdrachten op het gebied van procesverbetering rondom SAP-systemen en het opzetten en implementeren van GRC-tools.
coolen.bram@kpmg.nl

Drs. Ronald Jonker RE RA, drs. Maurice op het Veld RE en drs. Bram Coolen RE

De huidige uitdaging voor veel organisaties is naast het praktisch en efficiënt toepassen van 'Governance, Risk and Compliance' ook het verhogen van de efficiëntie en effectiviteit van de bedrijfsprocessen. Is dit mogelijk? Zijn de onderwerpen risico's en compliance niet strijdig met procesverbetering? In dit artikel wordt ingegaan op de vraag hoe een geïntegreerde visie op het gebied van Governance, Risk and Compliance en ondersteunende tooling kan leiden tot continue zekerheid, lagere compliancekosten en procesverbetering.

Inleiding

Het verwezenlijken van de toekomstige doelstellingen 'focus op verwerken van interne én externe informatie', 'exploitatie van informatie leidt tot creëren van business' en 'onmisbaarheid van bottom-up informatiestromen' waren de uitkomsten van het onderzoek van KPMG in de zomer van 2007. Kort samengevat wordt het goed omgaan met informatie steeds crucialer voor het succes van organisaties. Deze ontwikkeling wordt enerzijds gedreven door steeds hogere eisen op het gebied van compliance en het voldoen aan wet- en regelgeving. Anderzijds proberen organisaties op basis van veel investeringen in informatiesystemen processen steeds efficiënter en effectiever te maken. Beide onderwerpen, compliance en procesverbetering, lijken niet hand in hand te gaan. Hoe kan immers compliance leiden tot procesverbetering? In dit artikel wordt ingegaan op de relatie tussen compliance en procesverbetering en hoe een goede beheersing van beide onderwerpen kan leiden tot een beter presterende organisatie.

Allereerst wordt het onderwerp Governance, Risk and Compliance (GRC) nader toegelicht inclusief de verschillende volwassenheidsfasen die organisaties doorlopen. Vervolgens wordt toegelicht welke relatie bestaat tussen GRC en procesverbetering, waarbij tevens concrete voorbeelden worden gegeven hoe GRC-tools hierbij kunnen ondersteunen. Ten slotte wordt aangegeven welke soorten GRC-tools momenteel in de markt bestaan, op welke niveaus deze tools ingezet kunnen worden en hoe deze tools kunnen bijdragen aan een beter bedrijfsresultaat.

Tijdens het KPMG IT Advisory Seminar 'Trends in IT - Information Governance' op 1 november 2007 heeft in de workshop 'SAP compliance & business improvement' een open discussie plaatsgevonden met organisaties die bezig zijn met deze onderwerpen.

In dit artikel wordt tevens ingegaan op de resultaten van deze discussie.

Governance, Risk and Compliance

De aandacht voor risicobeheersing en het voldoen aan wet- en regelgeving is de afgelopen jaren flink toegenomen. Veel geïndustrialiseerde landen hebben als gevolg van financiële deconfitures wetten en regels in het leven geroepen die transparantie, de onafhankelijkheid van de auditor en financieel toezicht op bedrijven en instellingen versterken. De bekendste voorbeelden daarvan in Nederland zijn de code-Tabaksblat en de Amerikaanse Sarbanes-Oxley wet.

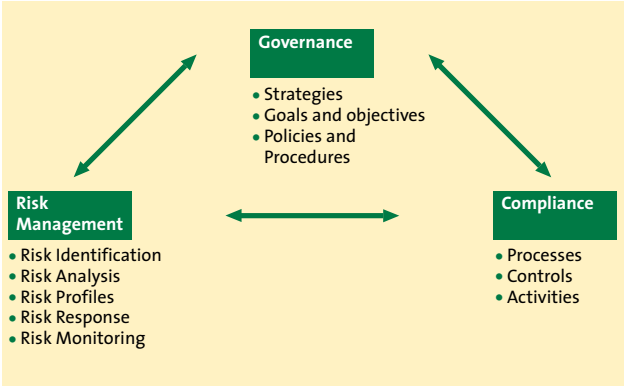
Bedrijven die dienen te voldoen aan deze wetten, zien zich voor de vraag gesteld hoe zij het vertrouwen van de aandeelhouders en toezichthouders kunnen vergroten door het instellen van een effectief stelsel van interne controle zonder dat dit ten koste gaat van de operationele slagkracht. Of beter nog, waarbij dit stelsel de bedrijfsvoering positief beïnvloedt.

Vooruitstrevende bedrijven en instellingen benaderen het invoeren van interne controle en het afleggen van verantwoording over de effectiviteit daarvan niet als een op zichzelf staand eenmalig project. Zij zien het verband tussen verschillende Governance, Risk and Compliance (GRC)-activiteiten binnen hun organisatie. Onder GRC wordt hierbij verstaan (zie ook figuur 1):

- *Governance:* het geheel van beleid, procedures en maatregelen om een organisatie te kunnen laten functioneren in overeenstemming met haar strategische doelstellingen.
- *Risk management:* het geheel van procedures en maatregelen dat zich richt op het systematisch identificeren van risico's, het nemen van mitigerende maatregelen en het rapporteren over het functioneren van risk management aan de leiding.
- *Compliance:* het voldoen aan wet- en regelgeving, dan wel: het geheel van maatregelen en procedures dat er zorg voor draagt dat een organisatie voldoet aan wet- en regelgeving en daarover verantwoording aflegt.

Organisaties met een geïntegreerde GRC-benadering weten de GRC-activiteiten te combineren in een samenhangend geheel van op elkaar afgestemde processen, waarmee zij doublures en inefficiënties weten uit te bannen. Het is duidelijk dat deze organisaties weten te profiteren van de geïntegreerde kracht van GRC en hun Total Cost of Compliance weten te verlagen, wat ze een concurrentievoordeel oplevert ten opzichte van hun 'peers'.

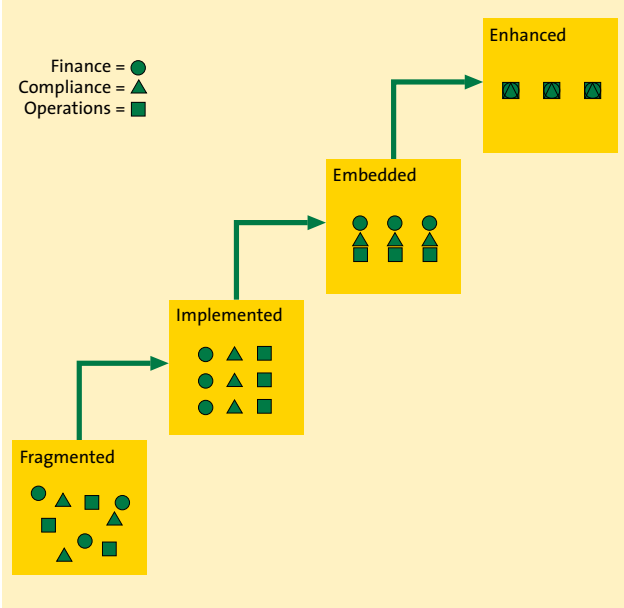
Integratie van GRC-activiteiten kan echter niet zonder geautomatiseerde ondersteuning. Zoals later in dit artikel wordt behandeld, zijn er voor de verschillende niveaus van GRC-activiteiten ook verschillende typen GRC-systemen beschikbaar. Het is interessant te zien dat diverse softwareleveranciers nu meer en meer toepassingen op de markt brengen die de verschillende niveaus van GRC-activiteiten ondersteunen. In het bijzonder geldt dit voor SAP, die onlangs haar visie rond GRC ontvouwde en in 2008 verwacht een complete suite van toepassingen voor haar cliënten beschikbaar te hebben ([SAP07]).



Figuur 1. **GRC uitgewerkt (bron: [SAP07]).**

Bij het integreren van de GRC-activiteiten doorlopen organisaties in de praktijk vaak vier volwassenheidsniveaus (zie ook figuur 2):

1. *Fragmented:* compliance is project-centric; compliance (bijvoorbeeld SOX) wordt in eerste instantie als een centraal project gerund. Dit vereist veel centrale projectcoördinatie om iedereen aangesloten te houden en uniform te laten werken.



Figuur 2. **GRC-volwassenheidsniveaus.**

2. *Implemented:* compliance is program-centric, waarbij een overkoepelend en gestructureerd programma dedicated personen aanwijst om de complianceactiviteiten te coördineren en communiceren.
3. *Embedded:* compliance is proces-centric, waarbij compliance in de processen wordt ingebouwd. Compliance wordt 'business as usual'. Verantwoordelijkheid voor compliance komt bij de business en process owners te liggen.
4. *Enhanced:* compliance is culture-centric en framework integrated. Compliance is verder ingebed in de organisatie, waarbij compliance niet een doel op zich is. Meerdere regelgevingen worden geïntegreerd en met de nieuwe werkwijze afgedekt. Daarnaast zal de transparantie ook kunnen leiden tot business process improvement.

Integrale visie op GRC en tooling is noodzakelijk voor verdere procesoptimalisatie en -efficiency

Organisaties die deelnamen aan de workshop op 1 november gaven aan gemiddeld op het niveau 'implemented' te zitten. Tevens werd aangegeven dat het realiseren van de volgende stap van groot belang is om de efficiëntie- en effectiviteitsvoordelen volledig te benutten. Hierbij werden de volgende stappen onderkend:
1. *Opzetten integrale GRC-strategie en GRC-roadmap.* Begonnen wordt met het identificeren van alle GRC-vereisten binnen de organisatie en het uitwerken daarvan in een strategie en roadmap.
2. *Controlstransformatie naar IT.* Er is de afgelopen jaren veel geïnvesteerd in IT- en SAP-systemen. Compliance dient daar ook gebruik van te maken om een juiste balans te bereiken tussen preventieve IT controls en de vaak detectieve handmatige controles.
3. *Embedding van controls in de organisatie.* Uiteindelijk dient compliance 'business as usual' te worden. Controls worden vaak al binnen de processen uitgevoerd, maar dienen verder transparant te worden gemaakt en er moet over worden gerapporteerd.
4. *Integreren van verschillende compliance frameworks.* Veel verplichtingen voor wet- en regelgeving worden binnen organisaties gezien als 'koninkrijkjes' (bijvoorbeeld SOX, FDA, Basel II, ISO, etc.). Organisaties die dit kunnen doorbreken en het eenmalig testen van controls voor meerdere wet- en regelgevingen laten gebruiken, hebben de mogelijkheid om het complianceproces verder efficiënt te maken.

Hoewel werd aangegeven dat GRC inmiddels op de agenda van het management staat, wordt een hogere prioriteit toegekend aan procesverbeteringsinitiatieven. Deze initiatieven staan vaak los van de activiteiten op het gebied van GRC. In de volgende paragraaf wordt aangegeven dat er wel degelijk een relatie bestaat tussen GRC en procesverbetering.

GRC en procesverbetering

Verbetering van procesefficiëntie en -effectiviteit is voor bijna elke organisatie één van de strategische speerpunten. Maar waar begin je? Welke processen presteren momenteel niet goed en welke verbeteracties dienen te worden ingezet? Bovendien worden processen steeds complexer en worden er steeds hogere eisen gesteld aan kwaliteit en betrouwbaarheid enerzijds vanuit de klant en anderzijds vanuit wet- en regelgeving.

De basis voor het verbeteren van efficiëntie, effectiviteit en betrouwbaarheid van processen ligt bij het verkrijgen van inzicht in het huidige proces en de 'root-causes' van problemen. Zonder dit inzicht is het niet mogelijk goede verbeteracties te definiëren en te implementeren. Wat veroorzaakt immers de lange doorlooptijd van het verkooptraject of waarom zijn de kosten per inkooporder zo hoog? Waarom is de klanttevredenheid zo laag voor een bepaalde productcategorie?

Om een goed inzicht te krijgen in de processen, is het noodzakelijk dat een organisatie de volgende twee randvoorwaarden heeft ingevuld:
- definiëren van de belangrijkste prestatie-indicatoren, en
- geautomatiseerd analyseren van deze prestatie-indicatoren.

Deze randvoorwaarden worden in de volgende subparagrafen behandeld.

Definiëren prestatie-indicatoren

Hoewel veel organisaties inmiddels zogenaamde KPI's (Key Performance Indicators) hebben opgezet om op strategisch en tactisch niveau de prestaties van de organisatie in de gaten te houden, hebben nog weinig organisaties dezelfde indicatoren op processtapniveau opgezet. Vaak wordt geconstateerd dat processen niet optimaal presteren, maar kan nog onvoldoende concreet worden aangetoond waar dit door wordt veroorzaakt. Door het definiëren van prestatie-indicatoren op processtapniveau kan dit worden voorkomen. Deze indicatoren worden PPI's (Process Performance Indicators) genoemd. Gedefinieerde PPI's kunnen namelijk concreet aantonen waar potentiële verbeteringen kunnen worden gerealiseerd.

Om deze stelling verder toe te lichten, wordt als voorbeeld de processtap facturatie binnen het inkoopproces gepakt. Om de performance van deze processtap te bepalen, zouden de volgende PPI's kunnen worden opgesteld:
- *Percentage inkoopfacturen zonder inkooporder*

Binnenkomende facturen waarvoor een inkooporder en een

bericht van goederenontvangst in het systeem aanwezig zijn, kunnen bij geen verschil vaak zonder aanvullende inspanningen worden betaald. Facturen waarvoor geen inkooporder in het systeem aanwezig is, dienen handmatig te worden gecontroleerd en te worden betaald. In dit geval dient de medewerker van de crediteurenadministratie handmatig te verifiëren of de gegevens op de factuur kloppen. Bovendien dient de betaling van deze facturen vaak door meerdere personen handmatig te worden goedgekeurd. Voor het verwerken van deze facturen is zowel de doorlooptijd als benodigde inspanning vele malen hoger dan bij facturen waarvoor reeds een inkooporder en een bericht van goederenontvangst aanwezig zijn.

- *Percentage inkoopfacturen dat geblokkeerd raakt*

Indien veel binnenkomende facturen geblokkeerd raken doordat volgens het systeem de gefactureerde gegevens niet kloppen (zoals prijs en hoeveelheid), dient de medewerker van de crediteurenadministratie handmatig te onderzoeken wat het probleem is. Waarom raakt de factuur geblokkeerd? Wellicht klopt de prijs niet. Of zijn de goederen nog niet ontvangen. Het kan namelijk zijn dat gefactureerde goederen weliswaar zijn ontvangen, maar dat de goederenontvangst nog niet in het systeem was geboekt door de magazijnmedewerker. In ieder geval veroorzaken geblokkeerde inkoopfacturen veel handmatig werk en kunnen zij bovendien leiden tot verlate betalingen aan leveranciers waardoor eventuele kortingen kunnen worden misgelopen.

- *Aantal ontvangen creditnota's*

Een groot aantal ontvangen creditnota's leidt tot hoge administratieve verwerkingskosten. Er moeten immers correctieboekingen worden gemaakt en de betreffende verantwoordelijke personen dienen te worden ingelicht. Bovendien zijn de kosten initieel niet juist geregistreerd, waardoor managementrapportages verkeerde informatie kunnen geven (of kostprijzen van eindproducten verkeerd worden berekend).

Het definiëren en meten van PPI's geeft een goede basis voor procesverbetering

Dit zijn enkele voorbeelden van PPI's, die in detail inzicht kunnen geven in de performance van een processtap. Het definieren van PPI's geeft dan ook een goede basis voor procesverbetering.

Geautomatiseerd analyseren van prestatie-indicatoren

Zoals reeds is toegelicht, ligt de basis voor het verbeteren van efficiëntie, effectiviteit en betrouwbaarheid van processen bij het verkrijgen van inzicht in de performance van processen. Eenmaal gedefinieerde PPI's zijn waardeloos als niet kan worden gemeten wat de werkelijke situatie is. Bovendien is het wenselijk om de PPI's continu in de gaten te kunnen blijven houden om steeds op de hoogte te zijn van de performance van een proces.

Discussie tijdens de SAP compliance & business improvement-workshop

GRC-tools zijn in staat dit soort PPI's continu te meten. Zonder GRC-tools dient een organisatie zelf data-extracties uit systemen te gaan opzetten in vaak dure Business Intelligence-oplossingen. Dit kan, met name door de grote hoeveelheid PPI's, een kostbare oplossing worden en niet opwegen tegen de verwachte voordelen. GRC-tools daarentegen zijn vooral opgezet om analyses te maken op processtapniveau en werken vaak met dezelfde data die nodig zijn om de PPI's te meten. Rapporteren in dashboards is hierbij aan te bevelen, waardoor eventuele aandachtspunten direct kunnen worden herkend en worden opgevolgd.

Om te kunnen rapporteren in dashboards dienen de gedefinieerde PPI's in verband te worden gebracht met kwaliteitscriteria en een verwachte norm. De kwaliteitscriteria kunnen worden onderverdeeld in twee gebieden:

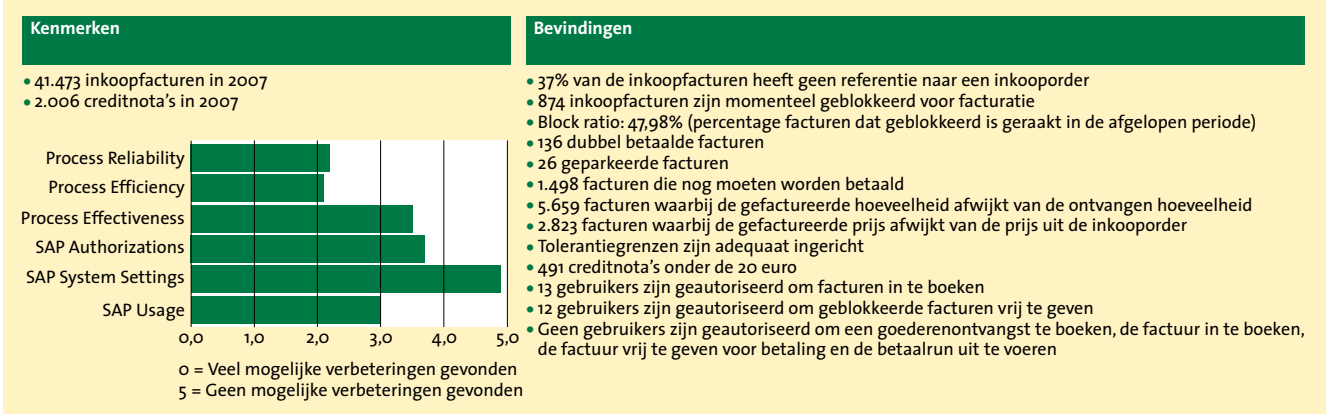
1. *Proces:* kwaliteitscriteria die samenhangen met de manier waarop de organisatie het proces heeft ingericht. Hieronder vallen drie criteria:
   - *procesbetrouwbaarheid:* de mate waarin de gegevensverwerking binnen het proces juist, volledig en geoorloofd plaatsvindt;
   - *proceseffici*ë*ntie:* de mate waarin het proces het gewenste prestatieniveau bereikt tegen een zo laag mogelijk kostenniveau (doelmatigheid);
   - *proceseffectiviteit:* de mate waarin het proces bijdraagt aan de organisatiedoelstellingen en de mate waarin het proces zo snel mogelijk wordt doorlopen.
2. *Systeem:* kwaliteitscriteria die samenhangen met de manier waarop de organisatie het systeem heeft ingericht. Hieronder vallen ook drie criteria:
   - *autorisaties:* de mate waarin de toegekende rechten in het systeem aansluiten met het organisatiemodel en de gewenste functiescheidingen;
   - *systeeminstellingen:* de mate waarin de geprogrammeerde systeeminstellingen een adequate werking van het proces ondersteunen;
   - *gebruik van functionaliteit:* de mate waarin de organisatie gebruik heeft gemaakt van de beschikbare functionaliteit die wordt aangeboden door het systeem.

Gedefinieerde PPI's kunnen worden toegekend aan meerdere kwaliteitscriteria. Zo kan de PPI 'percentage inkoopfacturen dat geblokkeerd raakt' worden toegekend aan de criteria proceseffici*ë*ntie en proceseffectiviteit. Een hoog percentage geblokkeerde inkoopfacturen veroorzaakt namelijk hoge kosten (veel aanvullende manuren vanwege het moeten uitzoeken en opvolgen van de geblokkeerde facturen) en een vertraging van de processnelheid.

Nadat de gedefinieerde PPI's zijn toegekend aan één of meer kwaliteitscriteria dient de gewenste norm te worden gedefinieerd. Er zullen namelijk altijd facturen binnenkomen die blokkeren doordat de gefactureerde prijs of hoeveelheid niet klopt. Een teveel aan geblokkeerde facturen veroorzaakt echter een inefficiëntie in het proces. Een organisatie dient te definiëren welk niveau van geblokkeerde facturen acceptabel is. Hierbij moet een goede analyse worden gemaakt van wat de mogelijke baten zijn afgezet tegen de te verwachten implementatie-inspanning om het percentage verder terug te dringen. Een magazijnmedewerker die namelijk de ontvangen goederen alleen op het einde van de week in het systeem boekt, is wellicht eenvoudig te trainen om elke ontvangst nog op dezelfde dag te boeken waardoor veel manuren kunnen worden gewonnen op de financiële administratie. Facturen echter die geblokkeerd raken doordat de leverancier een verkeerde prijs heeft gehanteerd, zijn niet altijd te voorkomen.

In figuur 3 is een voorbeeld opgenomen van de output van een SAP-tool waarbij enkele mogelijke verbetergebieden zijn gescand voor de processtap facturatie binnen het inkoopproces.

Uit de workshop van 1 november kwam naar voren dat organisaties interesse hebben en de toegevoegde waarde hiervan inzien

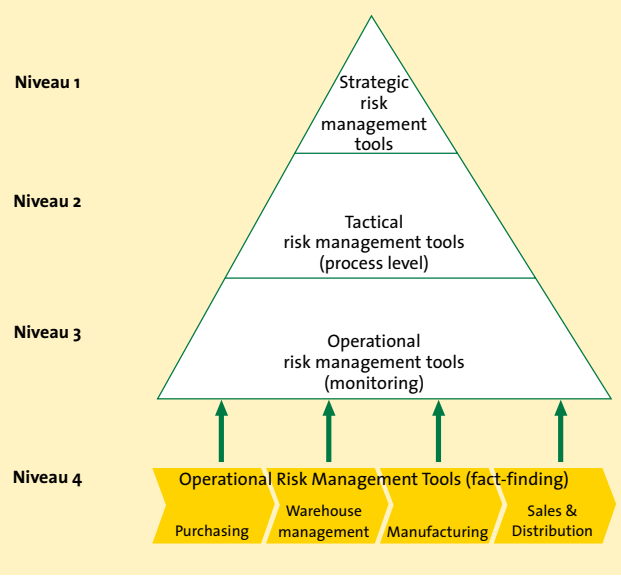


Figuur 3. **Voorbeeld output GRC-tool.**

of zelfs momenteel bezig zijn om GRC-tools verder uit te breiden met PPI's voor procesverbetering. Deze organisaties zijn daarna in staat continu de performance van hun processen te verbeteren, doordat de GRC-tools hen in staat stellen om concreet gesignaleerde aandachtsgebieden direct op te volgen.

GRC-tools: een praktisch overzicht

In de vorige paragraaf is gesproken over het gebruik van GRC-tools voor de ondersteuning bij het verder verbeteren van processen door gebruik van informatie rechtstreeks uit de SAP-systemen (fact-finding). Echter, niet alleen op het SAP-niveau waar de dagelijkse werkzaamheden worden uitgevoerd kunnen GRC-tools ondersteunen en daarmee de effectiviteit en efficiëntie verbeteren. Een GRC-raamwerk moet gedragen worden door de gehele organisatie en heeft daarom invloed op verschillende niveaus van een organisatie. GRC-tools sluiten zich daarbij aan en de GRC-tools die beschikbaar zijn hebben dan ook ieder een focus op één of meer van deze organisatieniveaus (zie figuur 4) ([Brou06]).

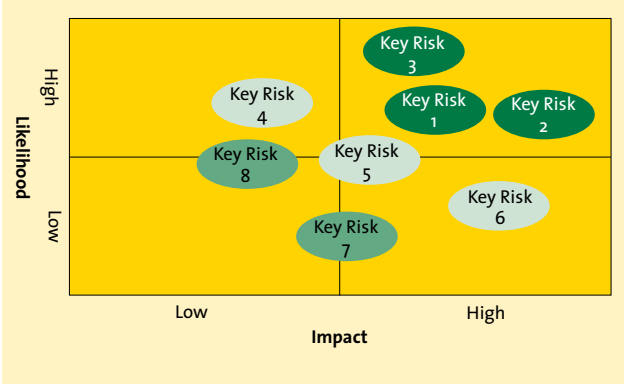


Figuur 4. **Typen GRC-tools binnen de organisatieniveaus.**

De kenmerken en mogelijkheden die GRC-tools kunnen bieden op de verschillende niveaus zijn hieronder beschreven.

Strategic risk management (niveau 1)

Op een strategisch niveau wordt risicomanagement toegepast door het management van de organisatie. Risicomanagement en -analyse wordt door GRC-tools ondersteund om strategische risico's (financiële, veiligheid, operationele, regelgeving, milieu, etc.) te analyseren, bijvoorbeeld door gebruik te maken van de traditionele ballenplaat (zie figuur 5). Daarnaast ondersteunen deze GRC-tools ook het bijhouden van de actielijsten die voortvloeien uit de (strategische) risicoanalyses.



Figuur 5. **Voorbeeld overzicht van strategische risico's.**

Tactical risk management (niveau 2)

Nadat de (strategische) risicoanalyses zijn uitgevoerd, dienen de proceseigenaren en managers deze risico's te beheersen door het opstellen van beleid en het treffen van voldoende controles en werkende maatregelen. Teneinde dit te kunnen doen worden procesrisicoanalyses uitgevoerd om een zo compleet mogelijk beeld van alle risico's in een proces te creëren. Hierin staan procesbeschrijvingen centraal waarin duidelijk de verantwoordelijkheden en controlemaatregelen beschreven worden. Vaak wordt dit verduidelijkt door gebruik te maken van processchema's (zie figuur 6). Op basis van een risicoanalyse op strategisch niveau en procesinzicht op tactisch niveau kan een organisatie een goede mix bepalen van de benodigde controlemaatregelen. Deze mix aan controlemaatregelen beperkt uiteindelijk het risico van een bepaalde proces(stap).

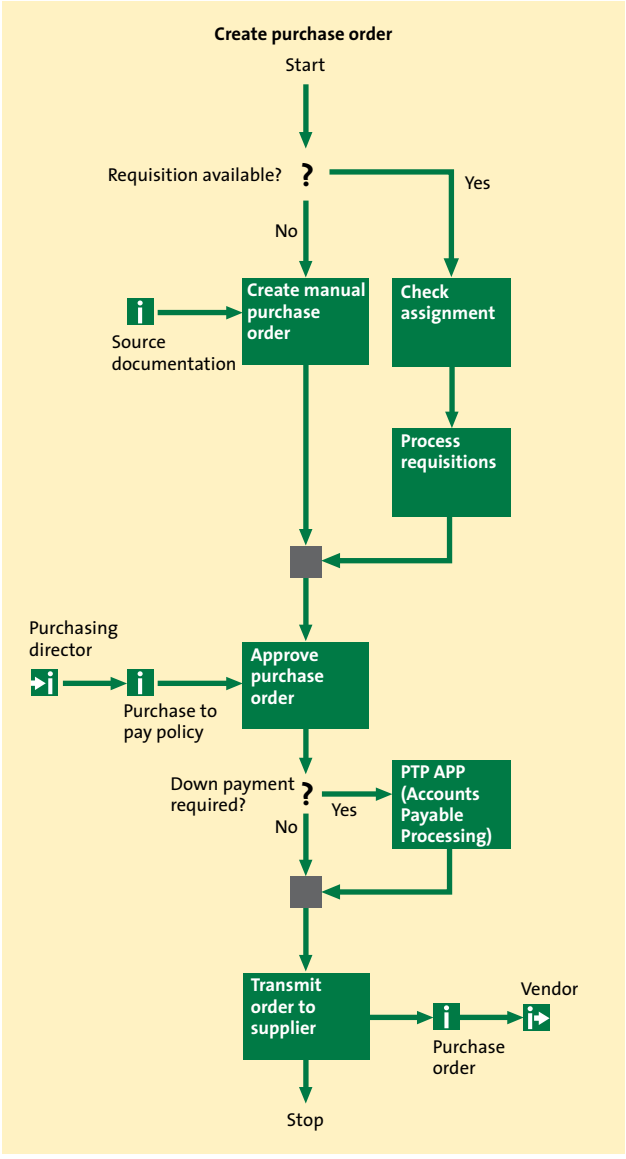
Om een goede mix van benodigde controlemaatregelen te bepalen in SAP-processen, kan gebruik worden gemaakt van het CARP-model, waarbij de afkorting CARP wordt gevormd door de eerste letter van de vier typen maatregelen:

- *Customising controls*

Hiertoe behoren de maatregelen gerelateerd aan de configuratie en stamdata van een informatiesysteem. Voorbeelden hiervan zijn de three-way-match instellingen, verplichte velden, tolerantiegrenzen en automatische boekingen. Deze bieden een goede preventieve controle maar moeten wel op de juiste manier zijn ingericht om te werken. Deze controls zijn instellingen die opgeslagen zijn in het systeem en dus kan het bestaan (het aan of uit staan van een dergelijke instelling) worden vastgesteld.

- *Authorisation controls*

Dit zijn maatregelen die gerelateerd zijn aan de logische toegangsbeveiliging in SAP. Bijvoorbeeld het beperken van het aantal personen aan wie het is toegestaan om een kritieke finan-



Figuur 6. **Voorbeeld processchema.**

ciële transactie (bijvoorbeeld: betalingsrun) uit te voeren, maar ook het beperken van het aantal personen dat een functiescheidingsconflict veroorzaakt (bijvoorbeeld het wijzigen van bankrekeningnummers van leveranciers en het uitvoeren van de betalingsrun). Gegevens gerelateerd aan de inrichting van de logische toegangsbeveiliging van SAP zijn verankerd in de autorisatiestructuur (profielen/rollen) van SAP. Deze gegevens kunnen worden gebruikt voor het maken van analyses ter beoordeling van de inrichting van logische toegangsbeveiliging (naast wie heeft toegang tot een bepaalde transactie, ook wie heeft in een bepaalde periode de toegang tot transacties verschaft).

- *Reporting controls*

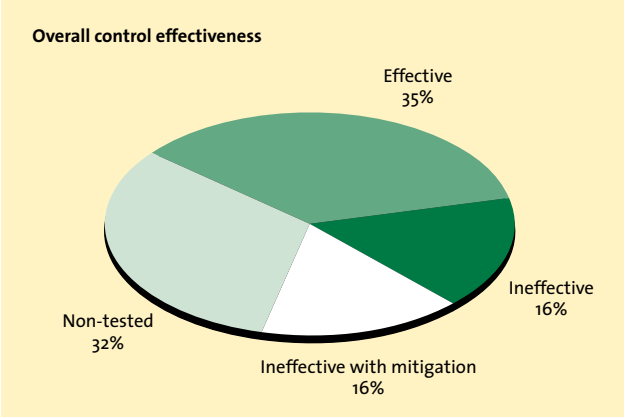
Als onderdeel van de beheersing van een proces door middel van controlemaatregelen, werken gebruikers met controle- en uitzonderingsrapportages die door het systeem worden gegenereerd. Voorbeelden hiervan zijn het periodiek bekijken van veranderingen in bankgegevens – zoals rekeningnummers – van leveranciers, het tijdig opvolgen van de openstaande factu-renwerkvoorraad of facturen verstuurd maar nog niet verwerkt in het grootboek. De gebruiker interpreteert het rapport en kan indien nodig de uitzonderingen rapporteren en opvolgen.

- *Procedural of manual controls*

Dit zijn alle maatregelen die een handmatig karakter hebben en een vangnet vormen indien niet de juiste maatregelen binnen customising, authorisation of reporting controls gekozen kunnen worden. Daarnaast zullen ook bij een geautomatiseerde controle nog enkele handmatige vervolgacties uitgevoerd dienen te worden indien er uitzonderingen zijn.

Operational risk management (niveau 3 en 4)

De procesbeschrijvingen die op een tactisch niveau worden gemaakt om risico's te onderkennen, ingegeven door een risicoanalyse op strategisch niveau, hebben een dagelijkse uitwerking op het operationele niveau. Op dit niveau worden de controles en maatregelen feitelijk uitgevoerd en onderhouden. GRC-tools op dit niveau ondersteunen bij de documentatie van controles, de registratie van de uitvoer daarvan en de registratie van de opvolging van uitzonderingen. Dit wordt veelal gedaan om verantwoording af te kunnen leggen. De controles worden uitgevoerd en de resultaten daarvan worden ingegeven in een dergelijke GRC-tool. Hierdoor kunnen opvolgingsacties worden getraceerd en kan snel een indruk worden verkregen van de status van een controle, ook wel monitoren genoemd.



Figuur 7. **Voorbeeld controlstatus-rapportage.**

Om te kunnen beoordelen of een proces beheerst wordt, dient te worden gekeken naar de werking van de gedefinieerde controlemaatregelen, ervan uitgaande dat de opgezette controlemaatregelen (opzet en bestaan) in een organisatie afdoende zijn om de risico's af te dekken. Het vaststellen en documenteren

van de werking van controlemaatregelen kan met geautomatiseerde fact-finding worden gestaafd. Met inzet van GRC-tooling kan door middel van data-mining[1] technieken deze fact-finding of bewijsvoering worden gegenereerd. Tevens kan GRC-tooling op dit niveau worden gebruikt om inzicht te krijgen in de performance van processen en concreet aan te tonen waar mogelijke procesverbetering kan worden doorgevoerd.

Het gebruik van GRC-tools kan dus ondersteunen op verschillende niveaus binnen een organisatie. GRC-tools op het strategisch en tactisch niveau zijn niet altijd noodzakelijk. Echter, hoe lager het niveau des te dichter op de operatie (en derhalve grotere benodigde inzet van mensen) waarbij het uitvoeren van controlemaatregelen daadwerkelijk veel tijd in beslag kan nemen, en daardoor des te hogere kosten en dus een grotere rol voor GRC-tooling om deze kosten te reduceren. Daarnaast kunnen gegevens over de effectieve werking van individuele controles (op het operationele niveau) geaggregeerd worden en daarmee een indicatie geven van de totale effectieve beheersing van een proces (tactisch niveau).

Ook de organisaties die waren vertegenwoordigd in de workshop op 1 november gebruiken momenteel GRC-tools op diverse niveaus voor het definiëren van risico's, het beschrijven van processen, het monitoren van key controls en het ondersteunen bij procesverbetering. GRC-tooling werd hierbij als absolute noodzaak gezien om tot een effectieve en efficiënte invulling van GRC te komen. Hierbij werd tevens aangegeven dat het hebben van een integrale visie op het gebied van GRC-tooling van groot belang is om GRC en procesoptimalisatie in de toekomst daadwerkelijk in te bedden in de organisatie.

Conclusie

Het in de inleiding aangehaalde KPMG-onderzoek laat zien dat organisaties informatie willen gebruiken om verder succesvol te zijn. Deze informatie dient wel betrouwbaar te zijn. Het op een effectieve en efficiënte manier inrichten van Governance, Risk and Compliance is hiervoor noodzakelijk. Het gepresenteerde GRC-groeimodel geeft over een aantal fasen weer hoe organisaties de transparantie van compliance uiteindelijk kunnen gebruiken om procesverbeteringen te identificeren en door te voeren. Het gebruik van GRC-tooling wordt gezien als noodzakelijke ondersteuning om tot een optimaal volwassenheidsniveau te komen.

Tijdens de workshop 'SAP compliance & business improvement' op 1 november werd het hebben van een integrale visie op GRC en tooling gezien als eerste stap om de hoge compliance effort van de afgelopen jaren daadwerkelijk om te zetten in sustainable added value.

De compliance effort van de afgelopen jaren kan echt worden omgezet in sustainable added value

Literatuur

[Brou06] Drs. P.P.M.G.G. Brouwers RE RA, drs. M.A.P. op het Veld RE en drs. A. Lissone, *Tool based monitoring en auditing van ERP-systemen, van hebbeding naar noodzaak*, Compact 2006/2.

[SAP07] SAP, *SAP Solutions for Governance, Risk and Compliance*, 2007, http://www.sap.com/grc/

1) Met data-mining wordt bedoeld het vergaren van informatie uit een informatiebron (meestal een database) en deze informatie gebruiken voor het creëren van meta-informatie (informatie over informatie).