Duurzame inrichting BPM is noodzaak in financiële sector

SUSTAINABLE COMPLIANCE

Business Process Management en compliance zijn in de financiële sector nauw met elkaar verbonden. De kredietcrisis heeft het bewustzijn ten aanzien van compliance in de financiële sector alleen maar verder vergroot. Een helder zicht op bedrijfsprocessen is voor een bedrijf een belangrijke voorwaarde om in staat te zijn een gedegen verantwoording af te leggen, zowel aan de externe toezichthouder als aan de interne organisatie, risico's helder in kaart te brengen en, indien nodig, maatregelen te treffen, en informatie snel boven water te halen.

Door Coen de Hoon en Cathelijne Snuverink

De grote diversiteit aan interne en externe wet- en regelgeving stelt echter specifieke eisen aan de inrichting van bedrijfsprocessen. Zou het voor een bedrijf niet een enorm voordeel bieden als het in één oogopslag kan zien in hoeverre de BPM-functie duurzaam ingericht is en welke verbeteringen doorgevoerd kunnen worden? Om dit te verwezenlijken is een Sustainable BPM-scan ontwikkeld, waarbij een instelling in een kort tijdsbestek kan onderzoeken of de BPM-functie en de bedrijfsprocessen op zo'n manier zijn ingericht dat het bedrijf 'in control' is, zodat nieuwe wet- of regelgeving weinig problemen zou moeten geven bij invoering. In dit artikel wordt de achtergrond van de scan besproken, zoals de kernelementen van de verschillende belangrijke wetten en regels, de onderdelen van de Sustainable BPM-scan en de resultaten die de scan heeft opgeleverd bij enkele financiële instellingen. Tenslotte zal er ook worden ingegaan op de toepasbaarheid van de scan binnen verschillende financiële instellingen.

BPM en Compliance

Bedrijven die opereren in de financiële markt worden blootgesteld aan een grote diversiteit van wet- en regelgeving. Deze diversiteit bestaat omdat wetten zich vaak richten op één of enkele aspecten van de bedrijfsvoering. Zo richt bijvoorbeeld de Sarbanes-Oxley Act zich met name op financiële verantwoording van ondernemingen die genoteerd staan aan de Amerikaanse beurs. Het Basel II akkoord focust op de risicobeoordeling door banken en de Wet op het financieel toezicht (Wft) legt weer de nadruk op beheersing, informatievoorziening en zorgvuldigheid door financiële instellingen ten behoeve van de consument.

Deze versnippering aan wetgeving leidt er toe dat veel financiële instellingen kiezen voor een ad hoc benadering als het op compliance aankomt. Toch bestaat er op een aantal onderdelen van deze wetten en regels een grote overlap. Zo ook als er specifiek wordt gekeken naar het gebied van Business Process Management.

BPM speelt een belangrijke rol binnen het vakgebied Compliance. Op het gebied van (risico)beheersing, transparantie

en controle is inzicht in hoe de processen ingericht zijn en werken van groot belang. Om ook op langere termijn te kunnen blijven voldoen aan alle wet- en regelgeving, met andere woorden om 'sustainable compliant' te blijven, is het van groot belang om een goede beheerstructuur in te richten.

Kernelementen wet- & regelgeving

De financiële sector heeft te maken met een grote hoeveelheid wet- en regelgeving. Het grootste gedeelte van deze wetgeving richt zich op het inzichtelijk maken en beheersen van risico's. De Sarbanes-Oxley Act en de Code Tabaksblat richten zich met name op het 'in control' zijn voor wat betreft de financiële verantwoording en algehele besturing van de onderneming (corporate governance). Het bestuur van de organisatie moet in kunnen staan voor de betrouwbaarheid en juistheid van de cijfers. Op deze manier moet de bedrijfsvoering transparanter worden. Vanuit dit oogpunt kan ook de International Financial Reporting Standard (IFRS) in dit rijtje geplaatst worden: de boekhouding en jaarrekening dienen op een eenduidige manier vastgesteld te worden.
Basel II en Solvency II richten zich ook op risicobeheersing, maar de focus ligt bij deze wet- en regelgeving op operationele en marktrisico's. Banken en verzekeraars dienen hun portefeuille te differentiëren naar risico's en hierbij hun verwachte verliezen in te schatten. Vervolgens moeten zij op basis hiervan een bepaalde hoeveelheid kapitaal aanhouden zodat de kans dat zij niet aan hun verplichtingen kunnen voldoen wordt geminimaliseerd. Deze risicomodellen dienen een integraal onderdeel uit te maken van de besluitvormingsprocessen binnen het bedrijf. Op operationeel vlak dienen banken en verzekeraars maatregelen te treffen die mogelijke verliezen ten gevolge van fouten veroorzaakt door systemen en mensen tegen gaan. De Basel II richtlijnen, ontwikkeld door het Basels Comité voor Bankentoezichthouders, zijn in de Europese Unie geïmplementeerd door middel van de Capital Requirements Directive. Lidstaten zijn verplicht de directieve over te nemen in hun nationale wetgeving. In Nederland is dit gebeurd door de Baselse richtlijnen over te nemen in de Wft en daaraan gerelateerde lagere regelgeving. Ook de Regeling Organisatie en Beheersing (ROB), het beheersingskader van De Nederlandsche Bank (DNB), richt zich op beheersingsmaatregelen op verschillende risicogebieden.

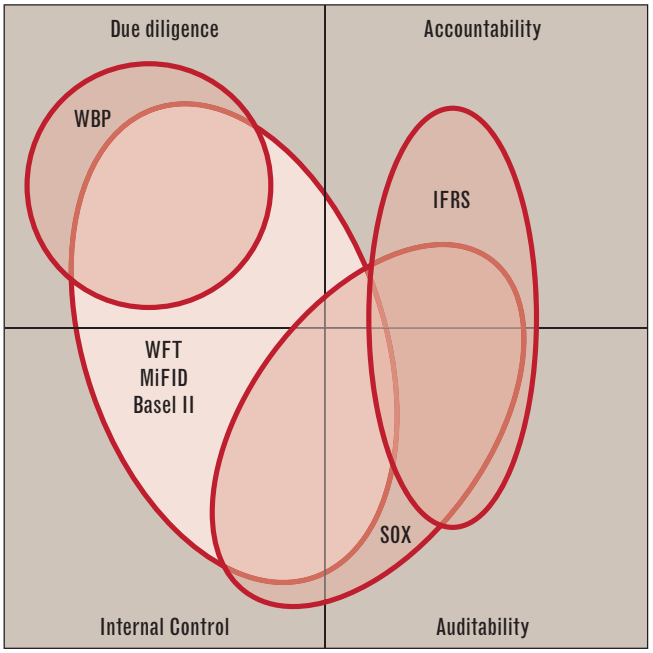
De Wft en onderliggende regelgeving richt zich met name op de zorgplicht van de financiële onderneming en beoogt transparantie voor de consument te creëren. De consument dient tijdig en juist geïnformeerd te worden over financiële producten. Daarnaast worden er eisen gesteld aan de deskundigheid en betrouwbaarheid van de financieel dienstverlener, de integriteit, en financiële zekerheid.

Integer handelen

Naast de hierboven genoemde wet- en regelgeving bestaan er nog veel andere wetten en interne dan wel externe regels waaraan financiële instellingen zich moeten houden. Vrijwel altijd zijn de elementen van deze wetten en regels echter terug te brengen tot het integer handelen, vergroten van de transparantie en terugdringen van risico's. Kijken we naar het totaalplaatje aan wet- en regelgeving in de financiële sector, dan komen we tot een viertal kernelementen.

1. Due diligence.
Een financiële instelling dient op een juiste manier om te gaan met haar cliënten. Ze moet weten met wie ze zaken doet en daarvoor cliëntenonderzoek doen. Maar ook dient ze haar cliënten juist te classificeren, in te delen in risicogroepen en corresponderende maatregelen te treffen om risico's tegen te gaan. Privacy speelt een belangrijke rol op het gebied van bescherming van persoonsgegevens in financiële transacties en bij dossiervorming. Wetgeving stelt eisen aan het beleid ten aanzien van gegevensbehandeling en consumenten dienen op accurate wijze voorgelicht te worden.

2. Accountability.
De administratieve organisatie dient op orde te zijn: de financiële instelling dient aan te kunnen geven hoe de processen lopen binnen de organisatie en hoe er beoordeeld wordt. Het kernpunt is aansprakelijkheid, waarbij taakduidelijkheid en feedback factoren zijn. Daarnaast is individuele verantwoordelijkheid belangrijk.
Jaarcijfers en jaarverslagen dienen een waarheidsgetrouwe weergave te zijn van de situatie waarin het bedrijf verkeert. Het bestuur van de organisatie kan in bepaalde gevallen hoofdelijk aansprakelijk worden gehouden voor wat betreft de volledigheid en juistheid van de informatie.



Afbeelding 1: Kernelementen wet- en regelgeving in de financiële sector.

3. Auditability.
In veel wet- en regelgeving wordt het steeds belangrijker dat informatiesystemen een volledig traceerbaar proces volgen. Audit trails zorgen er voor dat output volledig gereproduceerd kan worden. Transparantie op het gebied van besturing, risicobeheersing, en financiële prestaties verdient hierbij de meeste aandacht. Deze transparantie zorgt er voor dat de externe toezichthouder en accountant een goed zicht hebben op de bedrijfsvoering.

4. Internal control.
Bedrijven dienen hun processen op dusdanige wijze te beheersen dat wetten en regels niet overtreden worden. Bedrijven worden geacht te documenteren wat men doet binnen het bedrijf en aan te tonen dat ook gewerkt wordt volgens vastgestelde procedures en vastgesteld beleid. Bij een geconstateerd incident dient het bedrijf zelf corrigerende maatregelen te kunnen treffen. Hier speelt met name de interne controle een belangrijke rol.

BPM aspecten & onderdelen van de scan

De bovengenoemde kernelementen van wet- en regelgeving stellen eisen aan een scala van BPM-aspecten. De kernvraag die de ontwikkelde scan probeert te beantwoorden is: in hoeverre is de BPM-functie in een organisatie ingericht om de eisen ten aanzien van compliance en risk te ondersteunen? Deze aspecten en hoe deze in de Sustainable BPM-scan zijn meegenomen bespreken we hieronder.

Processen.
De eisen die vanuit de wetgeving gesteld worden aan de processen hebben met name betrekking op vastlegging ten behoeve van interne controle. Bedrijven zijn verplicht hun processen, organisatie-inrichting en beheersingsmechanismen vast te leggen.
Hierbij dient de actuele situatie weergegeven te kunnen worden. Het moet tevens duidelijk zijn welke documenten opgeslagen worden in deze processen en welke koppelingen er gemaakt zijn met organigram, bedrijfsdoelstellingen en prestatiemetingen.
De Sustainable BPM-scan gaat daarom in op de manier waarop processen gedocumenteerd worden, hoe de onderlinge samenhang vastgelegd is en of de verschillende eisen van wetten en regels aansluiten bij de processen. Tevens is er aandacht voor de mate van detail in de procesvastlegging.

Privacy.
Op het gebied van privacy dienen in de processen maatregelen getroffen te worden om persoonsgegevens te beschermen bij alle transacties die binnen de processen plaatsvinden. Daarom gaat de Sustainable BPM-scan in op het doel ten behoeve waarvan deze persoonsgegevens vastgelegd en verwerkt worden, hoe deze gegevens dan vastgelegd worden en hoe ze beveiligd worden.

Risico's.
Zoals eerder bij Kernelementen wet- en regelgeving is beschreven, richt vrijwel alle wetgeving zich in ieder geval op risicobeheersing. Er ligt hierbij een grote nadruk op verschillende soorten risico's, waaronder kredietrisico, ofwel het risico dat de tegenpartij niet aan zijn betalingsverplichtingen kan voldoen, en allerlei vormen van operationeel risico. Hierbij kan gedacht worden aan het afdekken van risico op ongewenst menselijk gedrag, zoals fraude en het niet delen van kennis, of aan de beveiliging van computersystemen. Bedrijven dienen voldoende aandacht te besteden aan risicoanalyse: risico's dienen geïdentificeerd, bewaakt en beheerst te worden. De risicobeheersing en vastlegging dient zo ingericht te zijn dat er volledig, juist en tijdig geanticipeerd kan worden.
De Sustainable BPM-scan gaat in op de aansluiting tussen de risico's die gelopen kunnen worden volgens wet- en regelgeving en de door de financiële onderneming geïdentificeerde risico's, op de risicocoördinatie binnen het bedrijf, de communicatie omtrent risico's en de externe oriëntatie.

Maatregelen.
Om de risico's goed te kunnen beheersen dienen er interne controlemaatregelen te zijn opgesteld. Deze maatregelen moeten zorgvuldig afgestemd zijn op de risico's om zo de juiste risico's af te dekken en dit op de juiste manier te doen. De genomen interne controlemaatregelen moeten zich focussen op autorisatie, validatie en de (beperking van) toegang tot gegevens. Meer algemeen wordt van bedrijven gevraagd om het beleid rondom compliance vast te leggen in handboeken en procedures. De Sustainable BPM-scan checkt de aanwezigheid van deze documentatie. Qua maatregelen wordt er gekeken naar volledigheid, documentatie, en publicatie.

Bewaking.
Zoals gesteld dienen bedrijven aan te tonen hoe gewerkt dient te worden, maar men moet ook inzichtelijk maken dat er wordt gecontroleerd of de vastgelegde processen en procedures ook nageleefd worden op de werkvloer. Aspecten die hier een rol in spelen zijn het verzamelen, vastleggen en verwerken van gegevens, het verstrekken van informatie ten behoeve van het besturen van de organisatie en het afleggen van verantwoording door diverse functionarissen.
De Sustainable BPM-scan gaat daarom in op interne audits en wat er wordt gedaan met de resultaten van de interne audits. Tevens gaat de scan in op de vastlegging van processen en procedures en hoe er wordt bijgestuurd wanneer de uitvoering van de processen afwijkt van de documentatie.

Beheersing.
Om te kunnen blijven voldoen aan wet- en regelgeving is de inrichting van de beheersorganisatie rondom BPM van groot belang. De externe omgeving van het bedrijf dient voortdurend in de gaten gehouden te worden en nieuwe ontwikkelingen dienen te worden vertaald naar eisen die gesteld worden

aan de BPM-inrichting. Vervolgens dient de BPM-inrichting gescreend te worden om vast te stellen of zij nog steeds voldoet. Aspecten waarnaar gekeken wordt zijn of prestaties worden gerapporteerd, vastgelegd en teruggekoppeld. Centraal toezicht op, en ondersteuning van, processen zijn tevens belangrijke aspecten. De scan gaat daarom in op waar de verantwoordelijkheid belegd is ten aanzien van procesbeheer en op het toezicht op procesbeheer en compliancekwesties.
Tevens is er aandacht voor het proces dat gevolgd wordt wanneer er onregelmatigheden in de processen worden geconstateerd.

Tooling.
BPM-tools kunnen helpen om transparantie aan te brengen ten behoeve van de te houden audit. Vrijwel alle software biedt de mogelijkheid snel inzichtelijk te maken op welke manier gewerkt dient te worden. De controlerende instantie of auditor kan hiervan gebruik maken bij het beoordelen of er binnen de door de wet gestelde kaders gewerkt wordt.
De Sustainable BPM-scan gaat daarom in op de consistentie in tooling die wordt gebruikt. Tevens wordt gekeken in hoeverre vastlegging binnen het hele bedrijf plaatsvindt en of dit te allen tijde op dezelfde manier gebeurt. Tenslotte wordt er bij het aspect van tooling nog ingegaan op de flexibiliteit van de gebruikte methode van vastlegging.

Resultaten van de scan

De Sustainable BPM-scan is reeds uitgevoerd bij enkele financiële instellingen, zijnde banken en een verzekeraar. De scan bestaat uit een vragenlijst die is ingevuld door werknemers die in hun dagelijks werk nauw betrokken zijn bij compliance en risicobeheersing.

> De scan maakt direct duidelijk waar de zwakke plekken liggen

De belangrijkste bevindingen zijn dat alle geïnterviewde instellingen voldoen aan de gestelde eisen binnen verplichte wet- en regelgevingen. Deze eisen zorgen ervoor dat instellingen veel aandacht besteden aan intern toezicht. Voor het dragen van de verantwoordelijkheden die hiermee gemoeid zijn wordt er regelmatig gerapporteerd aan de directie. Er zijn verschillende bedrijven die de benodigde data voor compliance hebben vastgelegd in systemen en documentatie. Wanneer er signalen komen van audit, risk- en compliance management dat er tekortkomingen zijn, dan worden deze besproken met de directie en worden er maatregelen getroffen, zoals het communiceren van wijzigingen of het geven van trainingen.
Over het algemeen is de privacy van cliënten goed gewaarborgd: op het gebied van gegevensbescherming wordt de wet door de organisaties over het algemeen op een correcte wijze nageleefd. De instellingen maken gebruik van beveiligde archieven, toegangsbeveiligingen, authenticatie en andere gebruikelijke maatregelen om risico's te beperken.

Niet alle instellingen zijn even ver met het voldoen aan sustainable compliance. Er zijn instellingen die de processen, organisatie-inrichting en beheersingsmechanismen niet systematisch en op een toegankelijke wijze hebben vastgelegd, waarbij ook niet duidelijk is of de organisatie controlemaatregelen in processen heeft geïncorporeerd die systematisch plaatsvinden. Daarnaast zijn er ook geen standaard procedures zoals interne audits. De bestuurders en managers worden veelal voorzien van rapportages inclusief kengetallen over de bedrijfsprocessen om de risico's te beperken. Deze processen geven geen inzicht in de wijze waarop de output en throughput tot stand zijn gekomen, maar alleen een indicatie. Ook over de oorzaken van het herhaaldelijk controleren en corrigeren van gegevens wordt niet gerapporteerd.
Uit het onderzoek blijkt dus dat de instellingen vooral op zoek zijn naar 'in control' zijn en blijven, risicobeheersing en integere bedrijfsvoering.

De toepasbaarheid van de Sustainable BPM-scan

De Sustainable BPM-scan stelt een organisatie in staat relatief snel inzicht te verkrijgen in de stand van zaken binnen het eigen bedrijf op het gebied van BPM en (sustainable) compliance. Het beeld dat de scan oplevert moet echter wel gezien worden in de context van de specifieke financiële instelling.
De scan is weliswaar ontwikkeld als basis voor alle financiële instellingen, maar er blijven verschillen bestaan tussen de ene financiële instelling en de andere. Denk hierbij aan interne regelgeving en 'best practices' die extra eisen stellen aan de processen of bijzondere wetten waar een bedrijf aan moet voldoen, die niet zijn meegenomen in de huidige vorm van de scan. Verder geeft de Sustainable BPM-scan een analyse van de organisatie en de verbeterpunten, maar zorgt er niet voor dat het geheel geïmplementeerd wordt en vertelt niet hoe dit gedaan moet worden.

De scan maakt wel direct duidelijk waar de zwakke plekken liggen. Het voordeel is dus dat er snel een oordeel geveld kan worden over welke onderdelen van BPM goed zijn ingericht.
De resultaten van de scan geven ook aan waar nog het een en ander verbeterd kan worden om een goede basis ten aanzien van BPM neer te zetten. Kortom, de Sustainable BPM-scan geeft de financiële instelling direct een beeld van wat er nog gedaan moet worden op het gebied van BPM, om nieuwe wetten en regelgeving makkelijker en sneller te kunnen implementeren.

Coen de Hoon en Cathelijne Snuverink
Coen de Hoon (coen.de.hoon@capgemini.com) is senior consultant bij Capgemini.
Cathelijne Snuverink (cathelijne.snuverink@capgemini.com) is consultant bij Capgemini.