Data Driven Compliance

Patrick Özer MSc en Thom Eijken MSc

De hoeveelheid wet- en regelgeving en daarmee compliancethema's nemen steeds meer toe en bedrijfsprocessen worden steeds complexer. Een groot deel van de complexiteit en inspanning die het kost om naleving van wet- en regelgeving te toetsen ontstaat doordat er in compliancesilo's wordt gewerkt. De huidige stand van de techniek maakt het echter mogelijk om te kiezen voor een overkoepelende en gegevensgerichte benadering. In dit artikel wordt het concept van Data Driven Compliance toegelicht, waarmee het voldoen aan verschillende relevante wet- en regelgeving naar een hoger niveau wordt getild door het gegevensgericht toetsen en monitoren van transacties, processen en communicatie.

P. Özer MSc
is senior manager bij KPMG Advisory N.V.
ozer.patrick@kpmg.nl

T.A. Eijken MSc
is manager bij KPMG Advisory N.V.
eijken.thom@kpmg.nl

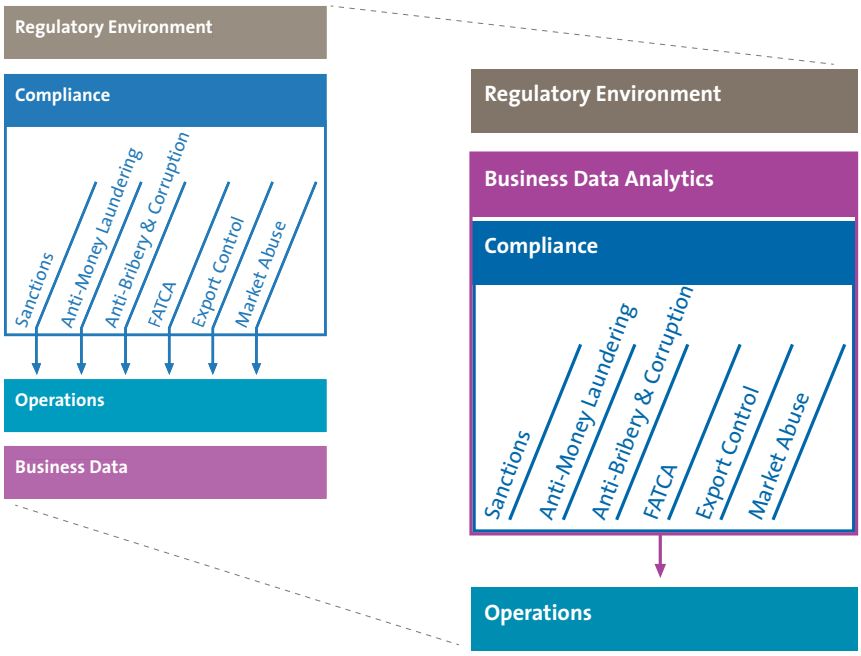
Inleiding

Het concept van Data Driven Compliance is ontstaan naar aanleiding van de 'miljoenen boetes' die grote internationale ondernemingen de laatste jaren hebben ontvangen. In de media zijn voldoende voorbeelden te vinden van dergelijke ondernemingen die enorme boetes hebben gekregen voor overtredingen of onvoldoende controle op omkoping en corruptie, kartelvorming, witwassen en het schenden van handelssancties. In de eerste helft van 2014 heeft de Office of Foreign Assets Control (OFAC) bijna $ 1.2 miljard aan boetes uitgedeeld voor overtredingen van sanctiewetgeving. Sinds 2008 zijn er boetes uitgedeeld voor omkoping en corruptie met afzonderlijke bedragen van € 100.000 tot meer dan € 1 miljard. Hadden deze ondernemingen geen compliance-programma of beheersingsmaatregelen ingesteld? Waarschijnlijk wel, maar toch is met onderzoek (door of in opdracht van de toezichthouder) in historische data non-compliance aangetoond. Het proactief monitoren op deze belangrijke 'compliancedata' had dus de non-compliance vroegtijdig kunnen signaleren en de miljoenen euro's aan boetes kunnen voorkomen.

Huidige stand van zaken

Complianceafdelingen van grote ondernemingen worden veelal bemand door medewerkers met een juridische achtergrond met veel kennis op het gebied van wet- en regelgeving. Er zijn weinig professionals met zowel een juridische achtergrond als een achtergrond in IT. Dit veroorzaakt een kloof tussen IT en compliance, waardoor men niet in staat is de reeds aanwezige omvangrijke databestanden met informatie over de mate van compliance in de bedrijfsvoering volledig te benutten.

Het proactief analyseren van gestructureerde compliancedata (bijvoorbeeld transactiegegevens of historische rentestanden) om aan te tonen dat een onderneming compliant is met wet- en regelgeving, wordt momenteel weinig toegepast. Dit terwijl bijvoorbeeld rentestandmanipulatie met de juiste analyses wel degelijk is aan te tonen. Het proactief analyseren van ongestructureerde data (bijvoorbeeld e-mailgegevens of voicedata) wordt op het moment niet of slechts beperkt toegepast.



Figuur 1. **Behalen van efficiëntie door overkoepelend control framework met integrale benadering.**

Compliancethema's zoals Anti-Money Laundering (AML), Anti-Bribery & Corruption en Foreign Account Tax and Compliance Act (FATCA) worden van oudsher individueel behandeld. Binnen complianceafdelingen van grote ondernemingen zijn vaak specialisten per thema werkzaam. Het voordeel hiervan is dat de complexe en veelvuldig veranderende materie beter ingevuld en bijgehouden wordt. Het nadeel is echter dat beleid en beheersingsmaatregelen in compliancesilo's binnen de onderneming worden uitgewerkt en het uitvoeren van deze maatregelen voor de operationele afdelingen binnen de onderneming een onnodig zware belasting kan zijn. Dit is grafisch weergegeven in

Figuur 2. **Algemeen compliancemonitoringproces.**

figuur 1 (links). Deze compliancethema's hebben ieder hun eigen beheersingsmaatregelen, zoals klantidentificatie, het screenen van relaties, het monitoren van communicatie of financiële transacties en ratio's. Hoewel er op detailniveau verschillen kunnen zijn in de wet- en regelgeving kan het ook een operationeel voordeel opleveren als er een overkoepelend control framework wordt ingericht en daarbij gebruik wordt gemaakt van een gegevensgerichte benadering. Dit laatste is ook weergegeven in figuur 1 (rechts).

Het overbruggen van de kloof tussen compliance en IT, het proactief analyseren van zowel gestructureerde als ongestructureerde data en het doorbreken van de individuele silo's is naar onze mening een grote stap richting het beter mitigeren van compliancerisico's. Dit noemen wij Data Driven Compliance.

Aanpak voor Data Driven Compliance

Het proces voor de inrichting van Data Driven Compliance is in figuur 2 in drie stappen weergegeven.

Risk Assessment

De eerste stap in de aanpak voor Data Driven Compliance is een lichte aanpassing op de traditionele risicogebaseerde benadering. In plaats van kans en impact, worden relevantie en compliancerisico tegen elkaar afgezet. Relevantie wordt bepaald door elementen als de sector, de jurisdictie en het wel of niet onder toezicht staan van de onderneming. Het compliancerisico wordt bepaald door de mate waarmee de onderneming het compliancerisico heeft afgedekt. Om het Risk Assessment-proces te begeleiden is er een app ontwikkeld waarmee een risicoprofiel kan worden bepaald. De app voert een quick-scan uit door middel van vragen die de relevantie van compliancethema's en compliancerisico's bepalen. Het resultaat wordt weerge-

Figuur 3. **Voorbeeld compliancerisicovraag (links) en (rechts) voorbeeld resulterende matrix op een vijftal compliancethema's.**

geven in een risicomatrix. Een voorbeeldvraag en resulterende risicomatrix zijn weergegeven in figuur 3.

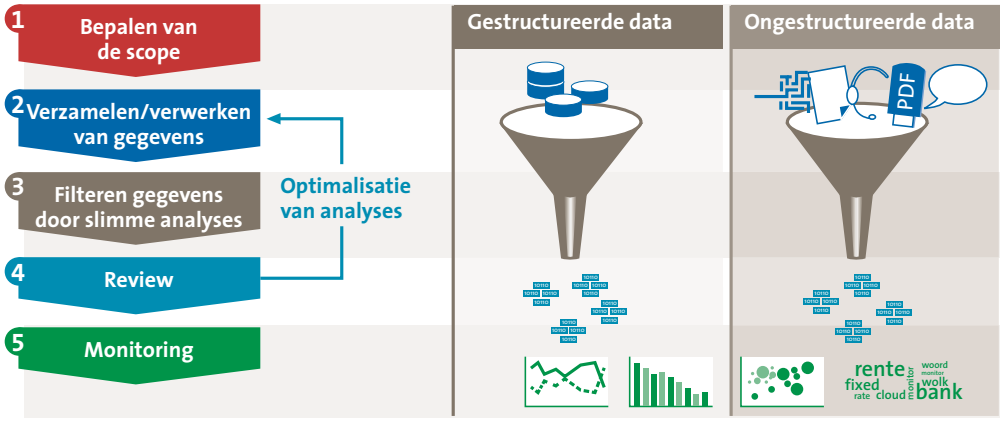
Identificatie van Key Compliance Indicatoren

Per compliancethema dat naar voren is gekomen uit de Risk Assessment kunnen Key Compliance Indicatoren (KCI) worden opgesteld die samen het niveau van compliance kunnen kwantificeren.

KCI's komen voort uit de wetgeving rondom de compliancethema's, uit doelstellingen van de onderneming of uit aanwijzingen van de toezichthouder. Een voorbeeld van een KCI is het aantal transacties dat heeft plaatsgevonden naar gesanctioneerde landen zoals Iran en Cuba. Dit soort transacties is vanuit de sanctiewetgeving beperkt toegestaan. Een ander voorbeeld met betrekking tot communicatie van medewerkers is de aanwezigheid van termen die relateren tot schendingen van wet- en regelgeving, zoals *'gaan we regelen'*, *'prijs'* of *'omzeilen'*.

Compliancemonitoring

Tot zover nog geen technisch of complex verhaal. De kracht van Data Driven Compliance is eerder beschreven als het overbruggen van de kloof tussen compliance en IT, het proactief analyseren van zowel gestructureerde als ongestructureerde data en het doorbreken van barrières tussen individuele compliancesilo's. De eerste twee hiervoor genoemde stappen gaan over het doorbreken van de barrières tussen de verschillende compliancesilo's. Bij de derde stap gaat het vooral om de proactieve analyse van data en het slaan van een brug tussen compliance en IT. Hier moeten namelijk de eerder opgestelde KCI's berekend worden op basis van grote hoeveelheden gegevens die in diverse hoeken van de IT-infrastructuur zijn opgeslagen. Gezien de moeilijkheidsgraad om dit te bewerkstelligen, zullen we hier nader op ingaan in het vervolg van dit artikel. De compliancemonitoringstap in figuur 2 kan in vijf onderdelen worden verdeeld. Deze zijn visueel weergegeven in figuur 4.



Figuur 4. **Het omzetten van 'compliancedata' naar compliancemonitoring.**

De uitdaging ligt in het definiëren hoe non-compliance tot uiting komt in ongestructureerde data

Bepalen van de scope

De eerder opgestelde KCI's dienen verder uitgewerkt te worden in technische vereisten, waarin de koppeling wordt gelegd naar data. Deze data kan worden gecategoriseerd in gestructureerde data en ongestructureerde data. Gestructureerde data varieert van Excel en ERP tot systemen die logs van fysieke toegangspoorten vastleggen. Met reeds beschikbare analysetools kan vaak al relatief snel inzicht in deze data verkregen worden. Bij ongestructureerde data gaat het om bijvoorbeeld e-mail, documenten, chatberichten (zoals Lync, Reuters of Bloomberg chat), sociale media en zelfs opgenomen telefoongesprekken. In bepaalde gevallen is non-compliance vooral te ontdekken in ongestructureerde data (zoals bij communicatie ten behoeve van het manipuleren van rentestanden), waarbij in andere situaties gestructureerde data de signalen van non-compliance zal bevatten (zoals transacties naar gesanctioneerde landen of organisaties). Om deze reden is de combinatie van gestructureerde data en ongestructureerde data essentieel.

Het is van belang om voldoende tijd te besteden aan het bepalen welke brongegevens relevant zijn en daarin weloverwogen keuzes te maken. Het achteraf wijzigen van deze scope leidt namelijk tot een additionele investering van tijd en kosten die vaak vele malen groter is dan wanneer dit van tevoren al bekend was.

Als het gaat om communicatie, dan bevinden aanknopingspunten voor non-compliance op basis van onze ervaring zich met name in de informele kanalen (bijvoorbeeld chat, sms of WhatsApp) omdat men vaak de formele communicatiekanalen (zoals e-mail) probeert te omzeilen.

Verzamelen en verwerken van gegevens

Om compliancemonitoring te kunnen uitvoeren dient de brondata op periodieke of continue basis te worden ontsloten. Het verdient aanbeveling om deze gegevens vervolgens in één omgeving samen te brengen. Hierdoor kunnen op een later moment analyses gebruikmaken van meerdere bronnen en heeft men bij het vinden van non-compliancesignalen direct toegang tot alle daaraan verwante gegevens (zoals communicatie die rond hetzelfde tijdstip heeft plaatsgevonden).

Om inzicht te kunnen verkrijgen in de ontsloten gegevens is er vaak een aantal voorbewerkingsslagen vereist. Dit is een bekend concept binnen het data-analysedomein, met het verschil dat de monitoring van compliance veelal betrekking heeft op grote hoeveelheden ongestructureerde data. Om hier inzicht in te verkrijgen en analyses op te verrichten kunnen technieken worden ingezet uit de forensische wereld. Met deze zogenaamde 'eDiscovery tools' kan er een voorverwerking plaatsvinden op bijvoorbeeld grote hoeveelheden e-mails, chatberichten en audiobestanden waardoor men zeer efficiënt dergelijke bestanden kan doorzoeken.

Filteren van gegevens door slimme analyses

Tijdens de analysestap dienen de KCI's vertaald te worden naar technische zoekslagen welke op periodieke of continue basis zullen worden uitgevoerd. Bij de monitoring van compliance ligt de uitdaging in het definiëren hoe non-compliance tot uiting komt in ongestructureerde data. Dit kan bijvoorbeeld door zoekwoorden toe te passen die men in geval van non-compliance verwacht aan te treffen in communicaties van medewerkers. Een belangrijke afweging in dit proces is dat de zoekwoorden breed genoeg gedefinieerd moeten worden om spelfouten, afkortingen of codetaal te kunnen ondervangen, terwijl de keerzijde is dat te breed gedefinieerde zoektermen kunnen leiden tot grote hoeveelheden 'false positives'.

Review

Review wordt over het algemeen gezien als een manuele en tijdrovende stap. Bij ongestructureerde data is het een belangrijk onderdeel om beter inzicht in de data te verkrijgen en het reduceren van 'false positives'. Daarnaast levert de review input voor een feedback-loop waarmee de precisie van de zoekwoorden verhoogd wordt. Na verloop van tijd kunnen slimmere algoritmes ontwikkeld worden waardoor de tijd benodigd voor reviewwerkzaamheden drastisch omlaag wordt gebracht. Een voorbeeld hiervan is het uitsluiten van resultaten die meldingen opleveren door aanwezigheid van termen als 'omkoping', terwijl de desbetreffende communicaties gaan over het interne beleid van de onderneming. Daarnaast kunnen tijdens de review ook patronen of codewoorden ontdekt worden, die medewerkers gebruiken om ontdekking te voorkomen, waarmee vervolgens de analyses ook weer geoptimaliseerd worden.

Monitoring

Het resultaat van voorgaande stappen is het monitoren van de compliancerisico's van de onderneming door middel van een compliance-dashboard. Dit dashboard

biedt een visuele helikopterview op de KCI-data en helpt daarmee overzicht te creëren. Hierdoor ontstaat real-time inzicht in wat compliant en non-compliant is. De hiervoor beschreven werkwijze maakt het ook mogelijk om vanuit het dashboard door middel van 'drill-down' in de details te duiken. Zo worden afwijkingen zichtbaar en is gericht ingrijpen vroegtijdig mogelijk waardoor boetes en sancties voorkomen worden. Het dashboard kan geïntegreerd worden in bestaande KPI's van de onderneming, waardoor het belang van KCI's weer wordt gestimuleerd.

Casus

Probleemstelling

Veel internationale financiële instellingen hebben in de afgelopen jaren te maken gehad met de manipulatie van rentestanden die plaatsvond binnen de eigen bedrijfsvoering en de daarmee gemoeide boetes van autoriteiten uit diverse landen. Hierdoor is een behoefte ontstaan om de communicatie van medewerkers op de handelsvloer op continue basis onder de loep te nemen zodat er bij een incident direct ingegrepen kan worden.

De hoeveelheid communicatie die in de gemiddelde internationale financiële instelling op dagelijkse basis plaatsvindt, is echter enorm. Medewerkers sturen honderden e-mails per dag, zijn continu via chatprogramma's in gesprek met collega's en hebben vaak meerdere telefoonlijnen tot hun beschikking. Dit leidt ertoe dat de hoeveelheid gegevens die dagelijks dienen te worden verzameld vanuit deze diverse media, tot in de terabytes loopt en vaak verspreid is opgeslagen over verschillende locaties en IT-systemen. Naast dat de real-time verzameling van deze gegevens een complex vraagstuk is, is het onrealistisch om met alle communicaties mee te lezen of luisteren.

Aanpak

Voor een specifieke internationale financiële instelling hebben wij de volgende aanpak gehanteerd. De aanpak voor de monitoring van communicaties volgde de stappen zoals uitgebeeld in figuur 4. De bepaling van de scope vond initieel plaats en de daaropvolgende stappen werden op continue basis uitgevoerd. Tijdens de implementatie van deze stappen moesten er verschillende afwegingen gemaakt worden. Zo kon de instelling enerzijds het proces van verzamelen, verwerken en reviewen van de communicaties volledig uit handen geven aan een externe partij. Anderzijds konden ze dit proces inregelen binnen de organisatie van de financiële instelling zelf. Een belangrijk voordeel van het uit handen geven was dat de monitoring zeer snel operationeel kon zijn en uitgevoerd zou worden door professionals die hier reeds meerdere jaren ervaring mee hadden. Hierbij kwam wel een extra stuk complexiteit kijken omdat er rekening gehouden moest worden met interne en externe privacyregels.

Bij het intern inregelen van het proces kon de financiële instelling zelf de benodigde kennis en ervaring opbouwen en intern delen en konden medewerkers opgeleid worden voor het uitvoeren van de technische en reviewwerkzaamheden. Hier zou echter meer tijd mee gemoeid zijn en dit zou ook een investering vereisen in de aanschaf van nieuwe technologie, de aanpassing van de bestaande IT-infrastructuur en de opleiding van medewerkers.

Toegevoegde waarde voor de klant

De financiële instelling in kwestie heeft ervoor gekozen om van beide voornoemde oplossingen gebruik te maken. Om op de korte termijn inzicht te hebben in mogelijke complianceovertredingen, heeft de instelling de externe partij gevraagd direct te beginnen met het monitoren van communicaties van handelaren. Ondertussen kan vervolgens gewerkt worden aan het opzetten van een monitoringproces binnen de onderneming zelf en het trainen van de eigen medewerkers.

De communicatie van honderden medewerkers wordt op dit moment op real-time basis gescreend en gereviewd op non-compliance. Dit biedt de mogelijkheid om continu controle te hebben over mogelijke complianceovertredingen. Verzoeken vanuit autoriteiten hoeven daardoor niet meer tot verrassingen te leiden en miljoenenboetes en daarbij behorende reputatieschade kunnen zodoende worden voorkomen. Monitoring heeft ook een preventieve werking zodra medewerkers op risicovolle posities weten dat er gemonitord wordt.

Monitoring heeft ook een preventieve werking zodra medewerkers op risicovolle posities weten dat er gemonitord wordt

Voordelen

De voordelen van de beschreven aanpak spreken voor zich: ondernemingen vermijden boetes van toezichthouders, reputatieschade, en creëren synergievoordelen door de naleving van (extraterritoriale) wetgeving integraal te realiseren. Het bieden van transparantie op basis van data zal, naast het in-control zijn en het inzicht verschaffen, in toenemende mate van invloed zijn op de reputatie en het succes van ondernemingen. Het is een aanpak die de vereisten van toezichthouders vooraf in kaart brengt en de naleving ervan aantoonbaar maakt. Met andere woorden, compliant en 100% transparant zijn doordat alle relevante feiten bekend zijn.

Conclusie

In dit artikel is een concept beschreven dat ondernemingen kan helpen met het beter beheersen en meten van hun compliancerisico's. Toegelicht is hoe er, in tegenstelling tot hoe voorheen deze risico's per compliancethema werden behandeld, efficiëntievoordeel behaald kan worden door specifieke vereisten binnen thema's te combineren en gebruik te maken van de overlap die deze thema's bevatten.

Er is stilgestaan bij de hoeveelheid compliancedata die een onderneming registreert of kan registreren. Door gerichter gebruik te maken van deze data kunnen ondernemingen aantoonbaar maken dat ze compliant zijn met bepaalde wet- en regelgeving. Is dit niet het geval, dan kunnen ze non-compliance proactief adresseren en daarmee hoge boetes of reputatieschade vermijden.

Door op een andere wijze naar data te kijken en door naast gestructureerde data ook ongestructureerde data te analyseren, kan de vraag 'hoe compliant is mijn onderneming' beter beantwoord worden. Door real-time te monitoren op communicatie kan non-compliance vroegtijdig gedetecteerd worden, terwijl dit met traditionele methoden pas naar voren zou komen wanneer het te laat is.

Over de auteurs

P. Özer MSc is senior manager in het Forensic Technology team van KPMG Advisory N.V. Hij heeft een achtergrond in de kunstmatige intelligentie en heeft meer dan zeven jaar ervaring met het uitvoeren van fraudeonderzoeken vanuit een IT-perspectief. Hij heeft ruime ervaring met data mining, computer forensics en corporate intelligence. Zijn laatste onderzoeken waren gericht op regulatory compliance waarbij grote hoeveelheden historische data gebruikt zijn om (non-)compliance aan te tonen.

T.A. Eijken MSc is manager in het Forensic Technology team van KPMG Advisory N.V. Hij heeft een achtergrond in de bedrijfswiskunde en informatica en heeft bijna vijf jaar ervaring met het uitvoeren van fraudeonderzoeken vanuit een IT-perspectief. Zijn focus ligt op het toepassen van innovatieve technieken, zoals visualisatie en predictive analytics, om betere inzichten te verkrijgen voor de klanten van KPMG. Recentelijk heeft hij de technische implementatie van een compliancemonitoring-proces gecoördineerd.

Door real-time te monitoren op communicatie kan non-compliance vroegtijdig gedetecteerd worden