

**ATTENTIE!
VERBODEN
TE LEZEN
TIJDENS
WERKTIJD!**



Governance geautomatiseerd

ERP-software is oorspronkelijk bestemd om de administratie van bedrijfsprocessen te integreren en efficiënter te maken. Maar diezelfde software kan ook worden ingezet om de compliance-activiteiten in een bedrijf te verbeteren. De top van het bedrijf is zich hiervan nog onvoldoende bewust en durft nauwelijks te steunen op geautomatiseerde beheersmaatregelen. Een mooie uitdaging voor de CIO om deze aanpak te promoten.

Door Suzanne Janse en Arne ter Laak

Governance en compliance zijn 'buzzwords'. Veel multinationals moeten voldoen aan de Amerikaanse Governance Wetgeving, Sarbanes Oxley (SOX), en ook binnen Nederland gelden regels op het gebied van Corporate Governance, de code-Tabaksblad.

Het management moet de interne beheersing op orde krijgen en aantoonbaar maken. Dat vergt doorgaans veel inspanning en brengt hoge kosten met zich mee. Compliance-activiteiten ontstijgen het ad hoc stadium maar langzaam. Jaarlijks is het een race tegen de klok om interne beheersing conform de gestelde richtlijnen aan te tonen. De toegevoegde waarde voor de organisatie is nog weinig zichtbaar. Daarom sporen Audit comités en executive management de compliance managers aan om projecten te versnellen en te

gelijkertijd kosten te minimaliseren. Reden om te onderzoeken of automatisering ook voor compliance activiteiten de efficiëntie en effectiviteit kan verbeteren.

Want hoewel ERP-software bestemd is om de administratie van bedrijfsprocessen te integreren en efficiënter te maken, kan diezelfde software vaak ook worden ingezet om de compliance-activiteiten in een bedrijf te verbeteren. ERP-software leent zich immers zeer goed voor het automatiseren van beheersingsmaatregelen en controles. En juist het automatiseren van controles kan significante voordelen opleveren. Door een juiste configuratie van controles in de applicatie, kunnen organisaties de inspanningen van personeel gericht op interne beheersing verminderen. Over het algemeen zijn

controles die een applicatie uitvoeren of afdwingen betrouwbaarder en duurzamer. En als controles goed zijn ontworpen, beveiligd en onderhouden, dan is het aantoonbaar maken van de werking van deze controles eenvoudiger en efficiënter. De kosten van jaarlijkse onderzoeken naar de effectiviteit van controlemaatregelen kunnen dan ook significant dalen.

Compliance-moe

Tijdrovende, handmatige, foutgevoelige onderzoeken door Interne Audit en Management worden vervangen door veel efficiëntere observaties van configuratie instellingen en parameters. De auditor kan immers steunen op deze instellingen in de applicatie. Ook budgetten voor de externe auditor kunnen actief worden gemanaged. De externe

auditor kan testresultaten opnieuw gebruiken en meer steunen op applicatiecontroles. Onderzoek wijst uit dat het testen van geautomatiseerde controles gemiddeld 75% minder tijd kost dan testen van handmatige controles. Van audit-budgetten zou gemiddeld 20% kunnen worden bespaard. Verder zijn medewerkers minder tijd kwijt aan het uitvoeren van, of het toezien op eentonige handmatige controles. En kan automatiseren van controles dus bijdragen aan plezier in het werk. Ten slotte leidt het verschuiven van controlemaatregelen naar de applicatie tot een kleinere kans op menselijke fouten en frauduleuze manipulaties door het afdwingen van consistentie en naleving van voorschriften. Veel organisaties zijn compliance-moe.

ste reden is dat softwareleveranciers, organisaties en consultants een ERP-systeem zo snel mogelijk willen implementeren. Er is vaak te weinig tijd om goed te kunnen bepalen welke controles en welk beveiligingsniveau moeten worden geconfigureerd. Dit resulteert veelal in tekortkomingen en inefficiënties achteraf.

Een andere reden dat organisaties de mogelijkheden van ERP-systemen nog maar beperkt benutten is de angst om op applicatiecontroles te steunen. Onzekerheid over de werking van de applicatie en controles leidt er toe dat organisaties blijven steunen op handmatige controles. Rond uitbestede applicaties is deze onzekerheid nog groter en daarom creëren organisaties handmatige controles om de betrouwbaar-

van deze controles stelt organisaties in staat deze kant op te gaan. Hier kan IT een belangrijke 'driver' zijn. De CIO mag deze kans niet voorbij laten gaan.

Aan de knoppen

Het internationaal gebruikte compliance raamwerk COSO definieert applicatiecontroles als volgt: "Geprogrammeerde procedures in applicatiesoftware en daaraan gerelateerde handmatige procedures, om de volledige en accurate verwerking van informatie te verzekeren."

Er zijn verschillende typen applicatiecontroles.

Om te beginnen **configureerbare procescontroles**, controles die de applicatie afdwingt. Het zijn 'knoppen' die ingesteld kunnen worden om gegevens te beschermen tegen onjuiste verwerking. Voorbeelden hiervan zijn verplichte velden, boekingslimieten, toleranties, autorisaties en uitzonderingsrapportages. Veel standaard software pakketten bieden de mogelijkheid om controles in overeenstemming met de bedrijfsprocessen te configureren.

Handmatige procescontroles die geschikt zijn voor automatisering. Hoe goed een applicatie ook is geconfigureerd, vaak gebruikt een organisatie handmatige controles om de betrouwbaarheid van met name financiële gegevens te waarborgen. Een voorbeeld van een handmatige controle is de afstemming en goedkeuring van facturen. Bedrijven zouden moeten overwegen om, waar mogelijk, handmatige controles 'om te zetten' naar systeemgebaseerde controles om de effectiviteit van de controle te vergroten alsmede de efficiëntie waarmee de controle kan worden gevalideerd.

Interface/integratie controles. Interfaces tussen applicaties vormen een bedreiging voor de betrouwbaarheid van gegevens, met name als die interface handmatig is. Controles moeten ingericht worden die de data-integriteit van de interface waarborgen. Deze kunnen de vorm aannemen van aansluitingsprocedures, mogelijk onder-

Het vergt een verregaande kennis van de ERP-functionaliteit om conflicten in functiescheidingen binnen een rol of tussen rollen te identificeren

In dat licht zitten de betrokken medewerkers en compliance teams niet te wachten op weer een verandering van de ingerichte interne controle structuur met veelal handmatige controles. De kansen en voordelen voor lange termijn kostenbesparingen zijn echter te groot om te negeren. Hoe meer bedrijfsprocessen en applicaties inhaken op het ERP-systeem, dat de bron is van financiële gegevens en rapportages, hoe meer aanleiding er is om handmatige controlemaatregelen naar de applicatielaag te verplaatsen en te 'automatiseren'. Uiteindelijk zal dat organisaties helpen om de compliance-activiteiten te verankeren en van de jaarlijkse ad hoc compliance-projecten te migreren naar een situatie waarin deze activiteiten deel uitmaken van het reguliere bedrijfsproces.

Er zijn verschillende redenen waarom organisaties het ERP-systeem nog maar beperkt benutten. De belangrij-

heid van de gegevens in het systeem te valideren.

De CIO heeft er een mooie uitdaging bij. Het automatiseren van controles en het automatisch monitoren van deze controles stelt ondernemingen in staat weer te focussen op de operatie en de efficiëntie daarvan. Verder kunnen controles in de systemen ook van toepassing zijn op allerlei risico's buiten compliance.

Belangrijke bedrijfsprocessen kunnen applicatiecontroles benutten om vele operationele risico's te beheersen, bijvoorbeeld door de implementatie van workflow automatisering en de bijbehorende monitoring controles. Deze mogelijkheid brengt organisaties een stap dichterbij Enterprise Risk Management. Enterprise Risk Management ontwikkelt zich tot een real time risk management proces. Automatisering en het volledig benutten van ERP-controles en automatische monitoring



steund door tools die de volledigheid en nauwkeurigheid van de interface monitoren.

Rapportage controles. Controlemaatregelen rond rapportages zijn belangrijk om de risico's te beperken dat gegevens worden gewijzigd gedurende het (financiële) rapportageproces. Alle hiervoor genoemde configureerbare applicatie- en interfacecontroles worden vergeefs als op dit punt een risico in het rapportageproces onverminderd blijft. Een alledaags voorbeeld is het downloaden van financiële gegevens van de applicatie voor financiële rapportage (bijvoorbeeld een ERP) naar een spreadsheet. De applicatiecontroles worden nu omzeild en aanvullende controlemaatregelen zijn nodig om de integriteit van de spreadsheetdata te waarborgen. Organisaties zouden ernaar moeten streven spreadsheet-functionaliteit zoveel mogelijk naar de ERP-omgeving over te brengen.

Autorisaties die functiescheiding binnen de applicatie afdwingen (Segregation Of Duties, ook wel SOD). Anders dan bij configureerbare controles, die zich richten op onjuistheid van gegevens door menselijke fouten, zijn autorisatie controles gericht op risico's als gevolg van onrechtmatige toegang en fraude. Voorbeeld van een belangrijke functiescheiding binnen een organisatie is 1) aanmaken van een verkoper en 2) het betalen van een verkoper. Een medewerker die beide transacties kan uitvoeren in een systeem zou een fictief bedrijf kunnen aanmaken en betalingen doen aan dit bedrijf. Een ander veel voorkomend probleem zijn medewerkers met onnodig veel toegangsrechten. Daarmee is het mogelijk om configureerbare controles te wijzigen, of zelfs autorisaties aan te passen.

Vermenigvuldigend effect

Welke controles komen in aanmerking voor automatisering? Automatisering maakt interne beheersing efficiënter en effectiever en maakt de aantoonbaarheid van deze interne beheersing eenvoudiger. Organisaties zouden de

beheersings- c.q. controlemaatregelen moeten identificeren waar automatisering de grootste winst oplevert. Zij kunnen daarbij de volgende criteria hanteren: 1) handmatige controles die duur zijn om uit te voeren en te testen, 2) controles die hoge c.q. materiële risico's met zich meebrengen wanneer ze niet werken, 3) controles die de externe accountant belangrijk vindt, zoals autorisaties en functiescheidingen, 4) foutgevoelige controles en 5) handmatige controles die repetitief zijn en waar weinig menselijke beoordeling en betrokkenheid voor nodig is.

Bedrijfsbrede, geïntegreerde oplossingen, zoals ERP-systemen, hebben extra toegevoegde waarde omdat controleverbeteringen vaak een vermenigvuldigend effect hebben. Voorbeeld hiervan is het onderhouden van autorisaties die door het hele systeem bestaan.

Autorisaties en functiescheidingen zijn een groeiend issue voor veel bedrijven met een ERP-systeem. Het opzetten en inrichten van het concept is erg lastig. Het vergt een verregeande kennis van de ERP-functionaliteit om conflicten in functiescheidingen binnen een rol of tussen rollen te identificeren. Hoewel veel organisaties inspanningen doen op dit gebied, stijgt het aantal voorbeelden van externe accountants die een onvoldoende gecontroleerde autorisatiestructuur 'materieel' genoeg vinden voor een opmerking bij de jaarrekening.

Het testen van applicatiecontroles verdient ook de nodige aandacht. Voor het testen van de applicatie is een juiste combinatie van testmethoden en technieken nodig. Over het algemeen zijn er twee primaire methoden om deze applicatiecontroles te testen: geautomatiseerd en handmatig, met semi-automatisch testen als tussenvorm.

Handmatig testen wordt vaak gezien als de 'makkelijkste' aanpak. De methode is doorgaans echter zeer tijdrovend, enerzijds vanwege het grote aantal scenario's dat nodig is voor het verzamelen van genoeg bewijs om het

effectief functioneren van de controle te kunnen valideren, anderzijds vanwege het grote aantal totaal te testen controles.

Daarnaast zijn vaak specifieke kennis en vaardigheden nodig om testcases te bouwen, testen goed uit te voeren, interactie te hebben met het bedrijfs-personeel en testresultaten juist te interpreteren.

Bovendien is bij het handmatig testen vaak toegang nodig tot een gesynchroniseerde omgeving om te garanderen dat de personen die de evaluatie uitvoeren, geen ongewenste toegang hebben tot, of invloed uitoefenen op de (live) productieomgeving.

Ten slotte is het belangrijk om op te merken dat, zoals bij elke handeling die wordt uitgevoerd door mensen, er altijd een vergrote kans is op menselijke fouten.

Al deze moeilijkheden van handmatige testtechnieken sluiten de werkzaamheid echter niet uit. Sterker nog, veel bedrijven gebruiken handmatige testtechnieken in hun omgeving, en zijn daarbij zeer succesvol. Echter, bij veel van deze bedrijven zijn, door het toegenomen gebruik van semi-geautomatiseerde en geautomatiseerde technieken, mogelijkheden voor het aanzienlijk verminderen van testactiviteiten en het verbeteren van de werkzaamheid.

Semi-automatisch testen door data extractie en analyse is vaak mogelijk voor een aantal applicaties. Gegevenstabellen kunnen als bewijs dienen dat controles op een bepaalde manier zijn geconfigureerd. Auditors kunnen eventueel handmatig een steekproef van de gegevenstabel testen op hun reikwijdte om te bevestigen dat wat de tabel aangeeft ook daadwerkelijk is geconfigureerd.

Geautomatiseerd testen kan vaak met behulp van geautomatiseerde tools die het testen kunnen vergemakkelijken en verbeteren. Sommige van deze tools kunnen een extractie van configuratie data uit de applicatie halen en deze gegevens automatisch analyseren.

Andere tools helpen een bedrijf bij het definiëren van instellingen transactieniveau, die vervolgens dienst doen als bewijs voor het functioneren van een bepaalde configureerbare controle. Ten slotte, zijn er recent de 'continuous monitoring' tools ontwikkeld. Deze helpen een bedrijf met het controleren van veranderingen in de van te voren gedefinieerde configuraties en transacties die een hoog risico voor het bedrijf opleveren.

Platformbreed

Veel ERP-software leveranciers hebben geïntegreerde tools ontwikkeld die het testproces ondersteunen. Ook kleinere software leveranciers hebben talloze producten op de markt gebracht. Bij het evalueren van software oplossingen moet rekening worden gehouden met specifieke bedrijfsbehoeften en functionele eisen. Zoals bij elke software-aankoop moeten ook de

beoordelingstools veel tijd kost. Veel bedrijven voelen zich overweldigd door de resultaten van de eerste beoordelingen van deze tools.

Om te garanderen dat de controleomgeving naar verloop van tijd steeds beter wordt moeten de tools worden geïntegreerd in het proces. Tools die maar een keer per jaar gebruikt worden voor een analyse, behalen vaak hetzelfde soort resultaat als voorgaande jaren, omdat de werkelijke oorzaak van problemen niet is geïdentificeerd en opgelost. Er zijn geen procesverbeteringen en preventieve controles geïmplementeerd om problemen op de lange termijn op te lossen. Tot slot is het belangrijk dat de mensen die de tools implementeren, configureren en toepassen, niet alleen kennis hebben van de tool, maar ook van de applicatie die wordt beoordeeld en de daaraan gerelateerde bedrijfsprocessen, risico's en controles.

Onvoldoende gecontroleerde autorisatiestructuur is 'materieel' genoeg voor een opmerking bij de jaarrekening

hardware-eisen en de bestaande infrastructuur worden meegenomen. Zo heeft een bedrijf dat meerdere ERP-systemen (zoals SAP en Peoplesoft) gebruikt, testsoftware nodig die platformbrede oplossingen bieden. Een bedrijf dat haar ERP-systeem volledig heeft geïntegreerd, kan waarschijnlijk beter kiezen voor een module die naadloos aansluit op het eigen systeem. Verder is het belangrijk om te realiseren dat geautomatiseerde compliance tools alleen niet de oplossing zijn. Ze vereisen, net als elk ander software pakket, gedegen planning en implementatie om zo goed mogelijk van toegevoegde waarde te zijn. Bedrijven die de aankoop van een compliance test tool overwegen, zouden in ieder geval goed moeten beseffen dat de verwerking van de eerste resultaten van de

Bronnen:

'Harness the Compliance Power of Your ERP Platform', John Harrison, Doug Papp, and Anthony Samer, Protiviti US, 2005

'Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls', Protiviti Inc. 2006

SUZANNE JANSE is manager en **ARNE TER LAAK** is senior manager bij Protiviti Nederland. Voor meer informatie en contactgegevens zie www.protiviti.nl