Auditing van single client ERP

Drs. R. van den Heuvel
is manager bij KPMG IT Advisory en betrokken bij een grote diversiteit aan audit- en adviesopdrachten rondom interne controle in SAP-omgevingen. Specifieke aandachtsgebieden zijn security, de logistieke en inkoopprocessen, continuous monitoring en GRC-tooling.

vandenheuvel.roeland@kpmg.nl

Drs. D. Hallemeesch
is manager bij KPMG IT Advisory en verantwoordelijk voor het aandachtsgebied SAP application security. Naast het ontwerpen, inrichten en beoordelen van autorisaties in SAP ligt een sterke focus op de implementatie van GRC-tooling en de uitrol van het SAP Netweaver Identity Management product.

hallemeesch.dennis@kpmg.nl

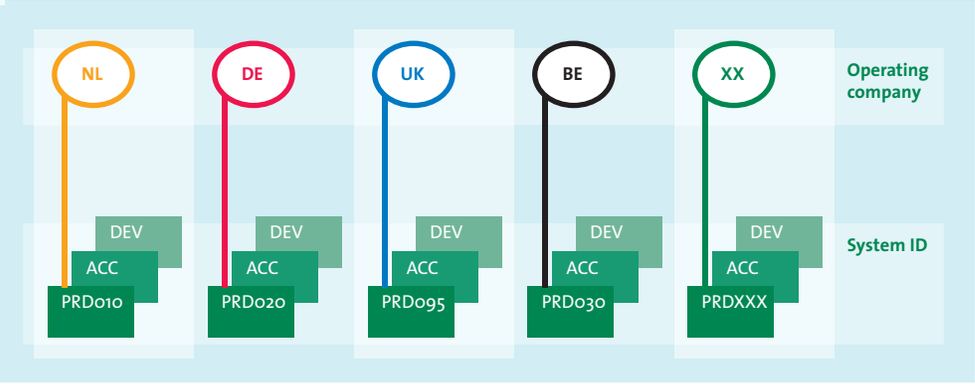
Drs. Roeland van den Heuvel en drs. Dennis Hallemeesch

Wij komen bij onze klanten steeds vaker in aanraking met zogeheten single client ERP-systemen, ofwel ERP-systemen waarin de klant de ERP-systemen van meerdere organisatie-entiteiten heeft ondergebracht in één overkoepelend ERP-systeem. Op het eerste gezicht lijkt er voor de auditor (en adviseur) weinig te veranderen, maar wanneer in meer detail wordt gekeken dient met een aantal specifieke aandachtspunten rekening te worden gehouden. In dit artikel gaan wij in op het fenomeen single client ERP-systeem en geven we een toelichting op de belangrijkste aandachtspunten.

Inleiding

De introductie van Enterprise Resource Planning (ERP)-systemen heeft bijgedragen aan de verschuiving van eilandautomatisering naar meer geïntegreerde systemen. Aan het eind van de jaren negentig hadden veel ondernemingen, al dan niet onder invloed van de hype die rondom ERP was ontstaan, een ERP-oplossing geïmplementeerd. In de loop der jaren bleek bij veel multinationals echter ook dat de afzonderlijke (nationale) organisatieonderdelen, ofwel de *operating companies* (afgekort tot OpCo) elk hun eigen ERP-systeem gebruikten. Het gebruik van verschillende ERP-systemen of het gebruik van hetzelfde ERP-systeem maar met verschillende versies of functionaliteit binnen één (multinationale) onderneming leidt tot een gebrek aan uniformiteit en standaardisatie van bedrijfsprocessen binnen de operating companies.

Een recente ontwikkeling is dat steeds meer (multinationale) organisaties kiezen voor het technisch samenvoegen van meerdere (en uiteindelijk alle) OpCo ERP-systemen in één ERP-systeem om zo de gewenste standaardisatie en efficiëntieverbetering na te streven. Het samenvoegen van meerdere ERP-systemen heeft echter ook mogelijk negatieve gevolgen. De risico's die in de oude situatie van toepassing waren op de bedrijfsprocessen van elke afzonderlijke OpCo (bijvoorbeeld inkoop, verkoop, financieel) zijn in de single client omgeving niet plotseling verdwenen. Het is echter nog maar de vraag of de internecontrolemaatregelen die in elke afzonderlijke OpCo geïmplementeerd waren, ook nog steeds toepasbaar en effectief zijn in de nieuwe single client omgeving. Naast dit beheersingsvraagstuk eisen nog vele andere aandachtsgebieden een rol, zoals het opzetten van het functionele en technische applicatiebeheer, het opzetten van een organisatiebreed beveiligingsconcept en het onderhoud van stamgegevens.



Figuur 1. **OpCo ERP-omgeving met eigen ERP-systeem per organisatieonderdeel.**

In dit artikel gaan wij in drie stappen verder in op single client ERP-systemen door eerst aan te geven wat 'single client' is, vervolgens de impact van het single client ERP-systeem op de interne beheersing (AO/IC) te beschrijven en tot slot in te gaan op de belangrijkste aandachtspunten van een single client ERP-systeem voor de IT-auditor.

De ontwikkeling van ERP naar single client ERP-systemen

De ontwikkeling van afzonderlijke ERP-systemen naar single client ERP heeft zich voltrokken in drie fasen, namelijk:

- afzonderlijke ERP-systemen per organisatieonderdeel – *OpCo ERP-systeem;*
- afzonderlijke ERP-systemen ingericht op basis van een template – *template ERP-systeem;*
- één ERP-systeem voor de gehele organisatie – *single client ERP-systeem.*

OpCo ERP-systeem

Het startpunt is de situatie waarin elke OpCo van een (multinationale) organisatie een eigen ERP-systeem heeft ingericht. Dit scenario komen wij in onze dagelijkse praktijk veelvuldig tegen, waarbij elke OpCo meestal sterk verschilt van de andere. Niet elke OpCo maakt gebruik van hetzelfde ERP-pakket en als dit wel zo is dan zijn er niet zelden verschillen in versienummer of gebruikte functionaliteit. Het gebruik van afzonderlijke ERP-systemen zonder concrete richtlijnen over de wijze waarop het ERP-systeem zal worden ingericht, noemen wij in dit artikel het OpCo ERP-systeem. In figuur 1 is deze situatie weergegeven.

Template ERP-systeem

Sommige organisaties, die de mogelijke problemen van losse ERP-systemen al vroeg onderkenden, kozen ervoor om een centrale template (ook wel *core* of *kernel* genoemd) te ontwikkelen waarin de belangrijkste functionaliteit van het ERP-systeem was opgenomen. Dit gaf een aanzienlijke verbetering in het gebruik van het ERP-systeem door de mogelijkheden voor standaardisering van de bedrijfsprocessen en de wijze waarop deze door het ERP-systeem worden ondersteund. Een belangrijke gedachte bij een template ERP-systeem is dan ook dat een onderneming die in verschillende landen hetzelfde product fabriceert, dezelfde processen heeft ingericht in elk van de landen. Immers, bijvoorbeeld de manier waarop een frisdrank wordt gemaakt in Nederland, is in de basis dezelfde als in Engeland[1]. Het gebruik van de template biedt de lokale OpCo een versnelde inrichting van het ERP-pakket. De template wordt uitgerold naar elke OpCo en mag waar nodig lokaal worden uitgebreid voor specifieke lokale processen.

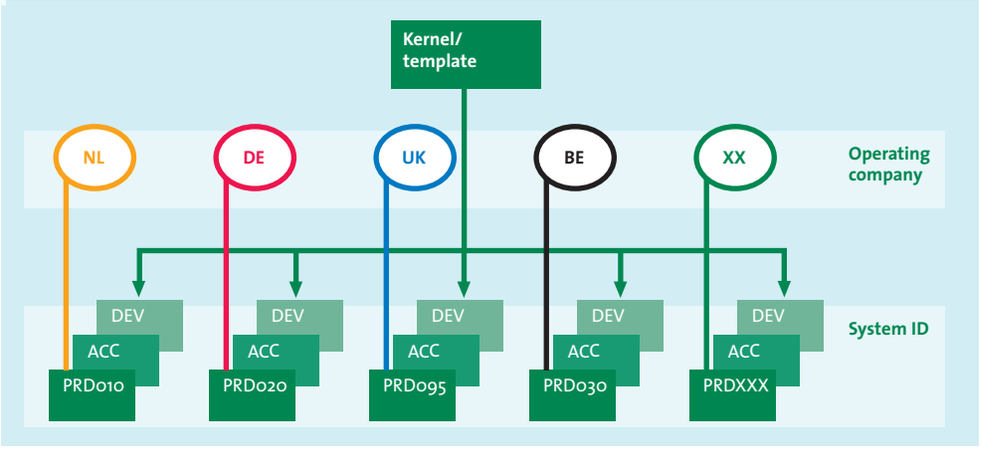
In figuur 2 staat de template ERP-omgeving weergegeven.

Single client ERP-systeem

Ondanks de voordelen van template ERP werkt de organisatie bij toepassing daarvan nog steeds met afzonderlijke ERP-systemen. De OpCo mag de applicatie in principe verder ontwikkelen en aanpassen, waardoor deze na verloop van tijd niet meer gelijk is aan de andere ERP-omgevingen. Een recente ontwikkeling is dan ook dat steeds meer (multinationale) organisaties kiezen voor het technisch samenvoegen van meerdere OpCo ERP-systemen in één overkoepelend single client ERP-systeem. In figuur 3 is een schematische weergave van het single client ERP-systeem weergegeven.

In tabel 1 worden de belangrijkste kenmerken van deze drie typologieën toegelicht aan de hand van de vier aandachtsgebieden 'Management en organisatie', 'Processen', 'Infrastructuur en beheerorganisatie' en 'Mensen en cultuur'.

1 Dit is tevens één van de redenen waarom SAP 'Industry Solutions' heeft ontwikkeld. Dit zijn SAP-systemen met voorgedefinieerde functionaliteit voor bepaalde bedrijfstakken. Voorbeelden hiervan zijn IS Healthcare, IS Oil, IS Telecom, IS Automotive en IS Consumer Products and Food.



Figuur 2. **Template ERP-omgeving met eigen ERP-systeem per organisatieonderdeel en sturing vanuit centrale template.**

De invloed van single client ERP op interne beheersing

De wijze waarop een organisatie wordt ingericht en waarop noodzakelijke stuur- en verantwoordingsinformatie wordt verkregen om de bedrijfsprocessen te kunnen besturen en beheersen ligt vast in de administratieve organisatie. Aangezien een single client ERP-systeem onderdeel is van deze inrichting heeft dit dus invloed op de administratieve organisatie.

Naast de administratieve organisatie heeft single client ERP ook invloed op het stelsel van interne controle, ofwel de wijze waarop het management via een gedegen proces- en risicoanalyse tot een stelsel van internecontrolemaatregelen komt en controleert of deze maatregelen hebben gewerkt.

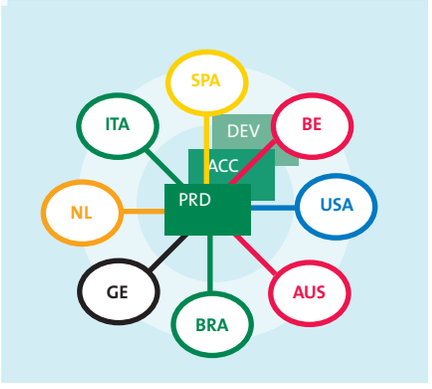
Single client ERP en de administratieve organisatie

De administratieve organisatie beschrijft de wijze waarop de organisatie van de informatievoorziening is ingericht en wordt voor dit artikel ingedeeld in de componenten *organisatiestructuur, processen en procedures, gegevensverzamelingen* en *controle- en beheersingsinformatie*. Het gebruik van single client ERP is een onderdeel van de administratieve organisatie en van invloed op de verschillende componenten.

Organisatiestructuur

De organisatiestructuur bevat het geheel van functies, afdelingen en personen inclusief een beschrijving van de taken en verantwoordelijkheden. Het gebruik van een single client ERP-systeem heeft invloed op zowel de gebruikersorganisatie als de IT-organisatie.

De succesvolle inrichting en invoering van een single client systeem betekent onder meer dat mogelijkheden bestaan voor



Figuur 3. **Single client ERP-omgeving met één ERP-systeem voor de gehele organisatie.**

het centraliseren van bepaalde activiteiten, zoals factuurinvoer of stamgegevensbeheer in daarvoor opgezette shared service centers. Deze shared service centers zullen dan bepaalde activiteiten zoals factuurinvoer, het uitvoeren van de betaalrun of het verwerken van salarissen centraal uitvoeren, waardoor op operating company-niveau deze taken en verantwoordelijkheden kunnen verdwijnen. Schaalvoordelen zijn door het gebruik van shared service centers op grote schaal mogelijk.

In de IT-organisatie vinden tevens veranderingen plaats. Door standaardisatie van de infrastructuur wordt de infrastructuur als geheel minder complex. Daarnaast hoeven er door het samenvoegen van meerdere ERP-systemen minder productieve systemen te worden beheerd. In OpCo ERP wordt elk lokaal ERP-systeem vaak nog door een lokale beheerorganisatie onderhouden. Voor single client ERP zal de organisatie in ieder geval het technisch beheer van de ERP-applicatie en bijbehorende infrastructuur dienen te centraliseren. Het beheer van een single client systeem kan dus efficiënter worden uitgevoerd dan wanneer meerdere OpCo ERP-systemen moeten worden beheerd. In dat geval zijn er immers meerdere lokale beheer-

Tabel 1. **Overzicht kenmerken ERP-technologieën.**

Aandachtsgebied	OpCo ERP	Template ERP	Single client ERP
Management en organisatie	• Ondersteuning OpCo-management bij maken strategische keuzen en beheersen en besturen van organisatie; hierbij wordt gebruikgemaakt van geïntegreerde managementinformatie. Tevens invloed op logistieke grondvorm van organisatie door op elkaar afstemmen van bedrijfsprocessen en ERP-systeem. • Op holdingniveau financiële gegevens van elke OpCo geconsolideerd. OpCo-management verantwoordelijk voor hele levenscyclus van ERP-systeem.	• Ondersteuning OpCo-management bij maken strategische keuzen en beheersen en besturen van de organisatie; hierbij wordt gebruikgemaakt van geïntegreerde managementinformatie. Tevens invloed op logistieke grondvorm van organisatie door op elkaar afstemmen van bedrijfsprocessen en ERP-systeem; hierbij is opgeleverde template uitgangspunt. • Op holdingniveau financiële gegevens van elke OpCo geconsolideerd. OpCo-management verantwoordelijk voor hele levenscyclus van ERP-systeem.	• Ondersteuning OpCo-management bij maken strategische keuzen en beheersen en besturen van organisatie; hierbij wordt gebruikgemaakt van geïntegreerde managementinformatie. Tevens invloed op de logistieke grondvorm van organisatie; single client-systeem bepaalt grotendeels hoe dit voor alle OpCo's eruit gaat zien. • Met behulp van de applicatie eenvoudig op holdingniveau gegevens te consolideren vanwege in systeem vastliggende gegevens. OpCo-management heeft geen volledige eigenaarschap meer over systeem doordat meerdere OpCo's gebruikmaken van systeem.
Processen	• Alle primaire en secundaire processen van OpCo te ondersteunen. Beslissing over te gebruiken functionaliteit en wijze waarop ERP bedrijfsprocessen gaat ondersteunen, ligt volledig bij OpCo-management.	• Alle primaire en secundaire processen van OpCo te ondersteunen. Beslissing over te gebruiken functionaliteit en wijze waarop ERP bedrijfsprocessen gaat ondersteunen, beïnvloed door template; hierin zijn belangrijkste bedrijfsprocessen geconfigureerd. Wanneer template niet alle lokale processen kan ondersteunen, mag OpCo zelf verder ontwikkelen op template. OpCo's kunnen van elkaar leren omdat basis van ERP-systemen dezelfde is.	• Processen zoveel mogelijk gestandaardiseerd; hierdoor mogelijk processen niet meer optimaal afgedekt door applicatie. Dit wordt vaak opgelost door maatwerk systeemaanpassing of door aanpassing bedrijfsprocessen. Soms gebruikgemaakt van shared service centers om voor alle OpCo's bepaalde processtappen voor hun rekening te nemen (bijvoorbeeld inkoop van ruwe materialen om kosten te besparen). Geld- en goederenstromen tussen OpCo's onderling eenvoudiger vast te leggen waardoor ook minder papierstromen en administratieve last. Zeer gedetailleerd en strikt wijzigingsproces noodzakelijk.
Infrastructuur en beheerorganisatie	• Eigen infrastructuur: eigen database en aparte server. OpCo kan zelf beslissen welke hardware en netwerkcomponenten ingezet worden. OpCo tevens zelf verantwoordelijk voor systeemconfiguratie, plannen van nieuwe systeemontwikkelingen en inrichting van de beheerprocessen (functioneel en technisch beheer).	• Eerste vorm van standaardisatie vindt plaats op hardwareniveau. Over het algemeen zullen OpCo's met zelfde versies van ERP-systeem werken en ook op zelfde typen databases en servers. Technisch beheer van applicatie vaak al centraal ingericht, met lokaal functioneel beheer (inclusief gebruikers- en autorisatiebeheer). Op centraal niveau beleid ontwikkeld voor beheer en inrichting van ERP-systemen.	• Centrale infrastructuur met één centrale database, waarbij gegevens voor verschillende OpCo's ook in zelfde set van tabellen worden opgeslagen. Gebruikers kunnen vanaf verschillende geografische locaties op hetzelfde ERP-systeem inloggen via bedrijfsnetwerk. Complexiteit van infrastructuur vereenvoudigd door minder applicaties, servers en databases. Vaak nog maar één partij die de applicatie (technisch en functioneel) beheert. Beheer 24 uur per dag beschikbaar vanwege vaak grensoverschrijdende karakter van applicatie. Bepaalde beheeractiviteiten gecentraliseerd. Gedetailleerde richtlijnen voor OpCo's beschikbaar.
Mensen en cultuur	• OpCo kan systeem geheel laten aansluiten bij kennis en ervaring van medewerkers en cultuur van bedrijf. Onderneming hiervoor geheel verantwoordelijk. • Alleen gebruikersaccounts van medewerkers van OpCo in productieve systeem (behoudens aantal consultants en auditors).	• OpCo kan systeem geheel laten aansluiten bij kennis en ervaring van medewerkers en cultuur van bedrijf. OpCo hiervoor geheel verantwoordelijk. OpCo kan zelf beslissen welke beheersingsmaatregelen worden ingezet (bijv. geprogrammeerde controles of gebruikerscontroles); op centraal niveau zijn hier beknopte richtlijnen voor. • Alleen gebruikersaccounts van medewerkers van OpCo in productieve systeem (behoudens aantal consultants en auditors).	• Gebruikers van verschillende OpCo's maken gebruik van zelfde systeem. OpCo dient kennis van mensen en cultuur te laten aanpassen bij de eisen die gebruik van single client daaraan stelt (foutieve acties van medewerkers door verschil in kennis of cultuur kunnen nu immers voor alle OpCo's gevolgen hebben). • Gebruikersaccounts van alle OpCo's in productieve systeem. Vaak vanuit centrale organisatie één autorisatiestructuur aangeboden waar lokale OpCo gebruik van moet maken (zo opgezet dat alle OpCo's ermee kunnen werken en medewerkers alleen activiteiten voor eigen OpCo kunnen uitvoeren).

organisaties die de lokale ERP-systemen beheren. In een single client ERP-systeem zal er een centrale beheerorganisatie zijn die het ERP-systeem beheert, waardoor er ten opzichte van OpCo ERP-systemen op het gebied van technisch beheer schaalvoordelen mogelijk zijn.

Het zelfde geldt voor functioneel beheer. Doordat de OpCo's binnen een single client systeem met gestandaardiseerde bedrijfsprocessen werken zijn er minder medewerkers nodig voor het functioneel beheer van het systeem. Daarnaast zijn deze functioneel beheerders fulltime bezig met het functionele beheer van het systeem, waardoor ook het kennisniveau van het functionele beheerteam ten aanzien van de specifieke inrichting van het systeem hoger is.

Processen en procedures

Processen en procedures bepalen de wijze waarop producten en diensten tot stand komen. Door gebruik van single client ERP kan vaak standaardisatie worden doorgevoerd, waardoor de manier waarop en de specifieke plaats in het proces waar ERP ondersteuning biedt, kunnen veranderen.

Een belangrijke afweging die hierbij gemaakt moet worden is of de lokale entiteiten zich volledig moeten aanpassen aan het single client ERP-systeem of dat het systeem zo moet worden ingericht dat het de specifieke lokale procesgang kan blijven ondersteunen. Op hoofdlijnen voeren alle entiteiten dezelfde processen uit (bijvoorbeeld inkopen van grondstoffen, productie, verkopen van eindproduct, financiële administratie) waardoor standaardisatie mogelijk kan zijn. De mate waarin is echter afhankelijk van de lokale omstandigheden (bijvoorbeeld wetgeving, interfaces) welke bepalen of de uitgevoerde activiteiten ook daadwerkelijk overal gelijk kunnen zijn.

Het (in meerdere of mindere mate) standaardiseren van de processen leidt ook tot de mogelijkheid om procedures te standaardiseren. Hierdoor kunnen bijvoorbeeld trainingsmaterialen en werkinstructies centraal worden aangemaakt en (al dan niet na vertaling of kleine aanpassingen) worden gebruikt door de lokale entiteiten.

Gegevensverzamelingen

Het belang van betrouwbare gegevens is in een ERP-omgeving groot omdat verschillende processen binnen één entiteit gebruikmaken van dezelfde gegevensverzamelingen. Bij single client ERP is dit belang nog groter omdat niet alleen meerdere processen gebruikmaken van dezelfde gegevens, maar ook meerdere entiteiten.

Een belangrijke groep van gegevens zijn de stamgegevens, zoals leveranciers en materialen. Aangezien stamgegevens veelvuldig worden gebruikt binnen ERP-transacties is adequaat beheer van stamgegevens zeer belangrijk voor effectieve en efficiënte bedrijfsprocessen. Doordat stamgegevens een organisatiespecifiek element hebben, zoals klantinformatie die specifiek is voor een bedrijfsnummer, dient de bevoegdheid om stamgegevens bij te werken beperkt te worden. Het bijwerken van organisatiespecifieke gegevens voor entiteiten waarvoor een gebruiker niet werkzaam is, dient zoveel mogelijk te worden voorkomen.

Meer nog dan in een regulier ERP-systeem dient het eigenaarschap van stamgegevens en transactionele gegevens te worden vastgelegd. De eigenaar is vervolgens bevoegd om beslissingen te nemen over bevoegdheden rondom deze gegevens.

Bestuurlijke informatievoorziening

Deze informatie betreft alle informatie die nodig is voor een adequate besturing van processen. Hierbij gaat het niet alleen om informatie uit de gebruikersorganisatie, maar ook uit de IT-organisatie. Door de invoer van single client ERP kan steeds meer gebruik worden gemaakt van controlepunten in de ERP-applicatie zelf (bijvoorbeeld een verschillencontrole tussen factuur en bestelling, controle op dubbele facturen) als vervanging van handmatige controles. Dit resulteert er mede in dat het management niet noodzakelijk informatie nodig heeft over alle details van de procesgang maar alleen over de uitzonderingen in de procesgang.

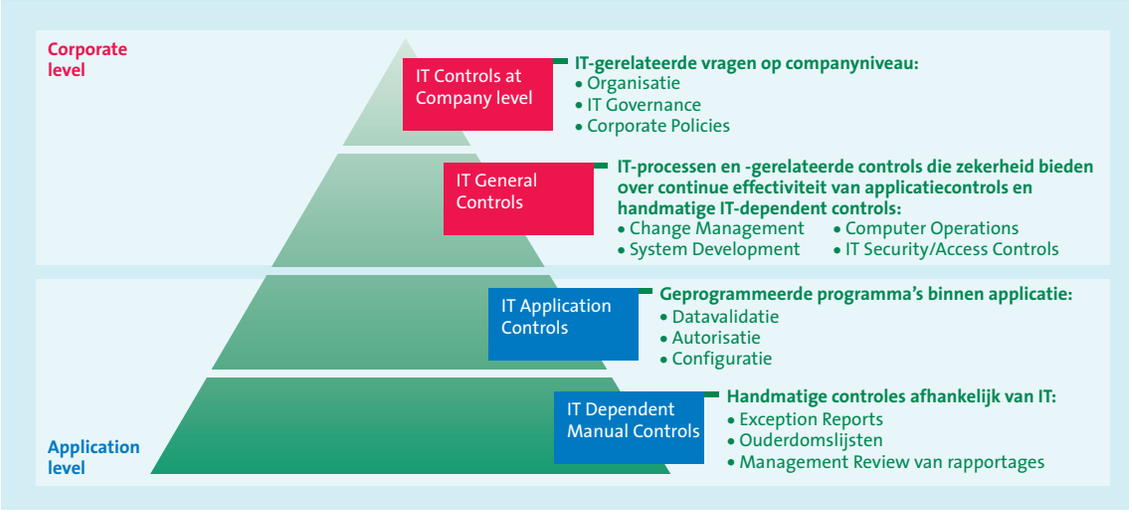
Bij het gebruik van single client ERP ontstaat het voordeel dat de kennis die elke afzonderlijke OpCo opdoet in het werken met de applicatie, gedeeld kan worden. Vooral op het gebied van rapportagemogelijkheden biedt dit voordelen, bijvoorbeeld wanneer een lokale OpCo een rapportage of query heeft ontwikkeld die voor een andere OpCo nuttig kan zijn.

Single client ERP-systeem en interne controle

Het management van een organisatie heeft bepaalde doelstellingen die het wil realiseren en het is daarom van belang dat risico's die deze doelstellingen in gevaar kunnen brengen, worden geïdentificeerd en (afhankelijk van de inschatting van het risico) worden afgedekt door een stelsel van internecontrolemaatregelen.

Het uitvoeren van een proces- en risicoanalyse verschilt bij een single client ERP-systeem in principe niet van het reguliere ERP-systeem. Men dient zich vooral te realiseren dat de risico's die al bestonden in de OpCo ERP-omgeving ook bij single client ERP-systemen van toepassing zijn, maar dat vooral de impact sterk toeneemt en dat de kwaliteit van de risicoanalyse van een lokale entiteit daarom ook van invloed kan zijn op de andere entiteiten.

In de praktijk zien we dat organisaties met een single client systeem zich dit langzaam beginnen te realiseren en vanuit het



Figuur 4. **Relatie tussen diverse typen controls.**

centrale management een risicoanalyse uitvoeren in samenwerking met de lokale entiteiten. Deze analyse leidt tot een centraal risicoanalysedocument waarin de overkoepelende processen met risico's zijn opgenomen en waarin, voor zover nodig, aanvullende processen en risico's zijn opgenomen voor de lokale onderdelen.

Figuur 4 geeft de relatie weer tussen de verschillende controlemaatregelen. De IT general controls zijn de controls die zekerheid bieden over de continue effectiviteit van de geconfigureerde controlemaatregelen en de controlemaatregelen die afhankelijk zijn van de IT-applicatie. Eén van de belangrijkste IT general controls is hierbij het wijzigingsbeheer.

Business process controls

De impact van single client ERP komt vooral naar voren als moet worden vastgesteld welke internecontrolemaatregelen gekozen gaan worden. Gezien de impact die risico's kunnen hebben op de single client omgeving, is een belangrijke rol weggelegd voor de IT application controls, de preventieve maatregelen, zoals configuratie en autorisaties. Een OpCo kan echter niet zomaar harde maatregelen implementeren zonder daarvan de mogelijke impact te kennen op andere organisatieonderdelen.

We zien in de praktijk dat organisaties steeds meer op centraal niveau vaststellen welke maatregelen worden ingevoerd. Waar de lokale entiteiten afwijken van de standaard, worden – al dan niet als maatwerk – aanvullende maatregelen opgesteld. Het is bij deze centrale analyse vanzelfsprekend van belang dat alle risico's voor de lokale entiteiten worden meegenomen.

In de praktijk blijkt dat organisaties met single client vaak nog niet voldoende in staat zijn voor de single client omgeving organisatiebrede interne beheersing op te zetten. Naast de standaardisatie van bedrijfsprocessen is ook uniformering van internecontrolemaatregelen nodig. Op centraal niveau wordt vaak wel een raamwerk voor interne beheersing ontwikkeld en beschikbaar gesteld, maar blijkt tegelijkertijd dat het management van de lokale OpCo's zelf ook bezig is met het uitvoeren van een risicoanalyse en het identificeren en implementeren van beheersingsmaatregelen. Hierbij maakt het management van de lokale OpCo lang niet altijd gebruik van het centraal aangeleverde raamwerk.

Daarnaast is een belangrijke voorwaarde voor het effectief en efficiënt beheersen van de single client omgeving dat voornamelijk gekozen wordt voor harde preventieve maatregelen en deze alleen aan te passen wanneer dit geen problemen oplevert voor de single client als geheel. In de praktijk blijkt nog maar beperkt gebruik te worden gemaakt van deze maatregelen, niet alleen door ontbrekende kennis over de mogelijkheden van de applicatie maar ook doordat in de praktijk de standaardisatie van de processen geringer is dan in theorie beschreven, waardoor eenduidige configuratie en autorisaties nog niet mogelijk zijn.

Door gebruik van single client ERP kan vaak standaardisatie worden doorgevoerd

In de volgende paragraaf wordt in meer detail ingegaan op de invloed van single client ERP op configuratie en autorisaties.

IT general controls

Door het gebruik van single client ERP neemt ook het belang van de IT general controls toe. Niet alleen maken meerdere organisatie-entiteiten nu gebruik van hetzelfde systeem, maar ook wordt vaak meer gesteund op de geprogrammeerde, preventieve maatregelen binnen het ERP-systeem waardoor wijzigingsbeheer en gebruikers- en autorisatiebeheer van groter belang worden.

Het eigenaarschap van configuratie-instellingen onafhankelijk van een OpCo ligt in principe centraal

De IT-organisatie zelf verschuift veelal van lokale beheerorganisaties naar meer centraal beheer, bijvoorbeeld via een shared service center met een helpdesk waardoor betere beheersing van IT mogelijk is. Veel beslissingen en goedkeuringsactiviteiten worden genomen in samenwerking met de lokale entiteiten. Hiervoor worden nieuwe overleggroepen in het leven geroepen of het eigenaarschap van delen van het systeem (bijvoorbeeld een deel van de autorisatiestructuur) wordt belegd bij het lokale management.

Gebruikers- en autorisatiebeheer

Het wijzigen van gebruikers en autorisaties en het toekennen van autorisaties aan gebruikers mogen alleen plaatsvinden na expliciete goedkeuring. Daarom dient het eigenaarschap van gebruikers en autorisaties te zijn belegd en dient in de processen steeds rekening te worden gehouden met de impact van een wijziging op het single client ERP-systeem als geheel.

Het eigenaarschap van reguliere gebruikers ligt bij de lokale entiteiten. Het eigenaarschap van speciale gebruikers zoals systeembeheerders, batchgebruikers, workflowgebruikers, interfaces en de helpdesk ligt op centraal niveau.

Voor het onderhoud van autorisaties geldt dat in een single client ERP-systeem bij voorkeur een zogeheten autorisatietemplate aanwezig dient te zijn, waarin de standaardtaken en -functies zijn vastgelegd die vervolgens kunnen worden uitgerold naar de diverse entiteiten. Het eigenaarschap van de template dient, gezien de impact op de gehele organisatie, altijd centraal te zijn toegewezen. Het eigenaarschap van de afgeleide sets autorisaties ligt bij de OpCo.

De security manager zal aan de hand van beschikbare autorisatierichtlijnen moeten vaststellen of aangevraagde wijzigingen op centraal niveau kunnen worden doorgevoerd. De security manager dient de eigenaar van de template te adviseren over de impact van de geplande wijziging.

Door de complexiteit van autorisaties, vooral in een single client ERP-systeem, dient de organisatie te beschikken over geautomatiseerde tools (bijvoorbeeld SAP GRC Access Controls, Approva, CSI AA) om de autorisaties op een beheerste wijze toe te kennen en te monitoren. Rapportages kunnen centraal worden uitgevoerd en gedistribueerd aan de lokale entiteiten.

Wijzigingsbeheer

Net als bij gebruikers- en autorisatiebeheer geldt dat voor wijzigingen goedkeuring vereist is en dat het eigenaarschap van de systeemconfiguratie dus toegekend moet zijn. Voor configuratie-instellingen die onafhankelijk zijn van een OpCo geldt in principe dat het eigenaarschap centraal ligt. Bij een verzoek tot wijziging dient dan een uitgebreide impactanalyse te worden uitgevoerd om vast te stellen wat de gevolgen voor de single client als geheel kunnen zijn.

Naast OpCo-onafhankelijke (systeemoverstijgende) parameters kent ERP ook instellingen die in meerdere of mindere mate afhankelijk zijn van het organisatieonderdeel (bijvoorbeeld factuurtoleranties). Alhoewel deze instellingen zijn gebaseerd op centrale richtlijnen (bijvoorbeeld inkoopbeleid) zal de OpCo eigenaar zijn van deze instellingen. Wederom geldt dat een impactanalyse vereist is voordat een wijziging wordt doorgevoerd.

De invloed van een single client ERP-systeem op de audit

De IT-auditor kan op diverse wijzen betrokken zijn bij het beoordelen van (onderdelen van) de interne controle in een single client ERP-omgeving. Dit kan bijvoorbeeld zijn in opdracht van de accountant bij het uitvoeren van werkzaamheden voor de jaarrekeningcontrole. Daarnaast kan ook het management van een organisatie zelf de opdrachtgever zijn, bijvoorbeeld in het kader van Sarbanes-Oxley of in het kader van een pre- of post-implementatie-audit.

Het auditproces

Een belangrijke stap in het auditproces is het bepalen van de opdrachtgever en daaraan gerelateerd het eenduidig vaststellen van de scope van de audit. Het maakt een groot verschil of op verzoek van lokaal management of een lokale accountant de configuratie van één specifieke entiteit binnen de single client ERP wordt bekeken of dat vanuit een centrale audit alle entiteiten worden meegenomen. De reden waarom dit binnen single client ERP-systemen zo belangrijk is, is dat er zoveel entiteiten in één systeem zijn opgenomen dat er makkelijk te veel of te

weinig entiteiten worden meegenomen in de werkzaamheden. De auditor dient specifiek vast te stellen welke entiteiten worden meegenomen (vergelijkbaar met regulier ERP), maar dient daarna ook concreet te maken hoe deze entiteiten in het single client ERP-systeem zijn gedefinieerd (bijvoorbeeld welke bedrijfsnummers).

Overigens betekent het auditen in een single client omgeving ook dat ondanks de gedetailleerde scoping issues kunnen worden gespot die niet direct binnen de scope vallen. Door het gebruik van tools en het bekijken van centrale tabellen verkrijgt de auditor veelal informatie over het gehele single client ERP-systeem. Als er hierbij specifieke punten worden opgemerkt, bijvoorbeeld de tolerantiegrenzen voor de OpCo in scope staan prima, maar voor andere OpCo's staan deze helemaal verkeerd, dan dient de auditor hier wel iets mee te doen.

Het te hanteren normenkader is een ander aandachtspunt. In eerdere paragrafen is al genoemd dat in de single client omgeving steeds vaker vanuit het centrale management een controleraamwerk wordt opgesteld. Wanneer de opdrachtgever het centrale management is dan dient te worden besproken hoe het centrale raamwerk is opgesteld en welke betrokkenheid de OpCo's hierin hebben gehad. Wanneer een opdracht wordt uitgevoerd voor het lokale management dan dient te worden nagegaan hoe het lokale controleraamwerk tot stand is gekomen. In de praktijk levert een snelle blik op het controleraamwerk voor de auditor al voldoende signalen op om het controlebewustzijn van de organisatie in te schatten. Bevat het document alleen standaardprocessen of zijn ook kenmerkende lokale processen opgenomen? Wat is de diepgang van de risicoanalyse? Is het een centraal aangeleverd of lokaal opgesteld document? Waar nodig worden voor aanvullende lokale processen aanvullende doelstellingen, risico's en controlemaatregelen opgesteld.

Organisatie van de audit

Door het opnemen van meerdere entiteiten in een single client ERP-systeem komt de vraag op wie de audit zal moeten uitvoeren. Denk bijvoorbeeld aan een jaarrekeningcontrole waarbij de diverse lokale entiteiten geaudit moeten worden maar waarbij het risico van dubbel werk op de loer ligt als iedereen voor zichzelf lokaal de configuratie in het ERP-systeem gaat beoordelen.

Het zal niet verbazen dat een centraal en een lokaal auditteam betrokken zullen moeten zijn bij de audit op een single client systeem. Het centrale auditteam zal hierbij verantwoordelijk zijn voor het opstellen van het generieke controleplan. Dit generieke plan zal door de lokale auditteams vervolgens specifiek gemaakt moeten worden voor de lokale OpCo. Hierdoor worden andere belangrijke systemen ook in de scope meegenomen en kan het lokale auditteam andere aandachtspunten, zoals het voldoen aan de lokale wetgeving ook in de scope meenemen. Een mogelijk nadeel is de communicatie tussen de verschillende partijen en het risico dat controleplannen, wanneer deze eenmaal door centraal zijn aangeleverd, niet als zodanig gebruikt worden of juist te veel worden aangepast. Dit houdt in dat vanuit het centrale auditteam één team de leiding moet krijgen over de volledige audit.

Het centrale team voert de controle uit op configuratie en autorisaties en levert deze gegevens aan de lokale teams aan. Deze beoordelen vervolgens de gebruikerscontroles. Een veelgebruikte wijze om de centrale bevindingen aan de lokale auditors kenbaar te maken, welke vooral wordt gebruikt bij de jaarrekeningcontrole, is de zogeheten 'comfort letter'. In de comfort letter is beschreven welke activiteiten de centrale auditors hebben uitgevoerd en wat de uitkomsten hiervan waren. Uit deze comfort letter zal dus blijken of de lokale auditors kunnen steunen op de centraal geteste internecontrolemaatregelen.

Inhoudelijke aandachtspunten

In dit laatste gedeelte wordt een aantal specifieke aandachtspunten genoemd rond het beoordelen van de interne controle in het single client ERP-systeem: configuratie, autorisaties en rapportages.

Configuratie

Bij het beoordelen van de configuratie van het systeem is het vooral van belang dat de IT-auditor zich realiseert wat de impact is van specifieke instellingen op het single client ERP-systeem als geheel. ERP kent instellingen op meerdere niveaus. Ten eerste zijn er de instellingen op gebruikersniveau, zoals gebruikersparameters. Ten tweede zijn er instellingen op organisatieniveau, zoals factuurtoleranties ingesteld per bedrijfsnummer. Tot slot zijn er de instellingen op systeemniveau, waarbij gedacht kan worden aan verplichte velden voor documenten.

Het type instelling bepaalt mede wie verantwoordelijk is en hoe wordt omgegaan met wijzigingen. Voor gebruikersafhankelijke instellingen ligt het eigenaarschap lokaal. De auditor zal de details van de instellingen moeten opvragen en bepalen hoe lokaal wordt omgegaan met wijzigingen hierin. Overigens betekent lokaal eigenaarschap niet dat geen centrale richtlijnen kunnen zijn opgesteld.

Een centraal en een lokaal auditteam moeten betrokken zijn bij de audit van een single client ERP-systeem

Een solide autorisatiestructuur in een single client ERP-systeem begint met een centraal autorisatieconcept

Instellingen op organisatieniveau zijn alle instellingen die de bedrijfsprocessen beïnvloeden op basis van de organisatie die wordt gebruikt bij het uitvoeren van een transactie zoals vrijgavestrategie op basis van vestiging. Voor instellingen op organisatieniveau geldt dat het eigenaarschap vrijwel altijd bij de OpCo ligt tenzij het overkoepelende organisatieonderdelen behelst. Voor instellingen die zijn gebaseerd op centrale richtlijnen – bijvoorbeeld inkoopbeleid bepaalt type vrijgavestrategie, financieel beleid bepaalt type tolerantiegrenzen – ligt de keuze voor de configuratiemaatregel veelal centraal maar kan de specifieke waarde – mandaten binnen vrijgave, hoogte tolerantiegrenzen – door de lokale entiteit worden bepaald.

Organisatieoverschrijdende instellingen zijn alle instellingen die het ERP-systeem beïnvloeden zonder directe relatie met een organisatieonderdeel. Denk hierbij niet alleen aan functionele instellingen zoals verplichte velden maar ook aan systeemsettings. Een wijziging in deze instellingen heeft zonder meer gevolgen voor elke OpCo die gebruikmaakt van het ERP-systeem. Het eigenaarschap van deze instellingen ligt altijd centraal en de wijziging zelf wordt, net als bij de overige typen instellingen, centraal uitgevoerd. De auditor zal vast moeten stellen dat de bevoegdheden tot wijziging beperkt zijn en alleen aan de juiste functies zijn toegekend.

Autorisaties

Autorisaties (en daarbij ook gerekend de authenticatie) dienen ervoor te zorgen dat gebruikers alleen die activiteiten kunnen uitvoeren die benodigd zijn voor hun functie en dat functiescheiding wordt gerealiseerd. De impact van single client ERP op autorisaties is vooral dat een dimensie wordt toegevoegd door te eisen dat gebruikers, tenzij anders bepaald, alleen transacties mogen uitvoeren voor de OpCo waarin zij werkzaam zijn. Niet goed ingerichte autorisaties geven al snel bevoegdheid om voor andere entiteiten werkzaamheden uit te voeren. De praktijk laat zien dat aan de simpele basiseis van 'alleen autorisaties voor eigen entiteit' vaak niet wordt voldaan.

Autorisatieconcept

Het realiseren van een solide autorisatiestructuur in een single client ERP-systeem begint met het opzetten van een centraal autorisatieconcept. Dit beschrijft de wijze waarop de functionaliteit van ERP wordt ingezet om de beveiliging vorm te geven. Om het autorisatieconcept in een single client ERP-omgeving beheerbaar te houden kan de organisatie gebruikmaken van templaterollen en afgeleide rollen. Indien een onderneming single client ERP heeft geïmplementeerd, dan heeft mogelijk in meerdere of mindere mate standaardisatie over de bedrijfsprocessen plaatsgevonden. In dat geval kan binnen het autorisatieconcept ook gewerkt gaan worden met standaardtaken en -functies door bijvoorbeeld samengestelde rollen te gebruiken. De auditor zal moeten vaststellen of deze functionaliteit in gebruik is en op een juiste manier wordt toegepast. Het gebruik van afleidingen en samengestelde rollen biedt de organisatie een hulpmiddel bij het inrichten van autorisaties voor meerdere entiteiten. Fouten zijn echter snel gemaakt en kunnen dan een tegengesteld effect opleveren.

Functiescheidingen

Functiescheiding in een single client ERP-systeem is in principe niet anders dan functiescheiding in een OpCo ERP-systeem, namelijk het voorkomen dat een gebruiker een kritische combinatie van transacties kan uitvoeren. Een verschil ligt echter in het feit dat er meer entiteiten in het single client ERP-systeem aanwezig zijn. Wanneer functiescheiding wordt bekeken, dient de auditor er zeker van te zijn dat beide transacties voor dezelfde OpCo kunnen worden uitgevoerd. Het invoeren van een inkooporder voor een vestiging van Operating Company A is immers niet in conflict met de mogelijkheid tot het invoeren van een goederenontvangst op een vestiging van Operating Company B.

Super users en systeembevoegdheden

Het gebruik van bijzondere bevoegdheden zoals zogenaamde 'super users' dient zoveel mogelijk te worden voorkomen (of in elk geval extra te worden bewaakt) omdat deze in single client ERP-omgevingen nog meer impact hebben dan in een regulier ERP-systeem. Hiermee wordt niet alleen functiescheiding tussen transacties verbroken maar ook de scheiding tussen organisatie-entiteiten.

Hetzelfde geldt voor de systeembevoegdheden. Dit zijn bevoegdheden voor de configuratie van het systeem of voor het beheer van het ERP-systeem inclusief uitvoeren van massawijzigingen. Misbruik van dit soort transactiecodes is bij ERP al kritisch maar kan in een single client omgeving extra grote gevolgen hebben omdat meerdere entiteiten afhankelijk zijn van de beschikbaarheid en de integriteit van het volledige ERP-systeem.

Maatwerk

Indien de standaardfunctionaliteit van een single client ERP-systeem niet voldoende is om alle bedrijfsprocessen te ondersteunen of om aan alle wensen van de gebruikers te voldoen, dan is het mogelijk dat maatwerk wordt ontwikkeld. Hierbij is het niet alleen van belang dat niet iedere gebruiker toegang heeft tot het maatwerk, maar ook dat de gebruikers die toegang hebben tot het maatwerk via dit maatwerk geen toegang krijgen

tot gedeelten van de applicatie waartoe zij eigenlijk geen bevoegdheid moeten hebben. In de praktijk zien we lokaal veel maatwerk om specifieke deelprocessen te ondersteunen dat bovendien niet altijd is afgeschermd met de benodigde autorisatiecontroles voor specifieke acties of organisatie-entiteiten.

Rapportages

Rapportages zijn onder meer overzichtslijsten en uitzonderingslijsten die binnen het ERP-systeem worden uitgevoerd door eindgebruikers. Bij rapportages in single client ERP is het van belang dat deze met de juiste selectiecriteria worden uitgevoerd én met de juiste bevoegdheden. Indien een gebruiker een rapportage uitvoert voor zijn eigen OpCo maar hij past niet de juiste selectiecriteria toe dan kan dit leiden tot onjuiste uitkomsten. Hetzelfde geldt voor het uitvoeren van een rapportage met te weinig bevoegdheden. In dit geval kan de gebruiker verkeerde (= niet alle) uitkomsten krijgen zonder dat het systeem daarvoor een waarschuwing geeft. Het risico is dan aanwezig dat de gebruiker of het management beslissingen neemt op basis van onjuiste en/of onvolledige informatie.

Voor het maken van nieuwe rapportages of het wijzigen van bestaande rapportages gelden de eerder beschreven aandachtspunten rondom wijzigingsbeheer. Voor centrale (standaard) rapportages ligt het eigenaarschap centraal. Voor lokale (maatwerk)rapportages kan het eigenaarschap lokaal liggen.

Conclusie

Het uitvoeren van audit- en advieswerk gerelateerd aan single client ERP-omgevingen brengt specifieke aandachtspunten met zich mee. Hoewel op hoofdlijnen de werkzaamheden niet anders zullen zijn dan in een reguliere ERP-omgeving is het juist het detailniveau waarop een auditor de plank mis kan slaan. Hierbij is het van belang om voor de start van de werkzaamheden duidelijk in kaart te hebben welke entiteiten binnen de single client in scope van de audit zijn. Daarnaast moeten er duidelijke afspraken worden gemaakt tussen het centrale auditteam en het lokale auditteam over welk team welke werkzaamheden uitvoert. Ten aanzien van controls is het duidelijk dat de General IT Controls van groot belang zijn, daar het single client systeem erg belangrijk zal zijn voor de organisatie. De mogelijke application controls die in een single client systeem kunnen worden aangetroffen, zijn gelijksoortig aan de application controls in een OpCo ERP-systeem. Bij het beoordelen van de application controls is het echter van groot belang dat de controls voor de OpCo's in scope worden beoordeeld. Door duidelijke afspraken te maken tussen het lokale team en het centrale team zijn vervolgens schaalvoordelen mogelijk doordat de uit te voeren activiteiten ook maar eenmalig worden uitgevoerd.