De schijnzekerheid van SAP-autorisatie-tools

De tools zijn prima, maar richt u ze wel goed in?

Drs. D. Hallemeesch
is manager bij KPMG IT Advisory. Hij is verantwoordelijk voor het aandachtsgebied SAP application security en heeft verschillende onderzoeken uitgevoerd naar de kwaliteit van de regels zoals geïmplementeerd in GRC software van SAP, Approva en SecurInfo. Daarnaast houdt hij zich ook bezig met het adviseren rond controls monitoring en de implementatie van GRC-tools.
hallemeesch.dennis@kpmg.nl

Drs. A. Vreeke
is senior manager bij KPMG IT Advisory. Sinds 1997 is hij betrokken bij complexe SAP internecontrolegerelateerde opdrachten. Sinds 2003 volgt hij actief de markt op het gebied van SAP-tooling. Zijn aandachtsgebied bestrijkt ook de informatiebeveiliging in SAP-BI-omgevingen en Identity- en Access-managementvraagstukken.
vreeke.arjan@kpmg.nl

Drs. Dennis Hallemeesch en drs. Arjan Vreeke RE

Veel ondernemingen zijn zich aan het oriënteren op tooling om functiescheidingsconflicten in SAP te monitoren of hebben reeds een ondersteunende tool aangeschaft. Hierbij kan bijvoorbeeld gedacht worden aan GRC Access control van SAP (voorheen Virsa), Approva BizRights, SecurityWeaver, CSI-AA en SecurInfo. Succesvol gebruik van zo'n tool hangt sterk af van de wijze waarop de functiescheidingsregels zijn ingericht. Uit een aantal onderzoeken uitgevoerd door KPMG blijkt dat de ingerichte regels in de tooling vaak van beperkte kwaliteit zijn, waardoor er grote kans is dat de uitkomsten van de tool onnauwkeurig zijn. Het melden van 'false positives' en 'false negatives' is het gevolg. Dit heeft dramatische gevolgen voor het vertrouwen in de werking van de tool.

Om de gevolgen van 'false positives' en 'false negatives' te illustreren, maken we eerst even een zijsprongetje. Medio 2007 brak er brand uit in het Armando-museum in Amersfoort. Terwijl de vlammen uit het dak van de voormalige kerk sloegen, keken omstanders toe. Sommigen namen de moeite om de brand met hun mobiele telefoon te filmen. Pas na enige tijd dacht iemand eraan de brandweer te waarschuwen. Toen die ter plekke kwam, was het museum echter al reddeloos verloren. De brandmelders die in het museum waren aangebracht, hingen te hoog en hadden pas rook gesignaleerd toen het vuur al vernietigend om zich heen had gegrepen. Tegenover dit geval van falende alarmmelding staat een berucht geval van alweer tientallen jaren geleden. Daarbij moest een brandweerkorps zeven, acht keer uitrukken om iedere keer ter plekke te ontdekken dat de brandmelding onterecht was geweest. Toen de brandweer voor de negende keer een brandmelding kreeg, was haar alertheid danig verminderd. Natuurlijk rukte zij wel uit, maar haar reactietijd was een stuk langer dan bij eerdere brandmeldingen. Wie gewend raakt aan onterecht alarm, wordt laconiek: het zal wel weer niets wezen!
Deze twee voorbeelden tonen aan dat er van alles mis kan gaan als een alarm niet goed 'getuned' is. Het alarm kan afgaan, terwijl er feitelijk niets aan de hand is. Daartegenover staan noodsituaties, waarbij juist geen alarm wordt afgegeven. In beide uiterste gevallen kan het eindresultaat dramatisch zijn.

Inleiding

Dit artikel gaat uiteraard niet over de brandweer of vergelijkbare hulpdiensten. Maar dit verhaal gaat wél over alarmmeldingen die al dan niet terecht zijn. En die in de context van een grote onderneming ook dramatische gevolgen kunnen hebben.

Sinds de boekhoudschandalen bij Enron en Worldcom is er in ondernemersland veel veranderd. Vooral door de omvang van de fraude en de dramatische gevolgen daarvan voor werknemers en particuliere investeerders, greep de Amerikaanse overheid na de fraude bij Enron en Worldcom stevig in. Dat leidde in 2002 tot de invoering van uitgebreide bedrijfsvoerings- en verslagleggingsregels voor beursgenoteerde ondernemingen. Ook Europese ondernemingen conformeren zich inmiddels aan deze Sarbanes-Oxley (SOx)-richtlijnen.

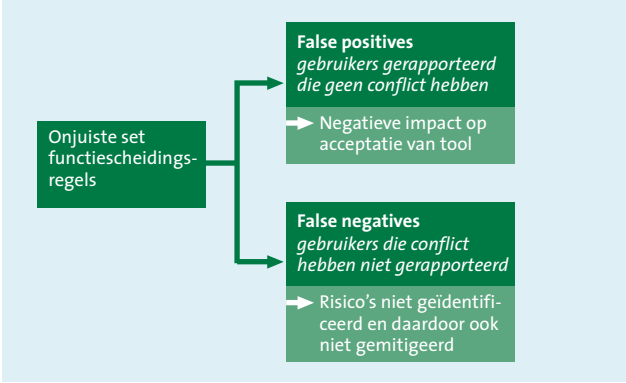
Eén van de rechtstreekse gevolgen daarvan is dat bij audits strenger wordt gecontroleerd op conflicterende bevoegdheden binnen een organisatie. In feite is er daarmee niets nieuws onder de zon. Starreveld, de grondlegger van de traditionele administratieve organisatie, hanteerde hieromtrent al duidelijk vuistregels. Zo was het volgens hem uit den boze dat één functionaris verantwoordelijk zou zijn voor twee of meer achtereenvolgende taken binnen een specifiek proces. Ter verduidelijking een voorbeeld: het is vragen om moeilijkheden als de functionaris die verantwoordelijk is voor inkoop ook de man is die leveringen in ontvangst neemt. Deze situatie maakt misbruik mogelijk. De taken Inkoop en Goederenontvangst zouden dus nooit op het bordje van één functionaris mogen liggen. Op vergelijkbare manier zijn er heel veel functierollen die in combinatie misbruik mogelijk maken. Om de kans op misbruik te beperken moet een organisatie dus voorkomen dat die combinaties van rollen door één medewerker uitgevoerd kunnen worden. Hoe belangrijk functiescheiding en interne controle is, werd overigens onlangs weer eens duidelijk door de gebeurtenissen bij de Franse bank Société Générale.

Inrichting van functiescheidingstools

De inrichting en implementatie van een functiescheidingstool is een project op zich met veel addertjes onder het gras, waarover later meer. Veel leveranciers van dergelijke tools hebben al enig voorwerk gedaan en leveren hun software met kant-en-klare tabellen. Daarin zijn min of meer algemeen geldende regels ten aanzien van functiescheiding als standaard opgenomen. Dit kan een nuttige basis vormen voor een organisatie die met deze software aan het werk wil. Echter, zowel met deze standaardtabellen als met tabellen die door een projectteam binnen een organisatie worden ingevuld, liggen nieuwe risico's op de loer.

Die risico's zijn onder te verdelen in twee typen, die enigszins vergelijkbaar zijn met de twee situaties rond brandalarmmeldingen aan het begin van dit verhaal. Ten eerste kunnen de tabellen zodanig zijn ingevuld dat risicovolle situaties wel degelijk aan de orde van de dag zijn, maar niet worden gesignaleerd. Anders gezegd: de vlammen slaan uit het dak, maar het alarmsysteem registreert niets, omdat dit niet juist is afgesteld.

Ten tweede kan, wederom door onjuist ingevulde tabellen, het aantal alarmmeldingen overstelpend groot zijn. Daarbij kunnen dan heel veel meldingen zijn van transacties die ten onrechte op die lijst staan, omdat ze helemaal niet risicovol zijn. Het gevolg van deze 'ruis' is dat werkelijk risicovolle transacties ondersneeuwen in de veelheid van onterechte meldingen en niet of nauwelijks meer opgemerkt worden. Dit is vergelijkbaar met het brandweerkorps dat zijn alertheid verliest als het diverse malen zonder reden is uitgerukt.



Figuur 1. **De invloed van foutieve functiescheidingsregels.**

Let wel, dat deze twee foutsoorten veel voorkomen is geen diskwalificatie van een functiescheidingstool op zich. Die software werkt prima. De fouten zijn echter het gevolg van het onjuist inrichten van zo'n tool of het niet adequaat up-to-date houden van die inrichting.

Tijdens het implementeren van een functiescheidingstool kan een aantal verschillende fasen worden onderscheiden zoals in figuur 2 schematisch is weergegeven.

Risk Recognition

De Risk Recognition-fase is één van de belangrijkste fasen. In deze fase zal de onderneming door middel van bijvoorbeeld workshops moeten vaststellen welke functiescheidingen de onderneming door de tool wil laten monitoren. Deze fase is een niet te onderschatten fase. Immers, indien tijdens deze fase

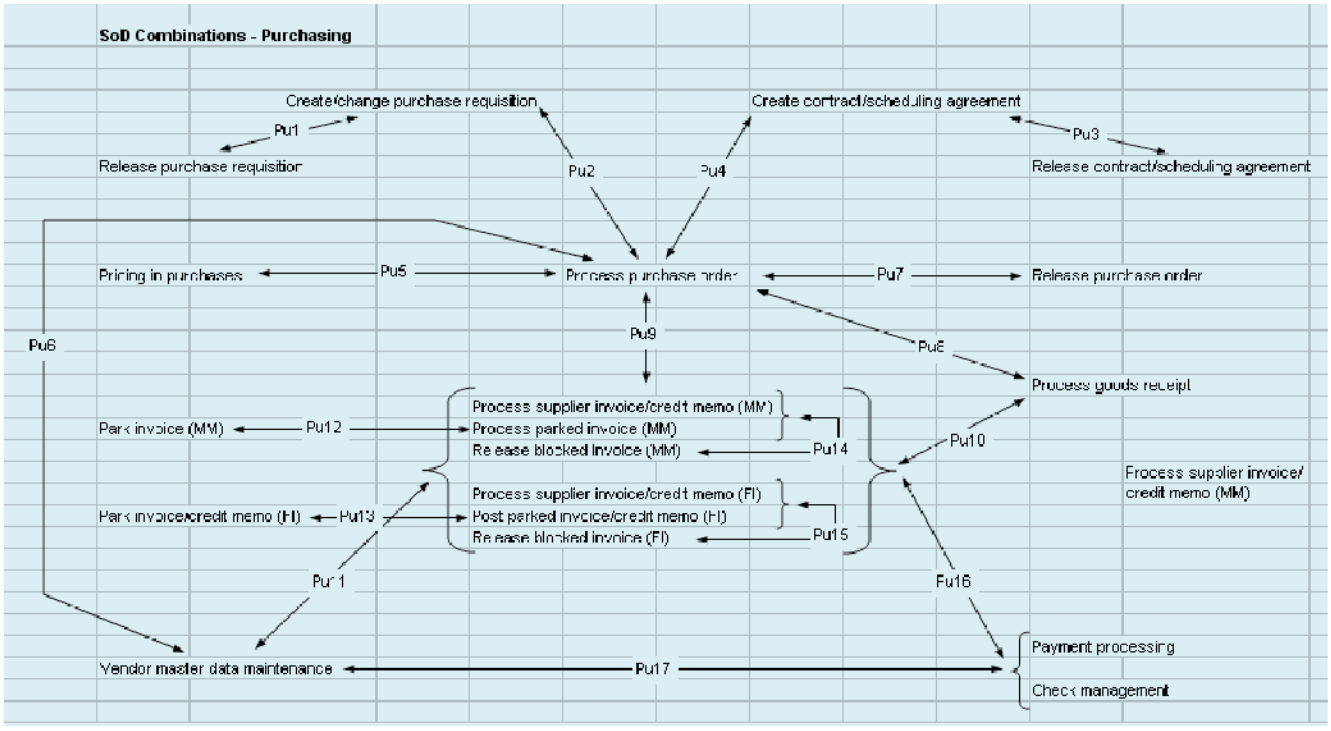
Figuur 2. **Fasen in een implementatietraject.**

bepaalde risico's niet worden geïdentificeerd, dan zullen deze risico's ook niet in de tool worden opgenomen. Tijdens de workshops dienen de verschillende businessprocessen de functiescheidingsconflicten en het bijbehorende risico te definiëren. Daarnaast kunnen de procesexperts ook aangeven of er in de verschillende processen reeds risicomitigerende maatregelen zijn ingeregeld. Het is daarnaast aan te raden om de gedefinieerde conflicten voor te leggen aan bijvoorbeeld de externe auditor of advieskantoor om deze de gedefinieerde conflicten te laten valideren en eventueel te laten aanvullen.

Een mogelijkheid om functiescheidingsconflicten te definiëren is eerst de verschillende processtappen en vervolgens de verschillende conflicterende relaties in kaart te brengen. Een voorbeeld hiervan is voor het Purchase-to-Pay-proces in figuur 3 opgenomen.

Daarnaast dient in deze fase reeds te worden vastgesteld hoe met conflicten zal moeten worden omgegaan. Hierbij zijn conflicten in drie categorieën in te delen:

- Hoog risico-conflicten: conflicten die absoluut niet in het systeem mogen voorkomen. De organisatie accepteert geen mitigerende maatregelen. Nee is nee.
- Medium risico-conflicten: conflicten die wel in het systeem mogen voorkomen maar die gemitigeerd moeten worden met compenserende maatregelen. De effectiviteit van de compenserende maatregelen moet periodiek worden getoetst.
- Laag risico-conflicten: proceseigenaren/afdelingshoofden moeten weten dat deze conflicten voorkomen en periodiek controleren of de bewuste conflicten nog steeds als laag risico gelden. De proceseigenaren/afdelingshoofden tekenen uit hoofde van hun functie een 'risk letter' waarin zij onder andere aangeven het risico te hebben afgewogen.



Figuur 3. **Voorbeeld van het opstellen van functiescheidingsconflicten.**

Tip: In de meeste functiescheidingsregels die worden ontwikkeld, worden geen regels gedefinieerd voor afzonderlijke kritieke activiteiten in het systeem. Zo zouden er naast functiescheidingsregels apart regels moeten worden ontwikkeld voor het onderhouden van de verschillende soorten stamgegevens, of kritieke activiteiten zoals de betaalfunctie of periode sluiten. Door de monitorende rol van de tool zo uit te breiden, wordt de effectiviteit van de tool verhoogd.

In de Risk Recognition-fase is het van groot belang dat alle mogelijke functiescheidingen worden gedefinieerd. Immers, indien conflicten niet worden gedefinieerd dan zullen deze niet in de tool worden opgenomen. In deze fase is het aan te bevelen om naast de business process owners bijvoorbeeld de interne en externe auditors en de controllers te betrekken in het definiëren of beoordelen van de gedefinieerde risico's om te voorkomen dat risico's niet geïdentificeerd worden én om te voorkomen dat conflicten worden opgenomen in de functiescheidingslijst die geen risico voor de onderneming vormen. Indien in de Risk Recognition-fase niet voldoende aandacht wordt besteed aan het identificeren van de juiste risico's, dan kan dit tijdens het in gebruik nemen van de conflicten veel invloed hebben op false negatives en false positives.

De best practice functiescheidingslijst is een goed startpunt voor het definiëren van de definitieve lijst

Technical Realization

In de tweede fase wordt gebouwd aan de Segregation of Duties (SoD). In deze fase worden de businessregels vertaald in SAP-transactiecodes en -autorisatieobjecten. SAP biedt veel verschillende mogelijkheden om een bepaalde activiteit uit te voeren. Zo zijn er bijvoorbeeld veel parametertransactiecodes gemaakt voor het boeken van financiële documenten, waardoor er, afhankelijk van de versie van SAP, meerdere transactiecodes zijn waarmee financiële documenten of facturen kunnen worden geboekt. Het is evident dat in een functiescheidingstool alle mogelijke opties voor het invoeren van data moeten worden meegenomen in de functiescheidingslijsten. Indien een transactiecode ontbreekt in de functiescheidingslijst, maar wel wordt gebruikt in het SAP-systeem, dan zullen er SoD-conflicten in het systeem voorkomen die wellicht niet bij het management bekend zijn. Het is van groot belang dat de impact van foutieve regels niet onderschat wordt. Indien de regels fouten bevatten dan worden de resultaten van de tool onbetrouwbaar. Dit kan grote gevolgen hebben voor de acceptatie van de tool door functionarissen die met de uitkomsten van de tool moeten werken. Het afstemmen van de resultaten en het komen tot oplossingen is dan een tijdrovend proces, omdat er veel overtuigingskracht aan vooraf dient te gaan.

In het tweede deel van het artikel gaan wij dieper in op de soorten fouten die wij tijdens verschillende reviews hebben aangetroffen. In de SoD-bouwfase is het van groot belang om personen te betrekken die zeer gedetailleerde kennis hebben van enerzijds de geïmplementeerde SAP-autorisaties, maar anderzijds van het SAP-autorisatieconcept op zich. Het team van deze personen kan immers gedetailleerd documenteren welke autorisatiecontroles worden uitgevoerd door de verschillende SAP-transactiecodes, welke controles door de onderneming zijn uitgezet en welke controles tijdens de implementatie zijn geactiveerd. Daarnaast is het aan te bevelen om de ingerichte functiescheidingsregels door een externe partij te laten beoordelen op juistheid en volledigheid.

Tip: Maak bij het definiëren van de functiescheidingslijsten gebruik van de best practices van bijvoorbeeld de toolleveranciers. Deze best-practicelijsten bieden over het algemeen een goed startpunt voor het technisch opstellen van een functiescheidingslijst. Let op: deze best practices zijn ook niet meer dan een goed startpunt. Daarnaast is het vaak ook nuttig om een autorisatiespecialist de blueprint van de functiescheidingsregels te laten beoordelen.

In de realisatiefase is het verder ook mogelijk om de kwaliteit van de ingerichte regels te testen, door bijvoorbeeld te kijken welke gebruikers toegang hebben tot bepaalde functionaliteit en deze te vergelijken met de statistieken. Indien er meer gebruikers voorkomen in de statistieken dan in de functiescheidingslijst, zit er waarschijnlijk een fout in de functiescheidingslijst. Deze kwaliteitsanalyse van de functiescheidingslijst kan tijdens het daadwerkelijk gebruik van de lijst veel discussie over de resultaten van de lijst voorkomen. Het testen kan ook door middel van een derde partij gebeuren. De derde partij runt dan met haar eigen tools een overeenkomstige lijst met regels. De resultaten zullen gelijk moeten zijn.

Risk Analysis

De derde fase in het implementatietraject is de Risk Analysis-fase. In deze fase wordt beoordeeld hoeveel conflicten en hoeveel werk er verwacht kunnen worden bij het oplossen van de functiescheidingsconflicten. Het aantal conflicten kan dan worden gecategoriseerd naar High, Medium of Low, of eventueel per proces Order-to-Cash, Purchase-to-Payment en Finance-to-Management.

Tip: Maak voor aanvang van het project een inschatting van het aantal conflicten door bijvoorbeeld een quick scan op de autorisaties te laten uitvoeren.

Daarnaast dient in deze fase een inschatting te worden gemaakt van conflicten die gemitigeerd kunnen worden of die opgelost kunnen worden door het ontkoppelen van autorisaties en het verplaatsen van bevoegdheid binnen de onderneming. Vooral bij het laatste is het van groot belang dat het autorisatieconcept zodanig is ingericht dat er eenvoudig wijzigingen in de koppeling van rollen aan gebruikers kunnen worden aangebracht. Indien het lastig is om bevoegdheden aan te passen doordat het autorisatieconcept niet eenvoudig is aan te passen, dan kan dit tot gevolg hebben dat er parallel aan het implementatietraject voor de functiescheidingstool ook een traject voor het opschonen of herinrichten van het autorisatieconcept gestart moet worden. Anders zult u continu dezelfde bevindingen moeten rapporteren, zonder dat deze opgelost kunnen worden. De impact van uw bevinding (denk aan het alarm) wordt dan steeds minder krachtig en leidt tot frustraties.

Het gebruik van gebruikersstatistieken kan in deze fase erg nuttig zijn. Het is mogelijk om uit SAP het daadwerkelijk gebruik van transactiecodes door eindgebruikers te downloaden. Met behulp van deze gebruiksstatistieken kan een aantal zaken in kaart worden gebracht:

1. Zijn er functiescheidingsconflicten in het systeem die niet gebruikt worden (technische conflicten)? Een gebruiker heeft de combinatie van conflicterende transactiecodes wel gekregen in zijn autorisatieprofielen, maar heeft een gedeelte van het conflict of beide gedeelten van het conflict niet nodig in zijn werkzaamheden.
2. Zijn er gebruikers die toegang hebben tot kritische functionaliteit (business of systeemactiviteiten) die deze bevoegdheid niet gebruiken? Door bijvoorbeeld ongebruikte masterdatabevoegdheid te verwijderen is het mogelijk het aantal conflicten zeer snel te laten dalen.
3. Hoeveel transactiecodes gebruikt een eindgebruiker uit autorisatierollen? Hiermee is in kaart te brengen of een eindgebruiker een bepaalde autorisatierol in het systeem wel gebruikt. In de praktijk blijkt dat ongeveer twintig procent van de gekoppelde rollen aan eindgebruikers niet door de eindgebruiker wordt gebruikt.

In de praktijk blijkt dat ongeveer tachtig procent van de conflicten die in het systeem voorkomen door toegang tot een combinatie van systeemtransacties, niet door de gebruikers wordt gebruikt. Het verwijderen van de twintig procent ongebruikte rollen kan dan al snel een grote impact hebben op het aantal conflicten dat in het systeem voorkomt. Gebruikers hebben wel toegang tot de combinatie van transacties, maar hebben simpelweg gezegd geen gebruik gemaakt van die combinatie. Uit analyse blijkt verder dat het redelijk eenvoudig is om ongeveer dertig tot veertig procent van de rolallocatie dan te verwijderen daar de gebruikers geen gebruik maken van de transactiecodes in deze rollen. Deze opschoning vooraf draagt bij aan de effectiviteit van de monitoring.

Zo'n twintig procent van de toegekende rollen wordt door eindgebruikers niet gebruikt

Daarnaast is het mogelijk de functiescheidingslijst te runnen over de geïmplementeerde rollen. Indien blijkt dat er conflicten voorkomen binnen de rollen, dan is het niet eenvoudig om een gedeelte van een conflict van een gebruiker af te nemen, daar dit een aanpassing in een autorisatieconcept vergt. Voordat de resultaten van de functiescheidingsconflicten binnen gebruikers naar de business process owners kunnen worden gecommuniceerd, moet ervoor gezorgd zijn dat de gebruikte rollen op zichzelf conflictvrij zijn. Indien dit niet het geval is, kan het voorkomen dat tijdens de Risk Remediation-fase de opmerking gemaakt wordt dat de rollen moeten worden aangepast, wat tot een vertraging in het remediationproces zal leiden.

Ten slotte kan in de Risk Analysis-fase worden beoordeeld of de functiescheidingstool geen false positives of negatives bevat door de uitkomsten van de tool te vergelijken met de uitkomsten van een andere tool (bijvoorbeeld van de huisaccountant). Voorwaarde hierbij is natuurlijk wel dat in deze vergelijkende tool gelijksoortige functiescheidingsregels worden gebruikt.

Tip: Maak gebruik van statistieken om vast te stellen welke mogelijkheden er zijn om autorisaties van gebruikers af te nemen om zo 'technische functiescheidingsconflicten ' te verminderen.

Risk Remediation

In deze fase dienen de functiescheidingsconflicten te worden opgelost door het conflict te verwijderen of door het risico te mitigeren. Daar uit ervaring blijkt dat er erg veel conflicten zullen voorkomen in het systeem, is het aan te bevelen om het remediationproces gefaseerd uit te voeren. Hierbij dient gestart te worden met de high risk-conflicten (conflicten die absoluut niet zijn toegestaan in het systeem) en daarna door te gaan met de medium risk-conflicten.

Starten met het remediaten van high risk-conflicten heeft als voordelen:

1. Over het algemeen zijn er niet bijzonder veel high risk-conflicten in het systeem (lijsten worden niet te lang).
2. High risks kunnen alleen worden opgelost door autorisaties af te nemen.
3. Door het beperkte aantal conflicten kunnen de business process owners worden getraind in het proces en in hun verantwoordelijkheden.
4. De grootste risico's zijn als eerste opgelost.

Tevens zijn in deze fase de statistieken goed bruikbaar. Deze statistieken geven immers aan of gedeelten van conflicten snel van gebruikers kunnen worden afgenomen, doordat bepaalde functionaliteit in een bepaalde periode niet gebruikt is. Het afnemen van bevoegdheid heeft geen enkele impact op de bedrijfsvoering en de gebruikers merken niet dat er bevoegdheid is afgenomen.

Echter, indien u echt functiescheidingen wilt voorkomen, en zeker in kleine bedrijfsonderdelen, dan dient u het proces van change management te accepteren. Taken zullen echt van rol naar rol moeten worden verplaatst of taken kunnen centraal worden uitgevoerd.

Tip: Begin met het remediaten van de high risk-conflicten, waardoor stakeholders worden getraind in het remediationproces en het gebruik van de tool. Daarnaast is er de quick win dat de grootste risico's het eerst worden opgelost.

In deze fase is het van groot belang dat de uitkomsten van de tool geen false positives of fase negatives bevatten. Indien er richting een gebruiker wordt gecommuniceerd dat bepaalde bevoegdheid zal worden afgenomen omdat hij een conflict heeft, dan moet te allen tijde worden voorkomen dat de gebruiker zal zeggen dat hij helemaal geen bevoegdheid heeft. Dit verstoort immers het communicatieproces met de verschillende gebruikers. Het gebruik van statistieken kan hier ook bij helpen doordat deze laten zien in hoeverre een gebruiker de bevoegdheid inderdaad niet heeft gebruikt.

Nadat alle high risks zijn opgelost, kan worden gestart met de medium risk voor bijvoorbeeld een workstream. Daar het aantal conflicten hierin naar verwachting redelijk beperkt zal zijn, blijft het remediationproces overzichtelijk.

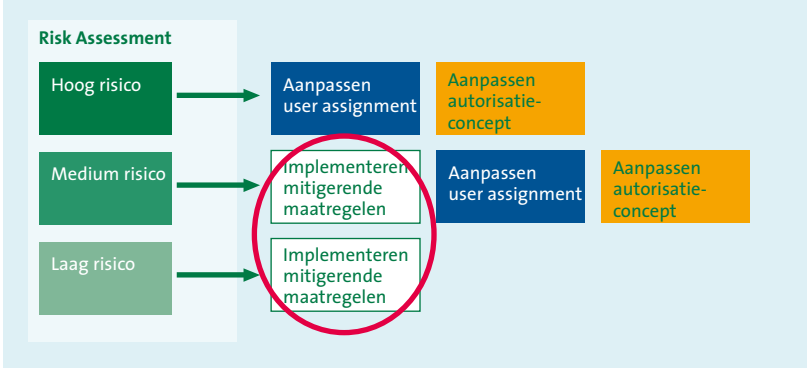
Risk Mitigation

In de Risk Mitigation-fase worden voor de conflicten die niet opgelost kunnen worden door het afnemen van autorisaties, mitigerende maatregelen getroffen. Indien het niet mogelijk is om bevoegdheden te beperken dan kan gebruik worden gemaakt van mitigerende maatregelen. Hierbij dient een gedegen proces te worden ingericht voor het goedkeuren van conflicten, het koppelen/goedkeuren van de mitigerende controle en het zorg dragen/monitoren dat de mitigerende maatregel ook daadwerkelijk wordt uitgevoerd. Hierbij dient de vraag te worden gesteld tot hoever bepaalde verantwoordelijkheid gaat. Bij veel ondernemingen hebben wij gezien dat centraal een tool wordt ingericht voor het identificeren van functiescheidingsconflicten en dat er centraal een project wordt gestart om bevoegdheden af te nemen. Echter, zodra het over mitigerende maatregelen gaat dan wordt de bevoegdheid voor de controle heel snel decentraal neergelegd. De vraag blijft dan of decentraal de mitigerende controle daadwerkelijk wordt uitgevoerd. Op centraal niveau wordt een zeer goed werkend brandmeldingsalarm geactiveerd en de lokale brandweer geeft aan dat de brand meester is, terwijl het lokale kantoor geheel afbrandt.

Door te starten met high risk-conflicten worden de grootste risico's het eerst opgelost

Tip: Definieer standaard mitigerende maatregelen, inclusief testplan, voor een functiescheidingsconflict. Laat ook de mitigerende maatregelen door de business accepteren. Geef de verschillende businessunits geen (of beperkte) mogelijkheid om zelf mitigerende maatregelen te definiëren (behoudens lokale SoD-conflicten).

Tip: Vraag periodiek de resultaten op van de uitgevoerde mitigerende maatregelen.



Figuur 4. **Het mitigeren van conflicten.**

Continuous Management & Monitoring

In de Continuous Management & Monitoring-fase zal periodiek de gehele set van functiescheidingsregels over de gebruikerspopulatie worden uitgevoerd. Hierbij dient onder andere te worden onderzocht:

- Zijn er gebruikers met conflicten die niet zijn toegestaan in het systeem?
- Zijn er gebruikers die conflicten hebben die niet zijn gemitigeerd?
- Zijn de mitigerende maatregelen op effectiviteit beoordeeld, en hebben zij adequaat gewerkt over een periode?

Daarnaast moeten er procedures ontwikkeld zijn die waarborgen dat de geïmplementeerde functiescheidingsregels up-to-date zijn én moet periodiek worden onderzocht of de mitigerende maatregelen ook daadwerkelijk worden uitgevoerd en dat ze effectief zijn.

Ten aanzien van het testen van de mitigerende maatregelen zien wij de tendens dat de laatste paar jaar ook veel ondernemingen bezig zijn om tooling in te richten waarmee gemonitord kan worden of de key controls van een onderneming daadwerkelijk getest zijn. Daarbij worden met behulp van workflows mails naar de betreffende testers gestuurd om aan te geven dat ze een bepaalde control moeten testen en is een real-time status beschikbaar van de controls die niet effectief zijn of die overdue zijn.

Foutsoorten in detail

Het aantal foutieve meldingen dat het gevolg is van verkeerde toepassing van een functiescheidingstool is veel groter dan veel organisaties beseffen. In onze praktijk komen we een groot aantal fouten regelmatig tegen. Tabel 1 bevat de fouten die wij nogal eens tegenkomen in de verschillende functiescheidingstools. Deze fouten zullen hierna kort worden toegelicht.

Het beoordelen van een functiescheidingslijst is erg complex. Indien op het autorisatieobject waardeniveau zal worden gekeken naar de conflicten dan zal de persoon die de conflicten zal beoordelen één of meer zeer grote Excellijsten krijgen met meer dan 20.000 entries. Daarnaast staan in deze lijsten vaak alleen de transactiecodes met autorisatieobjecten en de verschillende autorisatieobjectwaarden. Een typefout in zo'n lijst kan al tot gevolg hebben dat de resultaten van de lijst false positives of negatives bevatten.

1. Functiescheidingsconflicten

De volgende bevindingen komen wij tegen ten aanzien van gedefinieerde functiescheidingsconflicten:

Belangrijke functiescheidingsconflicten ontbreken in de functiescheidingslijst

Vaak wordt aan de hand van één of meer workshops een lijst gemaakt met functiescheidingsconflicten. Deze lijst dient vervolgens vertaald te worden naar de relevante transactiecodes en te worden ingericht in de functiescheidingstool. Indien de beheerder of de consultant deze activiteit niet uitvoert, kan het voorkomen dat het gedefinieerde conflict niet is opgenomen in de tool. Hierdoor zal niet over alle conflicten worden gerapporteerd. Daarnaast kan het voorkomen dat de accountant bepaalde conflicten belangrijk vindt die niet tijdens de verschillende workshops zijn gedefinieerd. Het is daarom belangrijk de accountant om input te vragen over de conflicten die opgenomen zullen gaan worden in de tool.

Functiescheidingsconflicten zijn opgenomen die in werkelijkheid geen conflict zijn

Bij een aantal organisaties hebben wij conflicten aangetroffen in de conflictenmatrix die geen conflict zijn. Als voorbeeld kan

Functiescheidingsregels
• Belangrijke conflicten ontbreken in functiescheidingslijst • Conflicten in functiescheidingslijst vertegenwoordigen geen risico
Toekenning van transactiecodes aan functiescheidingsconflicten
• Transactiecodes opgenomen in een conflict hebben niets te maken met het risico • Transactiecodes ontbreken in de functiescheidingsregels (standaard-SAP- en maatwerk-transactiecodes) • Weergave-transitiecodes niet opgenomen in conflict
Transactiecodes met incorrecte autorisatieobjecten
• Te veel autorisatieobjecten zijn opgenomen in het conflict • Optionele objecten zijn opgenomen in de functiescheidingsregels • Objecten die gecontroleerd worden door transactiecodes zijn niet opgenomen in de functiescheidingslijst • Transactiecodes zijn niet aligned binnen gedeelten van conflicten
Autorisatieobjecten met foutieve veldwaarden
• Objectactiviteitwaarden zijn opgenomen die niet relevant zijn voor de transactiecode • Relevante objectwaarden voor transactiecodes ontbreken • Objectwaarden voor weergave zijn opgenomen • Logica (ANY/ALL) wordt verkeerd gebruikt • Restricties voor transactiecodes zijn geïmplementeerd in de functiescheidingslijst • Geen objecten zijn gekoppeld aan transactiecodes • Incorrecte of niet-bestaande waarden zijn opgenomen • Incorrecte organisatieniveaus zijn opgenomen

Tabel 1. **Overzicht belangrijke fouten in functiescheidingsregels.**

hierbij gedacht worden aan het onderhouden van stamgegevens binnen crediteuren en het goedkeuren van wijzigingen binnen crediteuren. Het goedkeuren van wijzigingen binnen crediteuren is een activiteit waarbij een gebruiker een wijziging op een kritiek veld kan accorderen. Deze kritieke velden die goedkeuring op wijziging vergen, worden vastgelegd in de customizing in SAP en worden gebruikt om een vierogenprincipe in te richten. Hierbij geldt dat degene die een kritisch veld (bijvoorbeeld het bankrekeningnummer) wijzigt in SAP, zijn eigen wijziging niet kan goedkeuren. Dit is een inherente controle in SAP. Het conflict *onderhouden crediteuren* en *goedkeuren van wijzigen op crediteuren* is dus niet relevant daar SAP dit reeds via de configuratie afdwingt.

2. Het toekennen van transactiecodes aan functiescheidingsregels

Het toekennen van transactiecodes aan de functiescheidingsregels is van groot belang. Indien gebruikte transactiecodes immers niet aan een functiescheidingsregel worden gekoppeld, zal de tool geen gebruiker vinden die gebruik kan maken van de transactiecode. Het is van groot belang dat alle relevante transactiecodes aan de regels worden gekoppeld, teneinde een zo nauwkeurig mogelijk resultaat te krijgen. Ten aanzien van het koppelen van transactiecodes aan regels hebben wij de volgende observaties:

Het toekennen van weergave-transactiecodes aan functiescheidingsregels

Bij veel ondernemingen zien wij dat bepaalde weergave-transactiecodes in de regels zijn opgenomen. Indien weergave-transactiecodes zijn opgenomen in functiescheidingsregels, dan zullen al snel veel gebruikers worden geïdentificeerd die toegang hebben tot een gedeelte van een conflict, daar weergavebevoegdheid over het algemeen breder is uitgegeven aan gebruikers dan aanmaak- of mutatiebevoegdheid. De kans op false positives is hierdoor relatief groot. Immers, veel gebruikers zullen toegang hebben om data weer te geven in het systeem. Veelvoorkomende weergave-transactiecodes zijn de transactiecodes waarmee wijzigingen kunnen worden weergegeven. Dit komt hoogstwaarschijnlijk door de slechte omschrijvingen die SAP bij deze transactiecodes heeft gegeven.

Het toekennen van customizing transactiecodes aan functiescheidingsregels

In een aantal gevallen hebben wij gezien dat customizing transactiecodes zijn toegekend aan de functiescheidingsregels. Over het algemeen kan worden gesteld dat customizing transactiecodes geen risico opleveren met betrekking tot het invoeren van transactionele gegevens. Tevens kan gesteld worden dat customizing transactiecodes binnen een productieomgeving weinig invloed hebben op de integriteit van het systeem, daar de productieomgeving dicht hoort te staan voor customizing. Indien het systeem open zou staan, heeft een gebruiker nog steeds bevoegdheid voor het aanleggen van een transport request nodig. De aanwezigheid van customizing transactiecodes heeft een negatieve invloed op het aantal false positives.

Het toekennen van transactiecodes die niets met de functiescheidingsregel te maken hebben

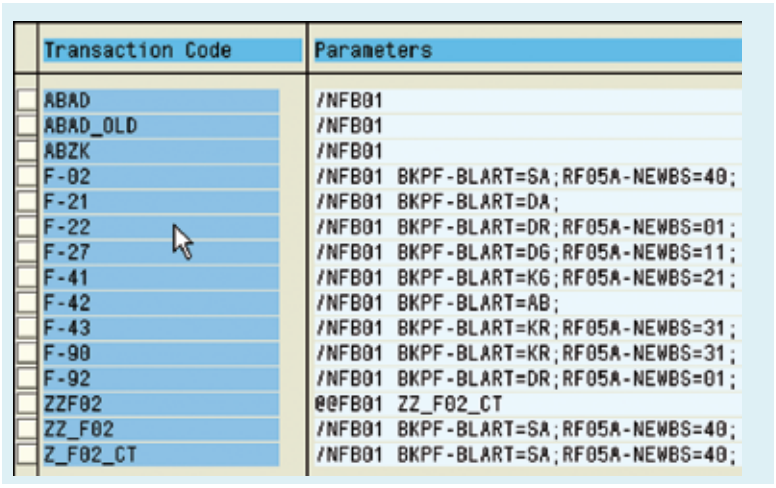
In een aantal gevallen hebben wij gezien dat transactiecodes erg ruim worden toegekend aan gedeelten van een functiescheidingsregel. Zo bevatten regels met de omschrijving verkooporders soms ook de transactiecodes voor contracten, offerteaanvragen en offertes of bevatten regels voor inkooporders ook de transactiecodes voor ATB's en contracten. Dit maakt de discussie met de business er niet eenvoudiger op. Indien immers een conflict wordt gerapporteerd met inkooporders, zal men in het kader van remediation ook op zoek gaan naar de echte inkooptransactiecodes en niet naar de transactiecodes voor bijvoorbeeld ATB's of contracten. De kans op false positives is dan erg groot. Dit heeft direct invloed op de acceptatie van de functiescheidingstool. De business process owners weten immers niet direct welke bevoegdheid er van een gebruiker moet worden ingenomen en zullen het conflict ook niet herkennen indien er ten onrechte transactiecodes in een conflict zijn opgenomen.

Het verschillend toekennen van transactiecodes aan functiescheidingsregels

Tijdens een aantal onderzoeken hebben wij gekeken naar de toekenning van transactiecodes aan gedeelten van conflictregels. Bijvoorbeeld in gevallen waarbij twee conflicten voorkomen waarbij bijvoorbeeld inkooporders worden gebalanceerd met leveranciers en goederenontvangsten. Het is dan op zijn minst opmerkelijk dat in de ene taak inkooporders meer trans-

	Language	Transaction code	Text
☐	N	FD04	Debiteurwijzigingen (boekhouding)
☐	N	FS04	Wijzigingen centr. grootboekrek.
☐	N	FSS4	Wijzigingen grootboek-bedrijfsnrs
☐	N	MK04	Wijzigingen crediteur (inkoop)
☐	N	MM04	Wijzigingsdocumenten artikel tonen
☐	N	XK04	Wijzigingen crediteur (centraal)

Figuur 5. **Voorbeelden van weergave-transactiecodes met misleidende omschrijving.**



Transaction Code	Parameters
ABAD	/NFB01
ABAD_OLD	/NFB01
ABZK	/NFB01
F-02	/NFB01 BKPF-BLART=SA;RF05A-NEWBS=40;
F-21	/NFB01 BKPF-BLART=DA;
F-22	/NFB01 BKPF-BLART=DR;RF05A-NEWBS=01;
F-27	/NFB01 BKPF-BLART=DG;RF05A-NEWBS=11;
F-41	/NFB01 BKPF-BLART=KG;RF05A-NEWBS=21;
F-42	/NFB01 BKPF-BLART=AB;
F-43	/NFB01 BKPF-BLART=KR;RF05A-NEWBS=31;
F-90	/NFB01 BKPF-BLART=KR;RF05A-NEWBS=31;
F-92	/NFB01 BKPF-BLART=DR;RF05A-NEWBS=01;
ZZF02	@@FB01 ZZ_F02_CT
ZZ_F02	/NFB01 BKPF-BLART=SA;RF05A-NEWBS=40;
Z_F02_CT	/NFB01 BKPF-BLART=SA;RF05A-NEWBS=40;

Figuur 6. **Voorbeelden van parametertransactiecodes.**

actiecodes zitten dan in de andere taak inkooporders. Het risico bestaat dan dat niet alle conflicten worden gerapporteerd (false negatives). Bij de SAP GRC Access controls tool is deze bevinding over het algemeen niet mogelijk daar in deze tool daadwerkelijk groepen van transactiecodes (functions) kunnen worden gecombineerd tot een risico. Hierdoor zullen de transactiecodes altijd hetzelfde zijn voor bijvoorbeeld de taak inkooporders (tenzij er meer gelijksoortige functies worden gemaakt).

Het ontbreken van transactiecodes in functiescheidingsregels

SAP bevat erg veel transactiecodes. Bij elke versie worden nieuwe transactiecodes geïntroduceerd. Het zal dus erg moeilijk zijn om volledig te zijn ten aanzien van het toekennen van transactiecodes aan gedeelten van een conflict. Het is evident dat het ontbreken van een transactiecode in een gedeelte van een conflict mogelijk kan leiden tot false negatives. Gebruikers zullen niet worden geïdentificeerd als gebruikers met een conflict. Vooral als transactiecodes ontbreken die wel in het autorisatieconcept gebruikt worden, is het risico op false negatives erg hoog. Het is aan te bevelen om in ieder geval te beoordelen welke transactiecodes daadwerkelijk in de autorisatierollen zijn opgenomen en kritisch te beoordelen of deze conflicten in een conflict thuishoren. Deze transactiecodes zijn immers bekend. Om te voorkomen dat ontbrekende transactiecodes tijdens het dagelijks onderhoud ongemerkt in SAP worden geautoriseerd, is het aan te bevelen om van een zo volledig mogelijke lijst van transactiecodes uit te gaan.

Voorbeelden van transactiecodes die vrijwel nooit in functiescheidingslijsten voorkomen, zijn de weergave-transactiecodes voor verkoopcondities (bijvoorbeeld VK13 en TK13). Met deze transactiecodes kunnen, mits er aanmaak-/wijzigbevoegdheid is, op autorisatieobjectniveau gewoon condities worden aangelegd.

Een ander voorbeeld zijn de parametertransactiecodes. Figuur 6 bevat de parametertransactiecodes uit een systeem voor de transactiecode FB01 (boeken van een financieel document). Deze parametertransactiecodes bieden over het algemeen dezelfde functionaliteit als de transactiecode waaraan gerefereerd wordt. In dit voorbeeld zijn de grootste verschillen het boekingsdocument en de posting key waarmee geboekt gaat worden. Echter, in het initiële scherm kunnen deze twee weer worden aangepast waardoor het mogelijk is een ander type boeking te maken. Zo kan standaard met de transactiecode F-02 een grootboekboeking worden gemaakt, maar indien het documentsoort en de posting key worden aangepast, zal er een factuur van een leverancier mee geboekt kunnen worden (net zoals met de FB01 kan). Het is dus van belang deze parametertransactiecodes mee te nemen in de functiescheidingslijst daar anders de kans op false negatives reëel is.

Het ontbreken van maatwerktransactiecodes

In veel van de functiescheidingsregels die wij aantreffen in de systemen wordt uitgegaan van de standaard SAP-transactiecodes. De maatwerktransactiecodes (beginnend met een Z of een Y) worden vaak niet meegenomen in de functiescheidingsregels. Daarnaast zien wij dat indien de maatwerktransactiecodes wel zijn opgenomen in de set van regels, er geen autorisatieobjecten zijn gekoppeld. Belangrijke reden hiervoor is natuurlijk dat over het algemeen geen autorisatiecontroles in het maatwerk worden opgenomen.

3. Het toekennen van autorisatieobjecten aan transactiecodes

Indien een gebruiker toegang heeft gekregen tot een transactiecode in SAP, worden er binnen de transactiecode additionele controles uitgevoerd (bijvoorbeeld op toegang tot een vestiging of toegang tot een documentsoort). In SAP zijn er ongeveer 1400 autorisatieobjecten. Een autorisatieobject bevat verder minimaal één veld waarop geautoriseerd kan worden, maar meestal meer. Eén van de belangrijkste, veelvoorkomende, velden in een autorisatieobject is het veld 'activiteit', waarmee geregeld kan worden welke bevoegdheid een gebruiker krijgt (bijvoorbeeld aanmaken, wijzigen of weergeven).

Indien een gebruiker bijvoorbeeld de automatische betaalrun wil uitvoeren, heeft hij activiteitwaarde 21 nodig voor autorisatieobjecten F_REGU_BUK en F_REGU_KOA. Deze beide autorisatieobjecten bevatten meerdere activiteiten, echter het daadwerkelijk uitvoeren van de betaalrun kan alleen indien de gebruiker activiteit 21 heeft. Indien met behulp van de functiescheidingslijst wordt gekeken naar wie de betaalrun kan uitvoeren, dan moet in de lijst heel specifiek worden gekeken naar

waarde 21. Wordt bijvoorbeeld gekeken naar F110 in combinatie met waarde 11 (uitvoeren proposal run) en 12 (wijzigen proposal), dan wordt gekeken naar wie een betaalvoorstel kan maken. Uit bovenstaand voorbeeld blijkt dat de toegekende waarde voor objecten van groot belang is voor de juistheid van de resultaten. Verkeerde waarden zullen grote invloed hebben op false positives en false negatives.

Bij het koppelen van autorisatieobjecten aan de transactiecodes wordt vaak uitgegaan van de door SAP uitgeleverde settings in tabel USOBT. Deze tabel dient echter te worden beschouwd als een goedbedoeld voorstel van SAP, maar dit voorstel is zeker niet volledig correct. Afhankelijk van de inrichting van het SAP-systeem zullen controles op autorisatieobjecten worden uitgevoerd. Daarnaast bevat het voorstel van SAP vaak te veel en soms ook te weinig autorisatieobjecten. Bovendien kan de beheerder of consultant autorisatiecontroles handmatig uitzetten in transactiecode SU24 of SU25.

Het gebruik van optionele autorisatieobjecten

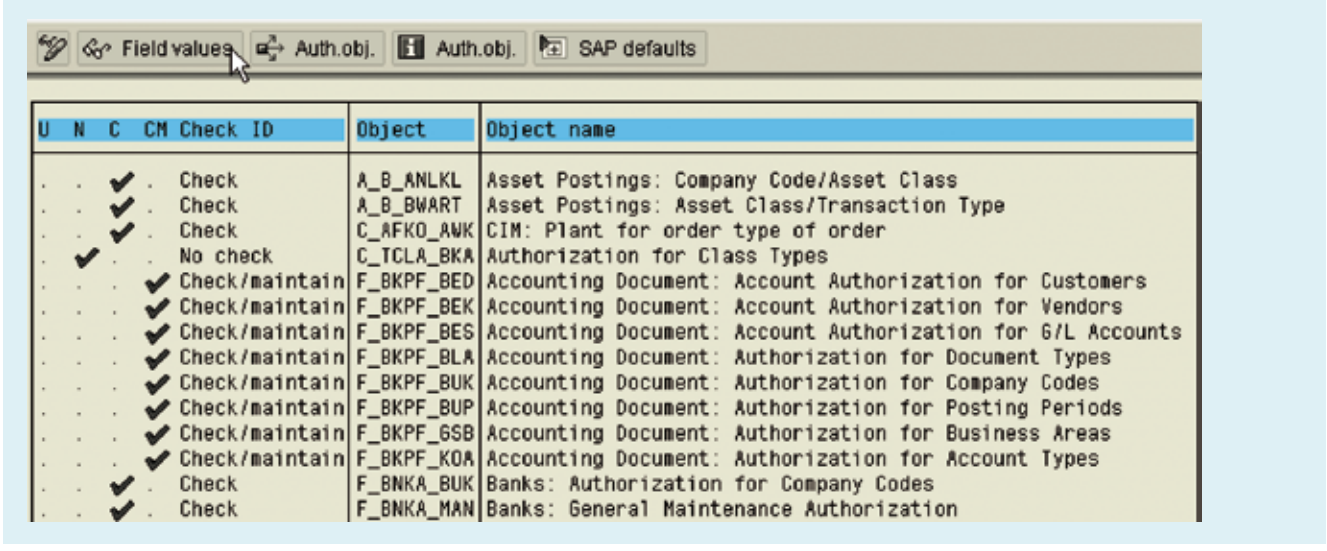
Optionele autorisatieobjecten zijn objecten die alleen door SAP gecontroleerd zullen worden indien:

- bepaalde settings in masterdata zijn gemaakt (autorisatiegroepen);
- bepaalde settings in customizing zijn gemaakt (activeren van controles of het koppelen van autorisatiegroepen).

Indien deze settings niet zijn ingesteld tijdens de implementatie van SAP, zullen deze autorisatieobjecten niet door SAP worden gecontroleerd. Als we kijken naar transactiecode FB01, zien wij dat de in figuur 7 weergegeven voorstelwaarden vaak voorkomen in SAP.

Uit dit overzicht blijkt dat de profielgenerator in SAP zal opkomen met de autorisatieobjecten die zijn aangevinkt bij de CM (check maintain)-indicator. Vaak wordt gedacht dat al deze controles worden uitgevoerd. Echter, de meeste van deze objecten hebben settings nodig in customizing of in masterdata:

- F_BKPF_BED. Dit autorisatieobject zal alleen worden gecontroleerd indien de autorisatiegroepen binnen de stamgegevens van klanten zijn onderhouden. Indien deze velden niet zijn onderhouden, zal SAP geen controle uitvoeren op dit autorisatieobject.
- F_BKPF_BEK. Dit autorisatieobject zal alleen worden gecontroleerd door SAP indien de autorisatiegroepen binnen de stamgegevens van leveranciers zijn onderhouden. Indien deze velden niet zijn onderhouden, zal SAP geen controle uitvoeren op dit autorisatieobject.
- F_BKPF_BES. Dit autorisatieobject zal alleen worden gecontroleerd door SAP indien de autorisatiegroepen binnen de stamgegevens van grootboekrekeningen zijn onderhouden. Indien deze velden niet zijn onderhouden, zal SAP geen controle uitvoeren op dit autorisatieobject.
- F_BKPF_BLA. Dit autorisatieobject zal alleen worden gecontroleerd door SAP indien autorisatiegroepen binnen de financiële documentsoorten zijn aangemaakt. Zijn deze velden niet onderhouden in customizing, dan zal SAP geen controle op dit autorisatieobject uitvoeren.
- F_BKPF_BUP. Dit autorisatieobject zal alleen worden gecontroleerd door SAP indien autorisatiegroepen zijn gekoppeld aan de boekingsperiode. Zijn deze velden niet onderhouden binnen de boekingsperiode, dan zal SAP geen controle op dit autorisatieobject uitvoeren.
- F_BKPF_GSB. Dit autorisatieobject zal alleen worden gecontroleerd door SAP indien er gebruik wordt gemaakt van business areas. Indien er geen business areas zijn aangemaakt, zal de gebruiker het veld business area niet invullen tijdens het



Figuur 7. **Voorbeelden van de check indicator voor transactiecode FB01.**

maken van financiële boekingen en zal SAP op dat veld geen controle uitvoeren.

Hieruit blijkt dat (in veel gevallen) SAP voor transactiecode FB01 alleen een controle zal uitvoeren op de autorisatieobjecten F_BKPF_KOA en F_BKPF_BUK. Zelfs indien al deze optionele settings wel zijn gemaakt, dan nog dient erg kritisch te worden gekeken naar de toekenning van de autorisatieobjecten. Wat is immers de kans dat indien transactiecode FB01 wordt gebruikt om een crediteurenfactuur te boeken, dat SAP zal controleren op het object F_BKPF_BED dat de afscherming van debiteuren bevat?
Indien optionele objecten in de regels worden meegenomen, is de kans op false negatives aanwezig.

Het koppelen van te veel autorisatieobjecten aan transactiecodes

Indien te veel autorisatieobjecten binnen de functiescheidingslijst aan transactiecodes worden gekoppeld, dan bestaat het risico van false negatives. Immers, een eindgebruiker heeft minder autorisatie nodig dan daadwerkelijk door SAP wordt gecontroleerd. Buiten de optionele objecten wordt nog te veel uitgegaan van de default settings in transactiecode SU24. De objecten waar SAP mee opkomt voor een transactiecode zijn niet allemaal noodzakelijk om een transactiecode uit te voeren.

Het koppelen van te weinig autorisatieobjecten aan transactiecodes

In sommige gevallen worden ook te weinig autorisatieobjecten gekoppeld aan transactiecodes. Ook dit is weer afhankelijk van het gebruik van de settings in transactiecode SU24. Indien het niet duidelijk is welke autorisatieobjecten gecontroleerd zullen worden door een bepaalde transactiecode, dan zijn er drie mogelijkheden:
1. Kijk naar de autorisatieobjecten die soortgelijke transactiecode gebruiken. Deze soortgelijke transactiecodes maken over het algemeen gebruik van dezelfde autorisatieobjecten. (Transactiecode V-01 controleert dezelfde autorisatieobjecten als transactiecode VA01.)
2. Maak een autorisatierol met de transactiecode en koppel deze aan een testgebruiker. Test vervolgens de rol met de testgebruiker. Met behulp van de output van transactiecode SU53 kan worden weergegeven welk autorisatieobject wordt gecontroleerd.
3. Zet een autorisatietracé op de transactiecode (transactiecode ST01). Dit tracé zal gedetailleerd laten zien welke autorisatieobjecten en waarden worden gecontroleerd bij het uitvoeren van de transactiecode.

De inrichting van regels voor stamgegevens van crediteuren en debiteuren

Het opstellen van functiescheidingsregels voor de stamgegevens van crediteuren en debiteuren is erg moeilijk daar er verschillende smaken mogelijk zijn. Zoals bekend zijn er binnen de crediteurenstamgegevens drie verschillende views aan te maken:
1. *de centrale view*, die onder andere de bankaccount van de leverancier bevat;
2. *de financiële view*, waarin de crediteur aan een companycode wordt gehangen;
3. *de inkoopview*, waarin de leverancier aan een inkooporganisatie wordt gehangen.

Bij het opstellen van de functiescheidingsregels zullen afspraken gemaakt moeten worden over de views die moeten worden beoordeeld. In tabel 2 is een aantal voorbeeldconflicten weergegeven die crediteurenstamgegevens bevatten.

In tabel 3 is een aantal voorbeeldconflicten weergegeven die debiteurenstamgegevens bevatten.

Voor beide voorbeelden is de toekenning van views aan de objecten van groot belang. Immers, te veel objecten controleren brengt het risico van false negatives met zich mee. Voor de regels van zowel debiteuren als crediteuren kan als uitgangspunt worden gebruikt dat een functiescheidingsregel maximaal drie objecten mag controleren voor crediteuren- en debiteurenbeheer. Voor bijvoorbeeld de GRC Access controls tool heeft dit tot gevolg dat er meerdere functies moeten worden gemaakt voor de verschillende views in de masterdata. Voor zowel Approva als SecurInfo zal gelden dat afhankelijk van het conflict dat is gedefinieerd objecten voor masterdata verschillend moeten worden toegekend.

Taak 1	Taak 2	Opmerkingen
Onderhouden crediteur	Betalen	Centrale view bevat bankaccount = object F_LFA1_GEN
Onderhouden crediteur	Invoeren crediteurenfactuur	Zonder financiële view kan geen factuur worden gemaakt = object F_LFA1_BUK
Onderhouden crediteur	Invoeren inkooporder	Zonder inkoopview kan geen inkooporder worden gemaakt = object M_LFA1_EKO

Tabel 2. **Voorbeelden van conflicten voor crediteurenstamgegevens.**

Taak 1	Taak 2	Opmerkingen
Onderhouden debiteur	Betalen creditnota	Centrale view bevat bankaccount = object F_KNA1_GEN
Onderhouden debiteur	Invoeren creditnota	Zonder financiële view kan geen creditnota worden gemaakt = object F_KNA1_BUK
Onderhouden debiteur	Invoeren creditnota-request	Zonder verkoopview kan geen creditnota-request worden gemaakt = V_KNA1_VKO

Tabel 3. **Voorbeelden van conflicten voor debiteurenstamgegevens.**

De inrichting van regels voor goederenontvangsten

Veel voorkomende conflicten hebben betrekking op Goederenontvangsten. Eén van de bekendste is het conflict Inkooporders vs Goederenontvangsten. Een belangrijke transactiecode om een goederenontvangst op een inkooporder te boeken is de transactiecode MIGO. In figuur 8 staan de belangrijkste autorisatieobjecten voor MIGO weergegeven.

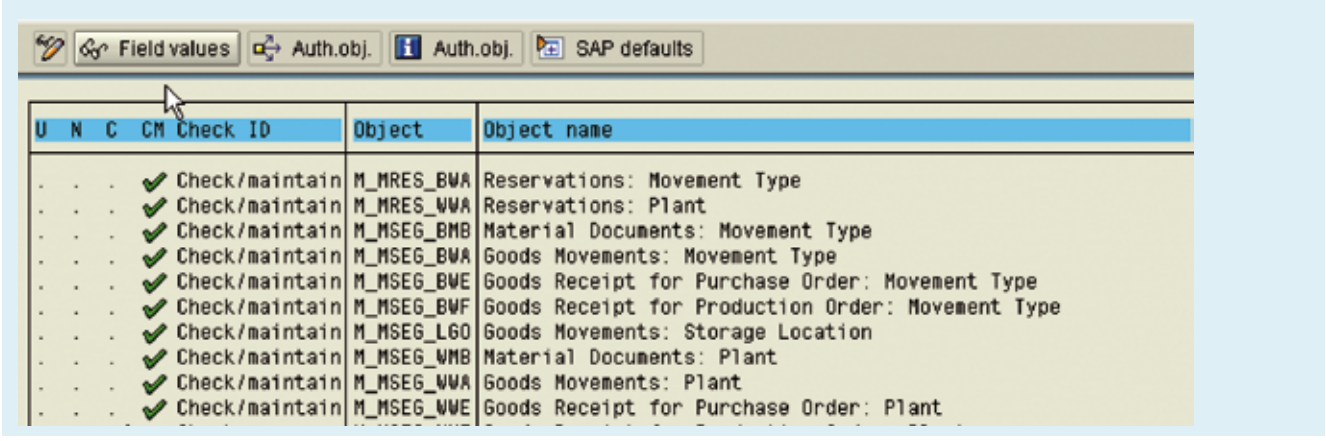
Uit dit overzicht blijkt dat binnen MIGO een aantal autorisatiecontroles mogelijk is, afhankelijk van wat er met transactiecode MIGO gebeurt. Indien een gebruiker een inkooporder wil inboeken, dan is het duidelijk dat een controle op de autorisatieobjecten M_MSEG_BWE en M_MSEG_WWE zal plaatsvinden. Dit zijn immers de autorisatieobjecten voor het inboeken van een goederenontvangst op een inkooporder. De andere objecten zijn voor het inboeken van een goederenontvangst op een inkooporder niet relevant. We zijn immers niet geïnteresseerd in gebruikers die een reservering, een goederenbeweging of een goederenontvangst op een inkooporder kunnen laten plaatsvinden. De functiescheidingsregels voor goederenontvangst op een inkooporder dienen dus maximaal twee objecten te controleren. Maakt een gebruiker van transactiecode MB01 voor goederenontvangsten gebruik, dan is het natuurlijk duidelijk dat dezelfde objecten zullen moeten worden gecontroleerd.

4. Het toekennen van autorisatieobjectwaarden aan autorisatieobjecten voor transactiecodes

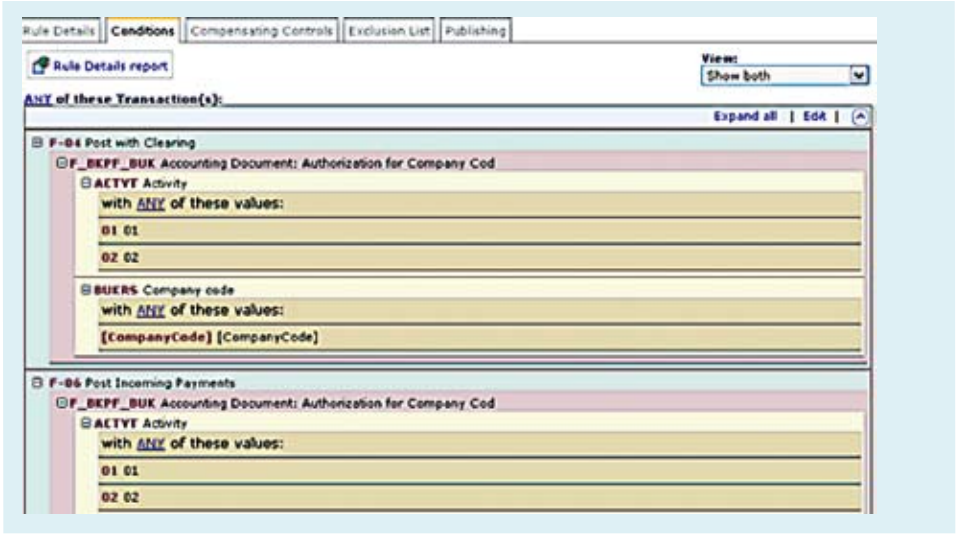
Het belang van de logica van de tool voor het lezen van objectwaarden

De logica waarmee de tool de functiescheidingsregels leest is van groot belang. Hierbij dient het doel van de tool niet uit het oog te worden verloren. Het doel van de tool is immers het vaststellen of een gebruiker een functiescheidingsconflict heeft. Dit zal de tool over het algemeen doen door te controleren of de gebruiker een transactiecode heeft aan de ene kant van het conflict (LHS) en een van de transactiecodes (RHS) aan de andere kant van het conflict. Daarnaast zal de tool kijken of de gebruiker alle autorisatieobjecten heeft en de daaraan gekoppelde autorisatieobjectwaarden.

Figuur 9 toont een gedeelte van een functiescheidingsregel zoals gebouwd in de Approva-tool. In dit voorbeeld vallen twee zaken op. Allereerst controleert de Approva-tool in dit geval maar één autorisatieobject voor transactiecode F-04. Een financiële boeking in SAP controleert over het algemeen twee autorisatieobjecten, te weten F_BKPF_BUK en F_BKPF_KOA. Het feit dat het object F_BKPF_KOA ontbreekt in deze regel kan tot gevolg hebben dat er door deze regel personen worden geïdentificeerd die eigenlijk geen conflict hebben (false positives). Indien we naar de waarden in het autorisatieobject kijken, dan zien we dat de ANY-logica relevant is. Indien een gebruiker waarde 01 (aanleggen) of waarde 02 (wijzigen) heeft, dan zal de Approva-tool de gebruiker identificeren als een gebruiker die toegang heeft. Indien we gedetailleerd naar de transactiecode kijken, dan wordt duidelijk dat het met deze transactiecode mogelijk is een financiële boeking te maken. Wordt iets in SAP aangemaakt, dan zal de gebruiker ten minste de bevoegdheid moeten hebben tot aanmaken (waarde 01). Indien de gebruiker iets wil wijzigen, heeft hij waarde 02 nodig. Bij deze transactiecode zal een gebruiker eerst moeten aangeven voor welk SAP-bedrijfsnummer hij iets wil posten. Op dat moment wordt direct gecontroleerd of de gebruiker ook daadwerkelijk bevoegdheid heeft tot aanmaken (01). Indien de gebruiker deze bevoegdheid niet heeft, zal hij ook niet verder kunnen in de transactiecode. Dit heeft dus tot gevolg dat de in figuur 9 weergegeven regel op objectniveau niet goed staat gedefinieerd. Waarde 02 is niet nodig voor het uitvoeren van deze transactiecode en het risico is dus aanwezig dat de tool mensen met de transactiecodewaarde 02 zal rapporteren.



Figuur 8. **Voorbeeld check indicators voor transactiecode MIGO.**



Figuur 9. **Voorbeeld functiescheidingsregel zoals ingericht in Approva.**

De ANY-logica voor objectwaarden heeft tot gevolg dat tijdens de inrichting van de functiescheidingsregels heel kritisch dient te worden gekeken naar de objectwaarden die worden toegekend aan transactiecodes. Hierbij zijn de volgende categorieën te onderscheiden:

- het toekennen van weergavewaarden aan autorisatieobjecten (weergave is van minder belang);
- het toekennen van te veel waarden aan objecten (01 vs. 02).

Het invoeren van beperkingen in velden

Een fout die soms wordt gemaakt is dat autorisatievelden al worden ingevuld in de tool. Indien de tool wordt gebruikt voor het identificeren van gebruikers die inkooporders kunnen aanmaken, dan wordt in sommige gevallen het belangrijkste documentsoort reeds in de regel in de tool gezet (bijvoorbeeld documentsoort NB). Echter, veel klanten hebben ook een maatwerkdocumentsoort gemaakt. Indien beperkingen op bijvoorbeeld documentsoort worden ingevuld, dan bestaat de kans dat andere relevante documentsoorten niet worden bekeken, waardoor niet alle gebruikers die toegang hebben tot de andere documentsoorten zullen worden gerapporteerd (false negatives).

Juiste inrichting biedt vertrouwen

Functiescheidingstools zijn in principe zeer waardevolle hulpmiddelen. Als zo'n tool optimaal is ingericht en geïmplementeerd, werkt die software als een adequate brandmelder. Pas als er echt conflicterende transacties aan een gebruiker worden gekoppeld, gaat het alarm af. Zolang dat niet het geval is, is het gevoel van veiligheid terecht. Mits de tool goed is ingericht!

Dat gevoel van veiligheid heeft positieve gevolgen voor de audits door een accountancyorganisatie. Als deze volledig kan vertrouwen op de juiste implementatie van een functiescheidingstool, kan de auditor erop vertrouwen dat er geen (niet-gemitigeerde) functiescheidingsconflicten voorkomen in de SAP-applicatie. Zoals hierboven uitgebreid betoogd, hebben we in de praktijk meer dan eens ervaren dat organisaties *ten onrechte* blind varen op hun implementatie. De uitgebreide lijst van mogelijke fouten die we hierboven noemden, is niet fictief maar gebaseerd op onze ervaringen.

Vaak varen organisaties ten onrechte blind op de inrichting van hun functiescheidingstool

Functiescheidingstools kunnen waardevolle hulpmiddelen zijn. Daar zijn ook de auteurs van overtuigd. Bedrijven die gebruik willen maken van functiescheidingstools doen er goed aan de inrichting en/of de controle daarvan over te laten aan specialisten. Het aantal beschikbare specialisten op dat gebied is nog niet bepaald groot. Organisaties (én hun accountants!) die willen blindvaren op die tools, ontkomen er niet aan om de inrichting daarvan aan specialisten voor te leggen. Alleen dan is volledig vertrouwen in de meldingen van die tools terecht!